Appunti delle lezioni del corso di Aritmetica

Giovanni Gaiffi

9 gennaio 2016

Indice

Capitolo 1. Lezione del 26 settembre 7
1. I numeri di Fibonacci e le successioni definite per ricorrenza. 7
2. Una formula per i numeri di Fibonacci 7
3. Un metodo per le ricorrenze lineari a coefficienti costanti 9
4. Qualche esercizio... 10

Capitolo 2. Lezioni del 1 e 2 ottobre 13
1. La divisione euclidea 13
2. Il massimo comun divisore e l'algoritmo di Euclide 14
3. Una stima del numero di passi necessario per portare a termine l'algoritmo di Euclide 17
4. L'Identità di Bezout 19
5. Un metodo costruttivo per ottenere l'Identità di Bezout 21
6. Le equazioni diofantee 22
7. Esempio di risoluzione di una equazione diofantea 25
8. Esercizi 26

Capitolo 3. Lezione del 8 ottobre 29
1. Alcune riflessioni sui numeri primi 29
2. Congruenze 32
3. Calcolo veloce dei resti e basi numeriche 33
4. Inverso di un numero modulo un intero positivo 34
5. Esercizi 36

Capitolo 4. Lezione del 9 ottobre 39
1. Metodo per risolvere le congruenze lineari in una incognita 39
2. Esempi di risoluzione di una equazione diofantea (usando le congruenze) 41
3. Sistemi di congruenze. Il teorema cinese del resto 43
4. Esercizi 46

Capitolo 5. Lezione del 16 ottobre 51
1. Il piccolo teorema di Fermat 51
2. Un interessante risvolto applicativo: il metodo di crittografia RSA 54
3. Le classi di resto modulo un intero positivo. Struttura additiva e moltiplicativa. 56
4. Esercizi 58

Capitolo 6. Lezione del 23 ottobre 61
1. Gruppi e sottogruppi: prime proprietà 61
2. Laterali destri di un sottogruppo. Il Teorema di Lagrange. Ordine di un elemento 63
3. Una prima applicazione: la funzione di Eulero e il Teorema di Eulero. 65
4. Esercizi 67

Capitolo 7. Lezioni del 29 ottobre e 30 ottobre 69
1. Omomorfismi di gruppi 69
2. Un esempio importante: il gruppo simmetrico 72
3. Esercizi 77

Capitolo 8. Lezione del 5 novembre 81
1. Sottogruppi normali e quozienti 81
2. Qualche esempio 84
3. Esercizi 87

Capitolo 9. Lezione del 6 novembre 89
1. Anelli 89
2. Omomorfismi 92
3. Ideali di un anello e anelli quoziente 92
4. Esercizi 94

Capitolo 10. Lezione del 13 novembre 95
1. Ancora su ideali e anelli quoziente 95
2. Due esempi 96
3. Anelli euclidei 98
4. Esercizi 99

Capitolo 11. Lezione del 20 novembre 101
1. Un anello euclideo è un dominio a ideali principali 101
2. Questioni di divisibilità nei PID. Ideali primi e massimali nei PID. 102
3. Un anello euclideo è un dominio a fattorizzazione unica 103
4. Gli elementi primi nell'anello degli interi di Gauss 104
5. Complementi (facoltativo): esempio di un dominio non UFD, in cui esistono elementi irriducibili ma non primi 105
6. Esercizi 107

Capitolo 12. Lezione del 26 novembre 109
1. 'Inventare' radici di polinomi 109
2. Approfondimenti sulle estensioni semplici di campi 110
3. Creare un campo con tutte le radici di un polinomio 113
4. Esercizi 114

Capitolo 13. Lezione del 27 novembre 115
1. Alcune considerazioni sul grado delle estensioni di campi 115
2. Estensioni algebriche 118
3. La caratteristica di un campo 119
4. Esercizi 119

Capitolo 14. Lezioni del 11 e 17 dicembre 121
1. Campi di spezzamento 121
2. Un teorema di isomorfismo per campi di spezzamento 122
3. La classificazione dei campi finiti 124
4. Campi finiti e gruppi ciclici 126
5. Esercizi 128

Capitolo 15. Qualche ulteriore esercizio o spunto di riflessione 129
1. Esercizi 129

2. Soluzione di due esercizi sui campi finiti 131
Bibliografia 133

CAPITOLO 1

Lezione del 26 settembre

1. I numeri di Fibonacci e le successioni definite per ricorrenza.

Consideriamo la successione di numeri F_n ($n \in \mathbb{N}$) così definita:

- $F_0 = 0$
- $F_1 = 1$
- per ogni $n \geq 2$,

$$F_n = F_{n-1} + F_{n-2}$$

Per prima cosa "costruiamo" i primi numeri della successione :
$F_0 = 0$
$F_1 = 1$
$F_2 = F_0 + F_1 = 1$
$F_3 = F_2 + F_1 = 1 + 1 = 2$
$F_4 = 2 + 1 = 3$
$F_5 = 3 + 2 = 5$
$F_6 = 5 + 3 = 8$
$F_7 = 8 + 5 = 13$
$F_8 = 13 + 8 = 21$
e così via.. I numeri F_n si dicono **numeri di Fibonacci** (con riferimento a Leonardo da Pisa, che pubblicò sotto il nome di Fibonacci il suo libro più celebre, *Liber abaci*, nel 1202)[1].

Osserviamo che, per conoscere il numero F_n non ci basta conoscere il numero precedente F_{n-1}, ma bisogna conoscere anche il numero F_{n-2}.

Una successione di questo tipo, ossia in cui il termine ennesimo si costruisce sapendo i termini precedenti, si dice *successione definita per ricorrenza*. Perché la successione sia ben definita, bisogna conoscere i valori iniziali. Per esempio, nel caso di Fibonacci, visto che ogni termine chiama in causa i due precedenti, F_0 e F_1 devono essere noti fin dall'inizio (non possono essere ricavati dalla "regola ricorsiva" $F_n = F_{n-1} + F_{n-2}$ che non li riguarda).

Un altro esempio di successione definita per ricorrenza potrebbe essere: $b_0 = 7$ e, per ogni $n \geq 1$, $b_n = 4b_{n-1}^2$.

2. Una formula per i numeri di Fibonacci

Partiamo da una successione, molto semplice, definita per ricorrenza:

$$a_0 = 1$$

$$a_n = 3a_{n-1} \qquad \forall n \geq 1$$

[1]Rispetto alla notazione usata a lezione, gli indici dei numeri F_n sono stati traslati di 1: a lezione avevo posto $F_0 = 1, F_1 = 1, F_2 = 2$ etc...

Più avanti, un'altra nota a pié di pagina vi inviterà a verificare che i risultati ottenuti qui e quelli ottenuti a lezione sono identici, a patto di tenere conto di questa traslazione di 1.

Sappiamo trovare una *formula* per a_n, ossia una equazione che ci permetta di calcolare a_n direttamente, senza dover calcolare prima a_{n-1}? Proviamo a scrivere i primi termini della successione:
$a_0 = 1$
$a_1 = 3 \cdot 1 = 3$
$a_2 = 3 \cdot 3 = 3^2$
$a_3 = 3 \cdot 3^2 = 3^3$
e così via.. Non ci mettiamo molto a congetturare che la formula giusta per a_n potrebbe essere:

$$a_n = 3^n$$

Dalla congettura alla dimostrazione in questo caso il passo è breve: ci basta notare che le due successioni $\{a_n\}$ e $\{3^n\}$ soddisfano la stessa regola ricorsiva e la stessa condizione iniziale, dunque si mostra facilmente per induzione che devono coincidere termine a termine, ossia $a_n = 3^n$ per ogni $n \in \mathbb{N}$.

Ma torniamo a Fibonacci: come possiamo trovare una formula per i numeri F_n ? Memori dell'esempio precedente, possiamo cominciare da un tentativo; proviamo se può funzionare una formula del tipo:

$$F_n = \alpha^n$$

per un qualche $\alpha \in \mathbb{R} - \{0\}$ (certamente $\alpha = 0$ non andrebbe bene, essendo $F_1 = 1$..).
Se fosse così, allora, visto che per $n \geq 3$ vale $F_n = F_{n-1} + F_{n-2}$, dovremmo avere

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2}$$

che, dividendo per α^{n-2}, diventa

$$\alpha^2 = \alpha + 1$$

Quindi il nostro numero α dovrebbe essere una radice del polinomio $x^2 - x - 1$. Sappiamo che le radici di tale polinomio sono due:

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \beta = \frac{1-\sqrt{5}}{2}$$

Cominciamo a pensare di essere sulla strada giusta: infatti, rifacendo il ragionamento a ritroso, notiamo che con il nostro tentativo abbiamo trovato due numeri $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ che soddisfano:

$$\alpha^2 = \alpha + 1 \qquad \beta^2 = \beta + 1$$

e quindi anche, per ogni $n \geq 2$:

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2} \qquad \beta^n = \beta^{n-1} + \beta^{n-2}$$

Entrambe le successioni $\{\alpha^n\}$ e $\{\beta^n\}$ soddisfano dunque la stessa regola ricorsiva della successione di Fibonacci: per $n \geq 2$, il termine n-esimo è somma dei due termini precedenti.
Il problema è che né α^1 né β^1 sono uguali a F_1 che è 1. Inoltre α^0 e β^0 non sono uguali a F_0, che è 0.

In altre parole queste successioni non "partono" dagli stessi numeri con cui parte la successione di Fibonacci, dunque i loro termini sono poi molto diversi dai numeri di Fibonacci.

Possiamo rimediare però osservando che anche una successione del tipo $\{a\ \alpha^n + b\ \beta^n\}$, con a e b numeri reali qualunque, soddisfa la richiesta che il termine n-esimo sia somma dei due termini precedenti:

$$a\alpha^n + b\beta^n = (a\alpha^{n-1} + b\beta^{n-1}) + (a\alpha^{n-2} + b\beta^{n-2})$$

Dunque potremmo controllare se è possibile scegliere a e b in modo che $a\alpha^0 + b\beta^0 = 0$ e $a\alpha^1 + b\beta^1 = 1$. Si vede subito che il sistema di equazioni:

$$a\ \left(\frac{1+\sqrt{5}}{2}\right)^0 + b\ \left(\frac{1-\sqrt{5}}{2}\right)^0 = 0$$

$$a\left(\frac{1+\sqrt{5}}{2}\right)^1 + b\left(\frac{1-\sqrt{5}}{2}\right)^1 = 1$$

ha come unica soluzione $a = \dfrac{1}{\sqrt{5}}$, $b = -\dfrac{1}{\sqrt{5}}$. Dunque la successione $\{c_n\}$ definita, per ogni $n \in \mathbb{N}$, così:

$$c_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

soddisfa tutte le richieste della successione di Fibonacci.

Ripetiamo allora, per metterlo bene in evidenza, il ragionamento conclusivo: poiché entrambe le successioni soddisfano la stessa legge ricorsiva e le stesse condizioni iniziali, allora (si tratta di una facile applicazione del principio di induzione) coincidono, ossia $c_n = F_n$ per ogni $n \in \mathbb{N}$.

Abbiamo dunque dimostrato il seguente:

TEOREMA 1.1. *Dato $n \in \mathbb{N}$, vale la seguente formula per i numeri di Fibonacci*[2]*:*

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

3. Un metodo per le ricorrenze lineari a coefficienti costanti

Il metodo che abbiamo usato per trovare la formula per i numeri di Fibonacci è partito da un tentativo ("vediamo se per caso vanno bene soluzioni del tipo α^n") ma si è rivelato poi molto efficace. Osserviamo che, ripetendo il ragionamento, il metodo si può generalizzare al caso di successioni definite per ricorrenza in cui la legge ricorsiva sia *lineare e a coefficienti costanti*, ossia del tipo:

$$a_n = \gamma_1 a_{n-1} + \gamma_2 a_{n-2} + \gamma_3 a_{n-3} + \cdots + \gamma_i a_{n-i}$$

dove i γ_j sono numeri complessi.
Per esempio prendiamo, per $n \geq 4$, la legge

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

con le condizioni iniziali

$$a_1 = 4 \quad a_2 = 22 \quad a_3 = 82$$

[2]Potete verificare che anche la formula data a lezione forniva i "numeri giusti", ovviamente con la traslazione di 1 dell'indice.

Lo stesso ragionamento usato per Fibonacci ci porta a cercare le radici del polinomio $x^3-6x^2+11x-6$. Tali radici (che in generale possiamo cercare in $\mathbb{C}$) si trovano in questo caso molto facilmente e sono 1, 2 e 3; allora tutte le successioni del tipo

$$a\ 1^n + b\ 2^n + c\ 3^n$$

con a, b, c numeri reali qualsiasi soddisfano la legge ricorsiva data. Facendo il sistema di tre equazioni per imporre che valgano le 3 condizioni iniziali si trova che la formula per la successione a_n è, per ogni $n \geq 1$:

$$a_n = -2 \cdot 1^n + (-3) \cdot\ 2^n + 4 \cdot\ 3^n$$

Quindi quando avete di fronte una successione definita per ricorrenza lineare e a coefficienti costanti potete tentare di applicare questo metodo per trovare la formula per il termine ennesimo.
Vi avvertiamo però che, quando cercate le radici del polinomio, possono capitare situazioni che richiedono ulteriori approfondimenti. Per esempio studiamo il caso di una successione che soddisfa, per $n \geq 2$, la legge

$$b_n = 4b_{n-1} - 4b_{n-2}$$

con le condizioni iniziali

$$b_0 = 5 \quad b_1 = 7$$

Il polinomio associato è $x^2 - 4x + 4$ che è $(x-2)^2$ ossia ha come radice 2 "ripetuta due volte" (detto meglio: con molteplicità due). Questo è dunque un caso che prima non avevamo trattato: qui le successioni che si usano sono $\{2^n\}$ e la sua "derivata" $\{n2^{n-1}\}$. Le successioni del tipo

$$a\ 2^n + b\ n2^{n-1}$$

con a, b numeri reali qualsiasi soddisfano tutte la legge ricorsiva data. Facendo il sistema di due equazioni per imporre che valgano le due condizioni iniziali si trova che la formula per la successione b_n è, per ogni $n \geq 0$:

$$b_n = 5 \cdot\ 2^n - 3 \cdot\ n2^{n-1}$$

Certamente, durante l'applicazione di questo metodo, può sorgere una difficoltà, ossia può risultare molto difficile trovare le radici in $\mathbb{C}$ del polinomio associato alla successione. A questo non c'è rimedio, visto che in generale il problema di trovare radici di polinomi è molto difficile; possiamo però garantirvi che negli esercizi che vi proporremo di svolgere in questo corso i polinomi saranno sempre "alla portata".

Per quello che riguarda il sistema finale che mette in gioco le condizioni iniziali, c'è una buona notizia, perché, come imparerete nel corso di Geometria 1, quel tipo di sistemi ha sempre una unica soluzione (la matrice che descrive il sistema è una *matrice di Vandermonde*).

Suggerimento per una ricerca. Il numero $\alpha = \frac{1+\sqrt{5}}{2}$ è il cosiddetto "rapporto aureo", ossia il rapporto fra la lunghezza di un segmento e quella della sua "sezione aurea". Sapete cosa è ?

4. Qualche esercizio...

Esercizio 1.2. Sia $\{u_n\}_{n\in\mathbb{N}}$ la successione così definita:

$$\begin{aligned} u_0 &= 0 \\ u_{k+1} &= 3u_k + 3^k \end{aligned}$$

Dimostrare che $u_k = k3^{k-1}\ \forall\ k \in \mathbb{N}$. [Osservazione: la successione proposta non è "lineare a coefficienti costanti" dunque non si applica il metodo descritto nei paragrafi precedenti]

Esercizio 1.3. Definiamo per ricorrenza $a_0 = 0, a_1 = 12$ e $a_{n+2} = 6a_{n+1} - 9a_n$. Trovare una formula per a_n.

Esercizio 1.4. Consideriamo la successione definita per ricorrenza da $a_0 = 8, a_1 = -1$ e, per ogni numero intero $n \geq 2$, dalla regola:

$$a_n = -a_{n-1} + 2a_{n-2}$$

Trovare un formula per a_n.

Esercizio 1.5. Si definisca una successione tramite la regola $a_0 = 2, a_1 = 1$ e, per ogni $n \geq 1$, $a_{n+1} = a_n + 6a_{n-1}$. Si trovi una formula per il termine a_n.

Esercizio 1.6. Si consideri la successione data da $a_0 = 1$ e $a_{n+1} = 2a_n + 3$.
a) Si dimostri che, per ogni $n \geq 1$, $2^n \mid a_n + 3$.
b) Si trovi una formula per a_n. [Osservazione: la successione proposta non è lineare.]

Esercizio 1.7. Si consideri la successione data da $a_0 = 1$, $a_1 = 1$ e $a_n = a_{n-2} + n$.
a) Trovare, motivando la risposta, il più piccolo numero $n_0 \in \mathbb{N}$ tale che, per ogni $n \geq n_0$, vale $a_n \geq 2n$.
b) Trovare una formula per a_n.

Esercizio 1.8. Sia a_n una successione di numeri interi tale che $a_0 = 1$, $a_{n+1} \geq 2a_n$ se n è pari, e $a_{n+1} \geq 3a_n$ se n è dispari. Dimostrare che per ogni $n \in \mathbb{N}$, $a_{2n} \geq 6^n$.

Esercizio 1.9. Questo problema è ricavato dal *Liber Abaci* (del 1202..) di Fibonacci. "Un uomo mise una coppia di conigli in un luogo circondato da tutti i lati da un muro. Quante coppie di conigli possono essere prodotte dalla coppia iniziale in un anno, supponendo che ogni mese ogni coppia produca una nuova coppia in grado di riprodursi a sua volta dal secondo mese?

Esercizio 1.10. Dato $n \in \mathbb{N} - \{0\}$, sia S_n il numero di tutte le possibili stringhe (cioè liste ordinate) di cifre binarie (ossia 0 e 1) che hanno le seguenti caratteristiche:

- hanno lunghezza n
- se $n = 1$ la stringa è 0, se $n \geq 2$ la lista comincia per 01
- non ci sono mai tre cifre uguali consecutive

Per esempio $S_5 = 5$ e le stringhe in questione sono 01001, 01010, 01011, 01100, 01101. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$, $S_n = F_n$.

Esercizio 1.11. Una lista di numeri interi strettamente crescente si dice *di parità alterna* se inizia con un numero dispari, ha come secondo termine un numero pari, poi il terzo termine è dispari, il quarto è pari, e così via. La lista vuota viene considerata anch'essa una lista di parità alterna. Sia $P(n)$ il numero delle liste di parità alterna i cui termini costituiscono un sottoinsieme di $\{1, 2, \ldots, n\}$. Che relazione c'è fra le successioni $\{P_n\}$ e $\{F_n\}$?

Esercizio 1.12. Provare che per i numeri di Fibonacci F_n $(n \geq 0)$ vale la seguente formula:

$$F_{n+4} = F_3F_n + F_4F_{n+1}$$

Esercizio 1.13. Provare che per i numeri di Fibonacci F_n vale la seguente formula ($n \geq 0$ e $m \geq 1$):

$$F_{n+m} = F_{m-1}F_n + F_mF_{n+1}$$

Esercizio 1.14. Provare che per i numeri di Fibonacci si ha che F_n divide F_{mn} ($n \geq 1$, $m \geq 0$).

Esercizio 1.15. Provare che per i numeri di Fibonacci si ha che $F_{n+4} \geq n^2$ per $n \geq 0$.

Esercizio 1.16. Data la successione $\{a_n\}$ definita da $a_0 = 1$,

$$a_n = 1 + a_0 + a_1 + \cdots + a_{n-1} \qquad \forall n \geq 1$$

trovare una formula per a_n.

Trovare una formula per la successione $\{b_n\}$ definita da $b_0 = 1$,

$$b_n = 1 - b_0 + b_1 - b_2 + \cdots + (-1)^n b_{n-1} \qquad \forall n \geq 1$$

[Osservazione: le successioni proposte non sono lineari.]

CAPITOLO 2

Lezioni del 1 e 2 ottobre

1. La divisione euclidea

Come possiamo distribuire 150 penne fra 70 studenti? Daremo ad ognuno $\frac{150}{70} = 2,142857$ penne? Oppure il problema lo dobbiamo affrontare dicendo che possiamo dare 2 penne ad ogni studente e poi avanza un resto di 10 penne? Questo secondo modo è il più adatto: visto che le penne non si possono "spezzare", il problema era relativo ai numeri interi e deve avere risposta in termini di numeri interi. La divisione che abbiamo fatto, con un quoziente intero (70) e un resto intero (10), è un esempio di "divisione euclidea".

TEOREMA 2.1. *(Teorema della divisione euclidea). Dati a, b interi con $b > 0$ esistono, e sono unici, due interi q (quoziente) ed r (resto), con*

$$a = bq + r \tag{1}$$

$$0 \leq r < b \tag{2}$$

OSSERVAZIONE 2.2. Rimarchiamo subito che uno dei punti qualificanti della definizione della divisione euclidea è la richiesta sul resto, ossia che valga $0 \leq r < b$. Per esempio, volendo distribuire 22 penne fra sette studenti, potrei darne 2 per uno e lasciarne avanzare 8:

$$22 = 7 \cdot 2 + 8$$

Oppure potrei darne tre per uno e avere una sola penna come resto:

$$22 = 7 \cdot 3 + 1$$

Solo quest'ultima è la divisione euclidea di 22 per 7. Infatti 1 soddisfa la condizione $0 \leq 1 < 7$ mentre 8 non soddisfa $0 \leq 8 < 7$. Il teorema che abbiamo enunciato, e che stiamo per dimostrare, dice appunto, a riguardo di questo esempio, che fra le scritture

$$22 = 7a + c$$

con a e c numeri interi, ne esiste una e una sola che è la divisione euclidea di 22 per 7.

OSSERVAZIONE 2.3. Facciamo ancora un altro esempio. Se $a = -15$ e $b = 7$, la divisione euclidea di a per b è:

$$-15 = 7(-3) + 6$$

con quoziente $q = -3$ e resto $r = 6$. L'uguaglianza

$$-15 = 7(-2) - 1$$

per quanto vera, non è la divisione euclidea.

DIMOSTRAZIONE DEL TEOREMA. Consideriamo il caso $a \geq 0$ (se $a < 0$ la dimostrazione è analoga). Possiamo utilizzare il principio del minimo. Consideriamo l'insieme

$$Q = \{m \in \mathbb{N} \mid mb \geq a\}$$

Tale insieme è un sottoinsieme di $\mathbb{N}$ non vuoto (visto che $b > 0$ e dunque $b \geq 1$, Q contiene infiniti interi maggiori di a). Per il principio del minimo Q ammette un minimo, appunto, che chiameremo q. Ora, se $qb = a$ abbiamo già trovato la nostra divisione euclidea:

$$a = bq + 0$$

Se invece $qb > a$ allora deve valere $(q-1)b < a$, altrimenti il minimo di Q sarebbe $q-1$ e non q. La differenza $r = a - (q-1)b$ soddisfa $0 < r < b$ e dunque la divisione euclidea che cercavamo è

$$a = (q-1)b + r$$

Il procedimento che abbiamo seguito dimostra in realtà anche l'unicità del quoziente e del resto. Per una qualunque altra scelta del quoziente diversa da q, infatti, si osserva facilmente che il resto ottenuto non soddisferebbe la richiesta $0 \leq r < b$. □

Esempio 2.4. Concretamente, il quoziente può essere calcolato come $\lfloor a/b \rfloor$, dove il simbolo $\lfloor a/b \rfloor$ indica la *parte intera* di a/b, ossia il più grande intero che è $\leq a/b$.

Per esempio: $a = 1781293$, $b = 1481$, $a/b \approx 1202.7637$, $q = 1202 = \lfloor a/b \rfloor$, $r = 1781293 - 1481 \cdot 1202 = 1131$.

Oppure $a = -7856123$, $b = 9812$, $a/b \approx -800.66840$, $q = -801 = \lfloor a/b \rfloor$, $r = -7856123 - 9812 \cdot (-801) = 3289$.

2. Il massimo comun divisore e l'algoritmo di Euclide

Notazione. Ricordiamo che, dati due numeri interi c e d, diciamo che c divide d se esiste un numero intero k tale che $ck = d$. In tal caso scriviamo $c \mid d$.

Definizione 2.5. Siano $a, b \in \mathbb{Z}$, con almeno uno dei due diverso da 0 (questo si può scrivere così: $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0,0)\}$). Allora il "massimo comun(e) divisore" di a e b è l'unico intero positivo d tale che:

- $d|a$ e $d|b$;
- d è più grande di ogni altro divisore comune di a e b: se $c|a$ e $c|b$, allora deve essere $c \leq d$.

Indicheremo il massimo comun divisore di a e b come $MCD(a, b)$ (talvolta, quando è chiaro che stiamo considerando il massimo comun divisore, ometteremo MCD e scriveremo soltanto (a, b)). Se vale che $MCD(a, b) = 1$ diremo che a e b sono *primi tra loro* o *coprimi*.

Osservazione 2.6. La definizione è ben posta. Infatti almeno un divisore comune positivo di a e b esiste sempre (il numero 1) e dunque l'insieme di tutti i divisori comuni positivi è un sottoinsieme di $\mathbb{N}$ non vuoto e finito (si noti a questo proposito che i suoi elementi sono tutti minori o uguali al minimo fra $|a|$ e $|b|$). Allora esiste unico il massimo di tale insieme, che è appunto il $MCD(a, b)$.

Osserviamo subito che:

$$MCD(a, b) = MCD(b, a) = MCD(|a|, |b|)$$

e anche che:

$$MCD(a, a) = MCD(a, 0) = |a|$$

Calcoliamo per esercizio qualche massimo comun divisore:

$MCD(9, 0) = 9$	$MCD(-5, 0) = 5$	$MCD(-8, -12) = 4$
$MCD(9, 54) = 9$	$MCD(-9, 54) = 9$	$MCD(45, 34) = 1$
$MCD(3, 100) = 1$	$MCD(10, 2^8) = 2$	$MCD(-1, 1) = 1$
$MCD(1, 100) = 1$	$MCD(1, 0) = 1$	$MCD(12, -12) = 12$

Da questi esempi risulta che 45 e 34 sono coprimi, come -1 e 1, 3 e 100, 1 e 100, e anche 1 e 0.

Fin dalle scuole medie conoscete un metodo per calcolare il massimo comuni divisore $MCD(a, b)$ di due numeri interi $a \geq 1$ e $b \geq 1$ di cui conoscete la fattorizzazione in prodotto di primi.

Infatti $MCD(a, b)$ è uguale a 1 se non ci sono primi che compaiono in entrambe le fattorizzazioni; se invece ci sono primi che compaiono in entrambe le fattorizzazioni, $MCD(a, b)$ è uguale al prodotto di tali primi, dove ciascuno di essi è preso con l'esponente minimo con cui compare.
Per esempio, se

$$a = 2^5 \cdot 3^4 \quad \text{e} \quad b = 5 \cdot 7 \cdot 17^3$$

allora

$$MCD(a, b) = 1$$

e se invece

$$a = 2^5 \cdot 3^4 \cdot 7^2 \cdot 11^3 \quad \text{e} \quad b = 2^4 \cdot 3^8 \cdot 5 \cdot 7 \cdot 17^3$$

allora

$$MCD(a, b) = 2^4 \cdot 3^4 \cdot 7$$

Dobbiamo fare adesso due importanti precisazioni su questo metodo.

- La prima è che questo metodo è veloce ed efficiente solo se conosciamo già la fattorizzazione in primi dei due numeri. Ma bisogna tenere conto del fatto che in generale il problema di trovare la fattorizzazione in primi di un numero dato è molto difficile (specialmente se il numero è molto grande), e anzi su questa difficoltà si basa uno dei metodi più efficienti di crittografia usato in questi anni, come vedremo più avanti.[1]
- La seconda è che questo metodo funziona perché la fattorizzazione in prodotto di primi di un numero è essenzialmente *unica*. Questa è una proprietà ben nota, ma che in realtà probabilmente non avete mai dimostrato. Noi la dimostreremo fra poche lezioni. Fino a che non la abbiamo dimostrata, dunque, dovete considerare il metodo esposto sopra "in attesa di spiegazione". Alla fine di tutto il percorso avrete una visione più profonda di questo aspetto dell'aritmetica.

Messo dunque per ora da parte il metodo che passa attraverso la fattorizzazione, il nostro obiettivo è quello di discutere un altro metodo per calcolare il massimo comun divisore, l'*algoritmo di Euclide*. Si tratta in realtà di un metodo molto più rapido ed efficiente del precedente e che oltretutto avrà il merito di aprire la strada ad un risultato fondamentale in aritmetica, il Lemma di Bezout.

Cominciamo con ordine, e descriviamo l'algoritmo di Euclide: supponiamo di voler trovare il MCD di due numeri $a, b \in \mathbb{Z}$ non entrambi nulli. Se uno dei due numeri (per esempio a) è 0, allora sappiamo subito dire che $MCD(0, b)$ è uguale al valore assoluto $|b|$ di b.

Occupiamoci dunque del caso in cui entrambi i numeri sono diversi da zero. Se vale per esempio che $|a| \geq |b| > 0$ applichiamo l'algoritmo direttamente al calcolo di $MCD(|a|, |b|)$. Cominciamo con la divisione euclidea di $|a|$ per $|b|$:

$$|a| = |b|q + r_1 \quad \text{con} \quad 0 \leq r_1 < |b|$$

[1] Per dare un'idea della scala di grandezza a cui si riferisce il nostro discorso, anticipiamo fin d'ora che il metodo di crittografia RSA si basa sul fatto che, attualmente, non sia possibile fattorizzare "in tempo utile" un numero di 600 cifre che è il prodotto di due primi.

Se $r_1 = 0$ abbiamo finito, perché possiamo concludere subito che $|b| = MCD(|a|, |b|) = MCD(a, b)$. Altrimenti proseguiamo con delle divisioni euclidee successive finché non si trova un resto uguale a 0:

$$\begin{gathered}
|a| = |b|q + r_1 \quad \text{con} \quad 0 < r_1 < |b| \\
|b| = r_1 \cdot q_1 + r_2 \quad \text{con} \quad 0 < r_2 < r_1 \\
r_1 = r_2 q_2 + r_3 \quad \text{con} \quad 0 < r_3 < r_2 \\
\cdots\cdots\cdots \\
r_{n-2} = r_{n-1} q_{n-1} + r_n \quad \text{con} \quad 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_n + 0
\end{gathered}$$

A questo punto concludiamo che $r_n = MCD(|a|, |b|) = MCD(a, b)$.

Per dimostrare che il metodo dell'algoritmo funziona, dobbiamo rispondere a due domande.

- Perché l'algoritmo termina sempre entro un numero finito di passi? Perché ad ogni passo otteniamo un resto r_j che è un numero naturale ed è strettamente minore del resto precedente. Se potessimo continuare all'infinito, l'insieme dei resti contraddirebbe il principio del minimo (sarebbe un sottoinsieme di $\mathbb{N}$ non vuoto senza minimo..).

- Perché r_n è proprio il MCD che cercavamo? Il punto cruciale, è dato dal seguente:

  TEOREMA 2.7. *Dati $a, b, c, d \in \mathbb{Z}$ con almeno uno fra a, b non nullo e almeno uno fra b, d non nullo, che soddisfano*

  $$a = bc + d$$

  allora vale che $MCD(a, b) = MCD(b, d)$.

  DIMOSTRAZIONE. La strategia è la seguente: mostreremo che l'insieme $DIV(a, b)$ dei divisori comuni positivi di a e b è uguale all'insieme $DIV(b, d)$ dei divisori comuni positivi di b e d. A quel punto avremo finito, perché $MCD(a, b)$ è il massimo elemento di $DIV(a, b)$ e $MCD(b, d)$ è il massimo elemento di $DIV(b, d)$, ossia...dello stesso insieme.

  Dimostriamo dunque che $DIV(a, b) \subseteq DIV(b, d)$ (l'inclusione opposta si dimostra in maniera analoga). Prendiamo un elemento $\gamma \in DIV(a, b)$. Visto che $\gamma | a$ e $\gamma | b$ allora γ divide anche $a - bc$ ovvero γ divide d. Dunque $\gamma \in DIV(b, d)$, come volevamo dimostrare.

  □

  Applicando questo lemma ai vari passaggi del nostro algoritmo di Euclide otteniamo:

  $$MCD(|a|, |b|) = MCD(|b|, r_1) = MCD(r_1, r_2) = MCD(r_2, r_3) = \ldots$$

  e così via (questo "così via" nasconde una facile induzione!) fino a

  $$\ldots = MCD(r_{n-2}, r_{n-1}) = MCD(r_{n-1}, r_n)$$

  Ma $MCD(r_{n-1}, r_n)$ è proprio r_n, visto che $r_n | r_{n-1}$. Ripercorrendo tutta la catena di uguaglianze scopriamo di aver dimostrato che

  $$MCD(|a|, |b|) = r_n$$

e dunque ora sappiamo perché l'algoritmo di Euclide funziona!

3. Una stima del numero di passi necessario per portare a termine l'algoritmo di Euclide

Come abbiamo anticipato, l'algoritmo di Euclide ha una grande importanza non solo sul piano teorico, ma anche su quello computazionale. Vogliamo allora trovare una stima del numero di passi necessario per terminare l'algoritmo.

Riferiamoci dunque all'algoritmo per trovare il $MCD(|a|,|b|)$ ($|a| \geq |b| \geq 1$) illustrato nel paragrafo precedente. Supponiamo che $a \geq b \geq 1 > 0$, per liberarci dei valori assoluti, che appesantiscono la notazione. Chiamiamo poi $b = r_0$, così da poter affermare che, se il massimo comun divisore risulta essere r_n, abbiamo dovuto fare $n+1$ divisioni euclidee per concludere l'algoritmo. Cerchiamo dunque di stimare il numero di passi $n+1$, in funzione dei dati iniziali (che sono a e b).

Per prima cosa osserviamo che $b = r_0 > 2r_2$, infatti $r_0 = r_1 q_1 + r_2 \geq r_1 + r_2 > r_2 + r_2$.

Allo stesso modo $r_2 > 2r_4$ e così via..., per induzione si mostra che $r_{k-2} > 2r_k$ per ogni $2 \leq k \leq n$. Dunque, se n è pari, $b > 2^{\frac{n}{2}} r_n > 2^{\frac{n}{2}}$. Se invece n è dispari, $b > 2^{\frac{n-1}{2}} r_{n-1} > 2^{\frac{n}{2}}$, visto che $r_{n-1} \geq 2$ (infatti $r_{n-1} > r_n \geq 1$). In entrambi i casi, comunque, possiamo dire che $b > 2^{\frac{n}{2}}$.

Allora $\log_2 b > \frac{n}{2}$, quindi $2\log_2 b > n$, da cui otteniamo

$$n + 1 < 2\log_2 b + 1$$

Questa che abbiamo appena ottenuto è una prima stima.

Il matematico francese Lamé nell'ottocento aveva ottenuto una stima, sempre legata al *logaritmo* di b, ma con una costante migliore. Vediamo come. Cominciamo col chiederci quali sono gli a e b più piccoli che generano un algoritmo di Euclide con $n+1$ divisioni. Se $n = 0$, la risposta è $a = b = 1$; se invece $n > 0$ otterremo gli a e b minimi percorrendo l'algoritmo alla rovescia e chiedendo che r_n, l'ultimo resto non zero, e $q_1, q_2, \ldots, q_{n-1}, q_n$ siano più piccoli possibile.

Quindi partiamo da $r_n = 1$; osserviamo poi che q_n deve essere ≥ 2 visto che $r_{n-1} = r_n q_n$ e $r_{n-1} > r_n$. Dunque il q_n più piccolo possibile è $q_n = 2$ e di conseguenza abbiamo $r_{n-1} = 2$. A questo punto $r_{n-2} = 2q_{n-1} + 1 \geq 2 + 1 = 3$. Continuando a percorrere alla rovescia l'algoritmo, abbiamo $r_{n-3} = r_{n-2}q_{n-2} + r_{n-1} \geq 3q_{n-2} + 2 \geq 3 + 2 = 5$. Al passo successivo otterremo $r_{n-4} \geq 5 + 3 = 8$...e così via. Scegliendo $q_1 = q_2 = \cdots = q_{n-1} = 1$ otteniamo proprio gli r_j minimi, ossia $r_{n-2} = 3$, $r_{n-3} = 5$, $r_{n-4} = 8$...

Sono apparsi i numeri di Fibonacci. !!!!

Nel nostro ragionamento abbiamo ottenuto come resti minimi $r_n = 1 = F_2$, $r_{n-1} = 2 = F_3$, $r_{n-2} = 3 = F_4$, $r_{n-3} = 5 = F_5$ e $r_{n-4} = 8 = F_6$. Come avete capito, si può facilmente dimostrare per induzione che $r_{n-j} \geq F_{j+2}$ e che con le scelte minime possibili di r_n e dei q_j risulta $r_{n-j} = F_{j+2}$.

Dunque b che, nelle nostre notazioni, è r_0, risulta sempre maggiore o uguale a F_{n+2}, e con le scelte minime possibili di r_n e dei q_j risulta esattamente uguale a F_{n+2}.

Inoltre nel caso minimo possibile le informazioni $r_1 = F_{n+1}$ e $b = F_{n+2}$ implicano che $a = F_{n+3}$, ossia, ricapitolando, abbiamo scoperto che l'algoritmo di Euclide per la coppia (F_{n+3}, F_{n+2}) richiede esattamente $n+1$ passi e che fra tutti gli algoritmi di Euclide lunghi $n+1$ passi è 'minimo', in questo senso: se l'algoritmo per la coppia (a, b) ha $n+1$ passi allora vale che $a \geq F_{n+3}$ e $b \geq F_{n+2}$.

Utilizzeremo adesso la formula non ricorsiva per i numeri di Fibonacci data dal Teorema 1.1: per ogni $n \geq 0$ vale

$$F_{n+2} = \frac{\alpha^{n+2} - \beta^{n+2}}{\sqrt{5}},$$

dove $\alpha = \frac{1+\sqrt{5}}{2} \cong 1,618$ e $\beta = \frac{1-\sqrt{5}}{2} \cong -0,618$ sono le due soluzioni dell'equazione $x^2 - x - 1 = 0$. Possiamo usare questa formula per stimare F_{n+2} dimostrando che $F_{n+2} \geq \alpha^n$.

Infatti

$$F_{n+2} = \frac{\alpha^{n+2} - \beta^{n+2}}{\sqrt{5}} \geq \alpha^n$$

equivale a:

$$\alpha^2 - \left(\frac{\beta}{\alpha}\right)^n \beta^2 \geq \sqrt{5}.$$

Per $n = 0$ si tratta di una uguaglianza. Per $n \geq 1$, dai valori approssimati scritti sopra deduciamo che certamente $|\frac{\beta}{\alpha}| < \frac{1}{2}$, quindi, sia che n sia pari sia che sia dispari,

$$\alpha^2 - \left(\frac{\beta}{\alpha}\right)^n \beta^2 > \alpha^2 - \frac{1}{2}\beta^2.$$

Adesso, anche senza sviluppare ulteriormente il calcolo, possiamo verificare direttamente che $\alpha^2 - \frac{1}{2}\beta^2 > \sqrt{5}$ (resistete alla tentazione di usare la calcolatrice, in realtà per questo conto non serve!).

In conclusione abbiamo scoperto che $b \geq F_{n+2} \geq \alpha^n$. Allora, passando ai logaritmi, abbiamo $n \leq \log_\alpha b$ e quindi $n + 1 \leq \log_\alpha b + 1$.

È una stima migliore della precedente; chi vuole ottenerne una senza il logaritmo in base α, può osservare che $log_\alpha b = \frac{1}{\log_b \alpha}$ oppure, a costo di peggiorare un pochino la stima, può utilizzare la disuguaglianza $\log_{10} \alpha > \frac{1}{5}$ (verificatela, stavolta anche con la calcolatrice). Infatti da $n \leq \log_\alpha b$ si ottiene, moltiplicando a sinistra per $\frac{1}{5}$ e a destra per $\log_{10} \alpha$, la nuova disuguaglianza $\frac{n}{5} < \log_{10} \alpha \log_\alpha b = \log_{10} b$, dove abbiamo usato le proprietà elementari del cambio di base nei logaritmi. Riassumiamo questo risultato nell'enunciato del seguente:

Teorema 2.8. *Dato un algoritmo di Euclide per trovare $MCD(a, b)$ con $a \geq b \geq 1$, che richiede $n + 1$ divisioni euclidee, vale*

$$n + 1 < 5 \log_{10} b + 1$$

Questa stima è migliore di quella che avevamo ricavato all'inizio del paragrafo, in cui compare $2 \log_2 b$, perchè $5 \log_{10} b = 5 \log_{10} 2 \log_2 b$, quindi tutto si riduce a controllare se $5 \log_{10} 2 = \log_{10} 2^5$ è minore di 2...e la verifica è immediata.

Dalla stima $n + 1 < 5 \log_{10} b + 1$ se ne può ottenere un'altra in cui entra in gioco il numero delle cifre di b (nella scrittura decimale). Infatti il numero di cifre che si usano per scrivere un numero intero positivo b in base 10 è uguale a $\lfloor \log_{10} b \rfloor + 1$ dove $\lfloor x \rfloor$ indica, come abbiamo già visto, la parte intera di x, insomma il più grande numero intero che è minore o uguale a x.

Allora da $n + 1 < 5 \log_{10} b + 1$ possiamo ottenere

$$n + 1 < 5 \log_{10} b + 1 < 5(\lfloor \log_{10} b \rfloor + 1) + 1$$

Abbiamo insomma, come corollario del Teorema 2.8, ancora una nuova stima:

Corollario 2.9. *Dato un algoritmo di Euclide per trovare $MCD(a, b)$ con $a \geq b \geq 1$, che richiede $n + 1$ divisioni euclidee, vale*

$$n + 1 \leq 5 \; cifre(b)$$

dove $cifre(b)$ indica il numero delle cifre di b scritto in notazione decimale.

4. L'Identità di Bezout

Vogliamo ora mettere in luce una proprietà del massimo comune divisore che giocherà un ruolo fondamentale in tutta la nostra introduzione all'aritmetica: il massimo comun divisore di due numeri a e b è il più piccolo intero positivo che può essere ottenuto quando consideriamo le espressioni del tipo $ax + by$ al variare di x e y fra i numeri interi.

TEOREMA 2.10 (Identità di Bezout o Lemma di Bezout[2]). *Dati due numeri interi a e b con $(a, b) \neq (0, 0)$, esistono due numeri interi m e n tali che*

$$MCD(a, b) = am + bn$$

Si dice che $MCD(a, b)$ può essere espresso come combinazione lineare a coefficienti interi di a e di b.

OSSERVAZIONE 2.11. Il teorema dice che esistono m ed n tali che $MCD(a, b) = am + bn$, ma non dice che sono unici. Infatti, come risulterà dalla teoria delle equazioni diofantee lineari, ci sono infinite scelte possibili di una coppia (m, n) tale che $MCD(a, b) = am + bn$.

DIMOSTRAZIONE. Consideriamo l'insieme $CL^+(a, b)$ di tutte le possibili combinazioni lineari **positive** a coefficienti interi di a e b, ossia

$$CL^+(a, b) = \{ar + bs \mid r \in \mathbb{Z},\ s \in \mathbb{Z},\ ar + bs > 0\}$$

Tale insieme è non vuoto. Infatti supponiamo che $a \neq 0$ (altrimenti si fa lo stesso ragionamento con b). Allora si trovano degli elementi dell'insieme $CL^+(a, b)$ per esempio scegliendo $s = 0$ e r tale che $ra > 0$. Già così abbiamo esibito infiniti elementi nell'insieme $CL^+(a, b)$.

Inoltre $CL^+(a, b) \subseteq \mathbb{N}$. Dunque, per il principio del buon ordinamento, $CL^+(a, b)$ ammette minimo.

Sia d tale minimo: in particolare, dato che $d \in CL^+(a, b)$, esistono un $m \in \mathbb{Z}$ ed un $n \in \mathbb{Z}$ tali che

$$d = am + bn$$

La dimostrazione del teorema si conclude ora mostrando che $d = MCD(a, b)$. Infatti d soddisfa le proprietà del massimo comune divisore, ossia:

- $d|a$ e $d|b$
- se $c|a$ e $c|b$ allora $c \leq d$

Per il primo punto, facciamo la divisione euclidea fra a e d. Sarà $a = qd + r$ con $0 \leq r < d$.

Allora

$$a = q(am + bn) + r$$

da cui

$$r = (-qm + 1)a + (-qn)b$$

Ma allora r si esprime come combinazione lineare a coefficienti interi di a e di b. Se fosse $r > 0$ avremmo che $r \in CL^+(a, b)$ per definizione di $CL^+(a, b)$. Questo non può succedere perché $0 \leq r < d$ e d era stato scelto come **minimo** elemento di $CL^+(a, b)$.

Dunque deve essere $r = 0$. Questo vuol dire che $a = qd + 0$, ossia che $d|a$. Allo stesso modo si dimostra che $d|b$.

Il secondo punto è immediato. Infatti se $c|a$ e $c|b$ allora $c|am+bn$ cioè $c|d$, in particolare $c \leq d$.

[2]Prende il nome dal matematico francese Etienne Bezout, 1730-1783.

□

COROLLARIO 2.12. *Dati due numeri interi a e b con $(a,b) \neq (0,0)$, se $c|a$ e $c|b$, allora non solo $c \leq MCD(a,b)$ ma più precisamente vale che $c|MCD(a,b)$.*

Riguardando la dimostrazione del teorema, ci accorgiamo che abbiamo dimostrato il risultato annunciato all'inizio del paragrafo (che è un po' più forte di quello nell'enunciato del teorema):

TEOREMA 2.13. *Dati due numeri interi a e b con $(a,b) \neq (0,0)$, $MCD(a,b)$ è il più piccolo numero intero positivo ottenibile come combinazione lineare intera di a e di b.*

Sottolineiamo che se dividiamo due numeri per il loro massimo comun divisore, i due quozienti ottenuti sono primi fra loro:

COROLLARIO 2.14. *Presi due numeri interi a e b non entrambi nulli, se li dividiamo per il loro massimo comun divisore $MCD(a,b)$ otteniamo due numeri*

$$a' = \frac{a}{MCD(a,b)} \qquad b' = \frac{b}{MCD(a,b)}$$

che sono primi fra loro.

DIMOSTRAZIONE. Si può vedere in due modi, entrambi molto semplici. Il primo modo è il seguente: se ci fosse un divisore comune $d > 1$ di a' e b', allora $d \cdot MCD(a,b)$ dividerebbe sia a sia b e sarebbe più grande di $MCD(a,b)$, assurdo.

Il secondo parte dall'identità di Bezout

$$MCD(a,b) = am + bn$$

Dividendo per $MCD(a,b)$ si ottiene

$$1 = a'm + b'n$$

e dunque 1 è il più piccolo numero intero positivo ottenibile come combinazione lineare intera di a' e di b'.

□

Concludiamo con una osservazione aritmetica importante, nella cui dimostrazione l'Identità di Bezout gioca un ruolo fondamentale:

TEOREMA 2.15. *Siano $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $MCD(a,b) = 1$ allora $a \mid c$.*

DIMOSTRAZIONE. Visto che $MCD(a,b) = 1$ allora per l'Identità di Bezout possiamo trovare $m, n \in \mathbb{Z}$ tali che

$$1 = an + bm$$

Moltiplicando entrambi i membri per c otteniamo:

$$c = acn + bcm$$

Questo ci permette di concludere che $a \mid c$. Infatti $a \mid acn$ (ovviamente) e $a \mid bcm$ (visto che $a \mid bc$ per ipotesi), dunque a divide la somma $acn + bcm$ che è uguale a c.

□

OSSERVAZIONE 2.16. La dimostrazione precedente è breve ma non è banale. **Il Teorema 2.15 è alla base del fatto che la fattorizzazione in prodotto di primi di un numero intero è unica**, come vedremo in seguito.

5. Un metodo costruttivo per ottenere l'Identità di Bezout

Dati due numeri interi non entrambi nulli a e b, l'Identità di Bezout, come abbiamo visto nel Paragrafo 4, ci dice che è possibile trovare due numeri interi m e n tali che

$$MCD(a, b) = am + bn$$

Ma la dimostrazione che abbiamo proposto in quel paragrafo non ci dà un metodo concreto per trovare un m e un n che soddisfino l'uguaglianza scritta sopra. In questo paragrafo colmeremo questa lacuna, descrivendo un metodo che si basa sull'algoritmo di Euclide, utilizzato due volte, nel modo usuale e "a rovescio".

Prendiamo per esempio $a = 1020$ e $b = 351$ e calcoliamo $MCD(a, b)$ tramite l'algoritmo di Euclide:

$$\begin{aligned}
1020 &= 351 \cdot 2 + 318 \\
351 &= 318 \cdot 1 + 33 \\
318 &= 33 \cdot 9 + 21 \\
33 &= 21 \cdot 1 + 12 \\
21 &= 12 \cdot 1 + 9 \\
12 &= 9 \cdot 1 + 3 \\
9 &= 3 \cdot 3 + 0
\end{aligned}$$

Dunque abbiamo trovato che $MCD(1020, 351) = 3$. Scriviamo adesso di nuovo tutte le equazioni dell'algoritmo (tranne l'ultima) ponendo a sinistra i resti:

$$\begin{aligned}
318 &= 1020 - 351 \cdot 2 \\
33 &= 351 - 318 \cdot 1 \\
21 &= 318 - 33 \cdot 9 \\
12 &= 33 - 21 \cdot 1 \\
9 &= 21 - 12 \cdot 1 \\
3 &= 12 - 9 \cdot 1
\end{aligned}$$

Ora ripercorriamo l'algoritmo "a rovescio": cominciamo da $3 = 12 - 9 \cdot 1$. Ricordiamo che come obiettivo finale vogliamo trasformare questa equazione in una del tipo

$$3 = 1020m + 351n$$

Cominciamo utilizzando l'equazione $9 = 21 - 12 \cdot 1$. Possiamo usarla per sostituire il 9 ed ottenere 3 espresso come combinazione lineare di 12 e di 21:

$$3 = 12 - 9 \cdot 1 = 12 - (21 - 12 \cdot 1) \cdot 1 = 12 \cdot 2 - 21$$

A questo punto facciamo entrare in gioco l'equazione $12 = 33 - 21 \cdot 1$. La utilizziamo per sostituire il 12 ed ottenere 3 come combinazione lineare di 33 e di 21:

$$3 = 12 \cdot 2 - 21 = (33 - 21 \cdot 1) \cdot 2 - 21 = 33 \cdot 2 - 21 \cdot 3$$

Continuando,

$$3 = 33 \cdot 2 - 21 \cdot 3 = 33 \cdot 2 - (318 - 33 \cdot 9) \cdot 3 = 33 \cdot 29 - 318 \cdot 3 =$$

$$= 33 \cdot 29 - 318 \cdot 3 = (351 - 318 \cdot 1) \cdot 29 - 318 \cdot 3 = 351 \cdot 29 - 318 \cdot 32$$

Infine, chiamando in causa $318 = 1020 - 351 \cdot 2$:

$$3 = 351 \cdot 29 - 318 \cdot 32 = 351 \cdot 29 - (1020 - 351 \cdot 2) \cdot 32 = 1020(-32) + 351 \cdot 93$$

Abbiamo dunque trovato $m = -32$ e $n = 93$:

$$3 = 1020(-32) + 351 \cdot 93$$

Osservazione 2.17. Come abbiamo già preannunciato, quando parleremo di equazioni diofantee mostreremo che questa è solo una delle infinite possibili coppie (m, n) che soddisfano l'identità di Bezout

$$3 = 1020m + 351n$$

Anche se si tratta solo di un esempio, non è difficile intuire che il metodo funziona sempre, per ogni a e b di cui è possibile calcolare il massimo comun divisore. Questa è dunque un'altra possibile via di dimostrazione dell'identità di Bezout (radicalmente diversa dall'altra, che era "esistenziale": questa la potremmo chiamare "costruttiva", visto che fornisce un algoritmo concreto per trovare i numeri m e n).

Lasciamo per esercizio (vedi Esercizio 2.24) i dettagli di questa dimostrazione (che può essere svolta per induzione sul numero di passi che occorrono per concludere l'algoritmo di Euclide).

Un metodo "compatto" per organizzare il calcolo viene illustrato nell'esempio seguente:

Esempio 2.18. Calcolare $MCD(252, 198)$ e trovare x, y interi tali che $MCD(252, 198) = 252x + 198y$.

Per prima cosa calcoliamo $MCD(252, 198)$.

$$\begin{gathered} 252 = 198 \cdot 1 + 54 \\ 198 = 54 \cdot 3 + 36 \\ 54 = 36 \cdot 1 + 18 \\ 36 = 18 \cdot 2 + 0 \end{gathered}$$

Dunque $MCD(252, 198) = 18$. Scriviamo ora:

$$\begin{array}{rcccccc} & & 252 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{0} \\ & & 198 & = & 252 \cdot \boxed{0} & + & 198 \cdot \boxed{1} \\ 252 - 198 & = & 54 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{(-1)} \\ 198 - 54 \cdot 3 & = & 36 & = & 252 \cdot \boxed{(-3)} & + & 198 \cdot \boxed{4} \\ 54 - 36 & = & 18 & = & 252 \cdot \boxed{4} & + & 198 \cdot \boxed{(-5)} \end{array}$$

Nella colonna centrale abbiamo scritto (dall'alto) 252, 198 e poi i resti ottenuti con l'algoritmo di Euclide. Di ognuno di questi numeri, nella colonna di destra è indicato come si può ottenere come combinazione di 252 e 198[3]. Dunque il risultato finale si legge dall'ultima riga ed è $x = 4, y = -5$.

6. Le equazioni diofantee

Una equazione del tipo

$$ax + by = c$$

dove a, b, c sono numeri interi e x, y sono le variabili, si chiama equazione diofantea.[4]

Risolverla vuol dire trovare una coppia di numeri interi $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ tali che

$$a\overline{x} + b\overline{y} = c$$

[3]Per passare dalla combinazione della terza riga a quella della quarta, per esempio, visto che $36 = 198 - 54 \cdot 3$, abbiamo sommato la combinazione della seconda riga a quella della terza moltiplicata per -3. Questo si traduce in modo rapido facendo la corrispondente operazione sui numeri incorniciati

[4]Il nome deriva da Diofanto di Alessandria, III-IV secolo d.C.

In questo paragrafo studieremo un criterio per decidere se una equazione diofantea ammette soluzione e, nel caso in cui la ammetta, descriveremo un metodo per trovare tutte le sue soluzioni.

Per prima cosa studiamo a parte il caso in cui $a = 0, b = 0$. L'equazione

$$0x + 0y = c$$

ha soluzione se e solo se anche $c = 0$ e in tal caso le sue soluzioni sono infinite, precisamente tutte le possibili coppie $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$.

Rimane da studiare il caso in cui a e b siano non siano entrambi nulli.

TEOREMA 2.19. *L'equazione diofantea*

$$ax + by = c \tag{2.1}$$

(con a e b non entrambi nulli) ha soluzione se e solo se $MCD(a, b)$ divide c.

DIMOSTRAZIONE. Viene in nostro aiuto l'Identità di Bezout. Il Teorema 2.10 ci dice infatti che certamente l'equazione diofantea

$$ax + by = MCD(a, b) \tag{2.2}$$

ammette soluzione.

Ma l'equazione che dobbiamo risolvere differisce da questa perché nel membro di destra c'è c invece di $MCD(a, b)$.

Allora tutta la nostra strategia si gioca su questa domanda: $MCD(a, b)$ divide o non divide il numero c?

Se la risposta è sì, ossia $c = MCD(a, b)\ k$ per un certo numero intero k, allora l'equazione (2.1) ammette soluzione. Infatti si parte da una coppia di numeri interi (m, n) che risolve l'equazione (2.2):

$$am + bn = MCD(a, b)$$

e si moltiplicano entrambi i membri per k. Troviamo allora:

$$a(mk) + b(nk) = MCD(a, b) \cdot k = c$$

dunque, (mk, nk) è una soluzione dell'equazione (2.1).

Viceversa, se la risposta è no, ossia $MCD(a, b)$ non divide c, allora l'equazione (2.1) non può avere soluzione e lo possiamo dimostrare per assurdo. Se infatti ammettesse una soluzione (chiamiamola $(\overline{x}, \overline{y})$) considerando l'uguaglianza

$$a\overline{x} + b\overline{y} = c$$

ricaveremmo che, visto che $MCD(a, b)$ divide il membro di sinistra (essendo un divisore sia di a che di b), allora $MCD(a, b)$ deve dividere il membro di destra, ossia c. Questo è assurdo perché eravamo proprio nel caso in cui $MCD(a, b)$ non divide c.

□

Studiamo meglio il caso in cui l'equazione diofantea (2.1) ha soluzione. In questo caso la soluzione sarà una sola o possiamo trovarne più di una?

Per rispondere, prendiamo in considerazione un'altra equazione, "più semplice" della (2.1):

$$ax + by = 0$$

Come vedete, abbiamo sostituito c con 0. Questa si chiama *l'equazione omogenea associata* alla (2.1).

La sua importanza è legata a questa osservazione: se $(\overline{x}, \overline{y})$ è una soluzione di (2.1) e (γ, δ) è una soluzione della equazione omogenea associata, allora $(\overline{x} + \gamma, \overline{y} + \delta)$ è ancora

una soluzione di (2.1). Lo potete subito verificare sommando membro a membro le due uguaglianze:

$$a\overline{x} + b\overline{y} = c$$

$$a\gamma + b\delta = 0$$

Abbiamo trovato un modo per generare altre soluzioni di (2.1), a partire da una soluzione $(\overline{x}, \overline{y})$ data. Ma quante sono le soluzioni della equazione omogenea associata? Troviamole: riscriviamo

$$ax + by = 0$$

come

$$ax = -by$$

Possiamo dividere entrambi i membri per $MCD(a, b)$:

$$\frac{a}{MCD(a,b)}\ x = -\frac{b}{MCD(a,b)}\ y$$

Questa equazione è equivalente a quella iniziale. Supponiamo di avere una soluzione (γ, δ):

$$\frac{a}{MCD(a,b)}\ \gamma = -\frac{b}{MCD(a,b)}\ \delta$$

A questo punto, visto che i due numeri $\frac{a}{MCD(a,b)}$ e $\frac{b}{MCD(a,b)}$ sono primi fra loro (vedi il Corollario 2.14), il Teorema 2.15 ci dice che $\frac{a}{MCD(a,b)}$ deve dividere δ. Allora δ è della forma $\frac{a}{MCD(a,b)}\ t$ e γ risulta uguale a $-\frac{b}{MCD(a,b)}\ t$.

Viceversa si nota subito che una qualunque coppia della forma

$$(-\frac{b}{MCD(a,b)}\ t, \frac{a}{MCD(a,b)}\ t)$$

con $t \in \mathbb{Z}$ è una soluzione della equazione omogenea associata. Abbiamo dunque trovato TUTTE le soluzioni della equazione omogenea associata, e notiamo che sono infinite!

Saranno dunque infinite anche le soluzioni della equazione diofantea iniziale (2.1). Il seguente teorema afferma che, con le argomentazioni appena esposte, abbiamo in realtà trovato tutte le soluzioni di (2.1):

Teorema 2.20. *Se l'equazione diofantea (2.1) ammette soluzione, allora ammette infinite soluzioni. Presa una soluzione particolare $(\overline{x}, \overline{y})$, l'insieme $\mathcal{S}$ di tutte le soluzioni può essere descritto così:*

$$\mathcal{S} = \{(\overline{x} + \gamma, \overline{y} + \delta) \mid (\gamma, \delta) \ \textit{è soluzione dell'equazione omogenea associata}\}$$

Dimostrazione. Le argomentazioni esposte poco sopra dimostrano che

$$\{(\overline{x} + \gamma, \overline{y} + \delta) \mid (\gamma, \delta) \ \text{è soluzione dell'equazione omogenea associata}\} \subseteq \mathcal{S}$$

Resta da dimostrare l'inclusione opposta, ossia che ogni soluzione di (2.1) è della forma "$(\overline{x}, \overline{y})$ + una soluzione dell'equazione omogenea associata".

Questo segue osservando che, se (α, β) è una soluzione di (2.1), allora $(\alpha - \overline{x}, \beta - \overline{y})$ è una soluzione della equazione omogenea associata.

□

7. Esempio di risoluzione di una equazione diofantea

Troviamo tutte le soluzioni dell'equazione diofantea

$$435x + 102y = 15$$

Ricordiamo che una soluzione è una coppia $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ che soddisfa l'equazione data:

$$435\overline{x} + 102\overline{y} = 15$$

- Per prima cosa verifichiamo se l'equazione proposta ammette soluzioni: sappiamo che questo accade se e solo se $MCD(435, 102) \mid 15$. Usiamo dunque l'algoritmo di Euclide per calcolare $MCD(435, 102)$.

$$435 = 102 \cdot 4 + 27$$

$$102 = 27 \cdot 3 + 21$$

$$27 = 21 \cdot 1 + 6$$

$$21 = 6 \cdot 3 + 3$$

$$6 = 3 \cdot 2 + 0$$

  Dunque $MCD(435, 102) = 3 \mid 15$ e la nostra equazione ammette soluzioni.
- Adesso troviamo una soluzione particolare dell'equazione. Se utilizziamo l'algoritmo di Euclide "alla rovescia" troviamo dopo qualche calcolo che

$$3 = 102 \cdot 64 - 435 \cdot 15$$

  Se moltiplichiamo questa uguaglianza per $\dfrac{15}{MCD(435, 102)} = 5$ otteniamo

$$15 = 102 \cdot 320 - 435 \cdot 75$$

  Abbiamo dunque che $(-75, 320)$ è una soluzione particolare di

$$435x + 102y = 15$$

  È possibile anche seguire una strada leggermente diversa: visto che abbiamo scoperto che $MCD(435, 102) = 3 \mid 15$, osserviamo che l'equazione

$$435x + 102y = 15$$

  è equivalente (ossia ha le stesse soluzioni) di quella che si ottiene dividendo tutti i coefficienti per 3:

$$145x + 34y = 5$$

  Dall'algoritmo di Euclide che abbiamo usato per calcolare $MCD(435, 102)$ possiamo ricavare, dividendo per 3 tutti i dividendi, i divisori e i resti, un algoritmo di Euclide che calcola $MCD(145, 34) = 1$. Ripercorrendo "alla rovescia" questo algoritmo si trova che

$$1 = 34 \cdot 64 - 145 \cdot 15$$

  Se moltiplichiamo questa uguaglianza per 5 otteniamo

$$5 = 34 \cdot 320 - 145 \cdot 75$$

  da cui ricaviamo che $(-75, 320)$ è una soluzione particolare di

$$145x + 34y = 5$$

  Potete scegliere voi fra le due strade illustrate quella che vi sembra più conveniente (in questa seconda i calcoli coinvolgono numeri più piccoli).

- Troviamo adesso tutte le infinite soluzioni della equazione diofantea data. Consideriamo la omogenea associata

$$435x + 102y = 0$$

e calcoliamone tutte le soluzioni. Dividendo entrambi i membri per $3 = MCD(435, 102)$ (IMPORTANTE: ricordarsi sempre di dividere per il MCD a questo punto dello svolgimento!) ci riduciamo a

$$145x + 34y = 0$$

OSSERVAZIONE 2.21. Ovviamente se avete scelto di seguire la strada di studiare invece che

$$435x + 102y = 15$$

l'equazione equivalente

$$145x + 34y = 5$$

avete subito che l'equazione omogenea associata è

$$145x + 34y = 0$$

Dobbiamo dunque trovare tutte le soluzioni di

$$145x = -34y$$

Sappiamo che 145 e 34 sono coprimi, e dunque se $(\overline{x}, \overline{y})$ è una soluzione deve valere $\overline{y} = 145q$, con $q \in \mathbb{Z}$. Sostituendo

$$145\overline{x} = -34 \cdot 145q$$

da cui ricaviamo $\overline{x} = -34q$. Dunque tutte le soluzioni di

$$145x + 34y = 0$$

devono essere della forma $(-34q, 145q)$ con $q \in \mathbb{Z}$. Il Teorema 2.20 ci permette a questo punto di concludere l'esercizio: le soluzioni di

$$145x + 34y = 0$$

sono tutte e sole le coppie $(-34q, 145q)$ al variare di $q \in \mathbb{Z}$ e l'insieme di tutte le soluzioni di

$$435x + 102y = 15$$

è

$$\{(-75 - 34q, 320 + 145q) \mid q \in \mathbb{Z}\}$$

Trovate altri esempi ed esercizi nel libro [**DM**], Capitolo 4, Paragrafo 5, pag. 61.

8. Esercizi

ESERCIZIO 2.22. Calcolare i seguenti massimi comuni divisori:

$$MCD(1094, 189) \qquad MCD(2562, 696)$$

Trovare dei numeri interi m, n, s, t tali che:

$$MCD(1094, 189) = 1094m + 189n \qquad MCD(2562, 696) = 2562s + 696t$$

ESERCIZIO 2.23. Trovare due interi a e b tali che l'algoritmo di Euclide per determinare $MCD(a, b)$ consista di esattamente 7 passaggi.

Esercizio 2.24. Dimostrare 'in maniera costruttiva' l'Identità di Bezout, per induzione sul numero di passi dell'algoritmo di Euclide per $MCD(a, b)$.

Esercizio 2.25. Consideriamo la successione dei numeri di Fibonacci F_n ($n \in \mathbb{N}$): Dimostrare che il massimo comun divisore di due numeri di Fibonacci consecutivi è sempre 1.

Esercizio 2.26. Consideriamo l'insieme:

$$A = \{3k \mid k = 1, 2, \ldots, 100\} \cup \{2, 4, 5\}$$

a) Quante sono le funzioni $f : A \to A$?
b) Esistono funzioni $f : A \to A$ tali che, $\forall x \in A$, $MCD(x, f(x)) = 1$?
c) Quante sono le funzioni $f : A \to A$ tali che, $\forall x \in A$, $MCD(x, f(x)) > 1$?
d) Fra le funzioni del punto c), ne esiste almeno una bigettiva diversa dall'identità ?

Esercizio 2.27. Dire se la funzione $f : \mathbb{N}^{>0} \times \mathbb{N}^{>0} \to \mathbb{N}^{>0}$ data da $f(x, y) = x^{MCD(x,y)}$ è iniettiva, surgettiva, bigettiva.
Dire se la funzione $g : \mathbb{N}^{>0} \times \mathbb{N}^{>0} \to \mathbb{N}^{>0} \times \mathbb{N}^{>0}$ data da $f(x, y) = (x \cdot MCD(x, y), y)$ è iniettiva, surgettiva, bigettiva.

Esercizio 2.28. Risolvere l'equazione diofantea

$$40x + 252y = 44$$

Esercizio 2.29. Trovare tutte le soluzioni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ della equazione diofantea

$$4060x + 1953y = 49$$

È vero che per ogni soluzione $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ vale che $x - y$ è un multiplo di 3?

Esercizio 2.30. Calcolare il MCD $(1573, 1144)$ e trovare tutti gli interi m, n che soddisfano

$$1573m + 1144n = 858$$

Esercizio 2.31. Si determini l'insieme $A = \{(x, y) \in \mathbb{Z}^2 \mid 102x + 153y = 459\}$ Si determini la cardinalità dell'insieme $B = \{(x, y) \in A \mid |x| + |y| < 100\}$.

CAPITOLO 3

Lezione del 8 ottobre

1. Alcune riflessioni sui numeri primi

Nelle lezioni precedenti abbiamo più volte chiamato in gioco i numeri primi. Dedichiamo loro un breve paragrafo in cui si accosta alla definizione tradizionale una definizione alternativa, e si cominciano a mettere a fuoco i due concetti di *elemento primo* e di *elemento irriducibile* di un anello. Dimostreremo anche il teorema della fattorizzazione unica, utilizzando il Teorema 2.15.

Cominciamo ricordando la più nota definizione di numero primo:

DEFINIZIONE 3.1. Un numero intero $p \geq 2$ si dice primo se gli unici suoi divisori interi positivi sono 1 e p stesso.

Ecco i numeri primi più piccoli: 2,3,5,7,11,13,17,19,23,29,31.

Anche se non abbiamo ancora introdotto la definizione formale di anello (che avete però visto al corso di Geometria 1), osserviamo che in questa prima definizione si mette in evidenza il fatto che i numeri primi sono elementi *irriducibili* di $\mathbb{Z}$, ossia elementi che non hanno una fattorizzazione 'vera': ogni volta che si scrive un numero primo p come prodotto $p = st$, visto che gli unici divisori di p sono 1 e p stesso, uno fra i numeri s o t è uguale a 1 o a -1, dunque è un elemento invertibile di $\mathbb{Z}$. In altre parole, ogni volta che si prova a fattorizzare p come prodotto di due fattori, uno dei due fattori è per forza invertibile.

Cerchiamo ora un'altra caratterizzazione dei numeri primi.

TEOREMA 3.2. *Sia p un numero primo. Supponiamo che, dati due numeri interi b, c, valga $p \mid bc$: allora possiamo concludere che o $p|b$ o $p|c$.*

DIMOSTRAZIONE. Se $p|b$ abbiamo finito. Consideriamo allora il caso in cui p non divide b; allora vale che $MCD(p, b) = 1$.[1]

Possiamo dunque applicare il Teorema 2.15: visto che $p \mid bc$ e che $MCD(p, b) = 1$ tale teorema ci dice che $p|c$. Dunque abbiamo dimostrato che o $p|b$ o $p|c$.

□

Vale anche il viceversa del Teorema 3.2:

TEOREMA 3.3. *Sia a un numero intero ≥ 2 con la seguente proprietà: per ogni $b, c \in \mathbb{Z}$, se $a \mid bc$ allora o $a|b$ o $a|c$. Allora a è un numero primo.*

DIMOSTRAZIONE. Dimostriamo la contronominale, ossia che se a non è primo, allora a non soddisfa la proprietà. Infatti se a non è primo allora deve avere un divisore positivo k diverso da 1 e da a, dunque deve valere

$$a = ks \qquad \text{con} \quad 1 < k < a \quad \text{e} \quad 1 < s < a$$

[1]Infatti $MCD(p, b)$ deve essere in particolare un divisore positivo di p, dunque ci sono solo due possibilità: $MCD(p, b) = 1$ o $MCD(p, b) = p$. La seconda però nel nostro caso è esclusa perché allora varrebbe $p|b$.

Ponendo $k = b$ e $s = c$ abbiamo allora trovato due numeri interi tali che $a \mid bc$ ma a non divide né b né c, ossia abbiamo mostrato che a non soddisfa la proprietà.

□

Gli enunciati dei due teoremi precedenti ci danno la seguente caratterizzazione dei numeri primi:

TEOREMA 3.4. *Un numero intero $p \geq 2$ è primo se e solo se soddisfa la seguente proprietà: per ogni $b, c \in \mathbb{Z}$, se $p \mid bc$ allora o $p|b$ o $p|c$.*

OSSERVAZIONE 3.5. L'enunciato di questo teorema costituisce una definizione alternativa di numero primo. Questa nuova definizione mette in evidenza il fatto che un numero primo è un *elemento primo* dell'anello $\mathbb{Z}$. In un anello, un elemento γ si dice *primo* se, comunque si prendano α, β elementi dell'anello tali che $\gamma|\alpha\beta$ allora si ha che $\gamma|\alpha$ o $\gamma|\beta$. Anche se abbiamo appena visto che in $\mathbb{Z}$ i concetti di elemento irriducibile e di elemento primo coincidono, in generale per altri anelli non è così: in certi anelli l'insieme degli elementi irriducibili e l'insieme degli elementi primi non coincidono. Approfondiremo questo aspetto più avanti.

Possiamo a questo punto discutere la proprietà, ben nota fin dalle scuole medie, che ogni numero intero ammette una fattorizzazione unica come prodotto di primi.

Spezziamo il discorso in due parti: innanzitutto mostriamo che ogni numero si fattorizza in prodotto di primi.

TEOREMA 3.6 (Esistenza della fattorizzazione in prodotto di primi). *Ogni numero intero ≥ 2 o è primo o si può scrivere come prodotto di numeri primi.*

DIMOSTRAZIONE. Questa dimostrazione è un facile esercizio di induzione. Utilizzeremo qui il principio del minimo.

Consideriamo il predicato $P(n)$: "il numero n o è primo o si può scrivere come prodotto di numeri primi" e sia S l'insieme dei numeri interi $m \geq 2$ tali che la proposizione $P(m)$ sia falsa.

Osserviamo che dimostrare l'enunciato del teorema equivale a dimostrare che S è vuoto. Procediamo per assurdo e supponiamo dunque che S non sia vuoto. Allora S, che è un sottoinsieme non vuoto di $\mathbb{N}$, per il principio del minimo ha un elemento minimo, che chiamiamo s.

Riassumendo, cosa sappiamo di s ? Sappiamo che è un intero ≥ 2 tale che $P(s)$ è falsa, ossia che non è né primo né prodotto di primi, e che è il più piccolo numero con queste caratteristiche.

In particolare, non essendo primo si potrà scrivere come prodotto di due numeri a e b, $s = ab$, dove $1 < a < s$ e $1 < b < s$. Quindi a e b, essendo ≥ 2 e strettamente minori di s, sono tali che le proposizioni $P(a)$ e $P(b)$ sono vere (altrimenti sarebbe uno di loro, e non s, il minimo dell'insieme S). Questo vuol dire che a e b sono o primi o prodotto di primi e dunque il prodotto ab ci fornisce una decomposizione in primi di s. Abbiamo ottenuto un assurdo, perché s per costruzione non può ammettere una decomposizione in primi.

□

ESERCIZIO 3.7. Riscrivere la dimostrazione appena vista utilizzando l'induzione 'forte' o l'induzione 'semplice'.

Teorema 3.8 (Unicità della fattorizzazione in prodotto di primi). *Siano*

$$a = p_1 p_2 p_3 \cdots p_r$$

$$a = q_1 q_2 \cdots q_s$$

due fattorizzazioni del numero intero $a \geq 2$, dove i numeri p_i $(i = 1, 2, \ldots, r)$ e q_j $(j = 1, 2, \ldots, s)$ sono primi. Supponiamo di avere scritto le fattorizzazioni in modo che $p_1 \leq p_2 \leq \cdots \leq p_r$ e $q_1 \leq q_2 \leq \cdots \leq q_s$. Allora vale che $r = s$ e, per ogni $i = 1, 2, \ldots, s$, $p_i = q_i$.

Dimostrazione. Sia $r \leq s$ e dimostriamo il teorema per induzione su r. Il passo base $r = 1$ è semplice: s deve essere uguale ad 1 altrimenti il numero a sarebbe contemporaneamente primo ($a = p_1$) e non primo ($a = q_1 \cdots q_s$). A quel punto è immediato concludere che $a = p_1 = q_1$.

Per il passo induttivo, supponiamo che l'enunciato del teorema sia vero quando la prima fattorizzazione ha $r - 1$ fattori primi.

Cominciamo considerando il primo p_1. Visto che p_1 divide $q_1 q_2 \cdots q_s = q_1(q_2 \cdots q_s)$, per il Teorema 3.2 o $p_1 | q_1$ oppure $p_1 | (q_2 \cdots q_s)$. Se vale $p_1 | q_1$ allora, visto che p_1 e q_1 sono entrambi primi, deve valere $p_1 = q_1$. Dimostriamo per assurdo che deve essere proprio così. Se invece non valesse $p_1 | q_1$ allora avremmo $p_1 | (q_2 \cdots q_s)$ da cui, iterando il ragionamento, potremmo alla fine trovare dopo un numero finito di passi un i tale che $p_1 = q_i > q_1$ (se fosse $q_i = q_1$ allora fin dall'inizio avremmo trovato $p_1 | q_1$). Dunque q_1, essendo strettamente minore di p_1, è strettamente minore di tutti i primi p_i.

Ma noi sappiamo che q_1 divide $p_1(p_2 \cdots p_r)$. Con ragionamento analogo al precedente potremmo trovare un j tale che $q_1 = p_j$, ma questo è assurdo, visto che q_1 è strettamente minore di tutti i primi p_i.

Dunque deve valere $p_1 = q_1$. Dividendo l'uguaglianza $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ per p_1 otteniamo $p_2 \cdots p_r = q_2 \cdots q_s$, dove a sinistra abbiamo il prodotto di $r - 1$ fattori e a destra abbiamo $s - 1$ fattori.

Per ipotesi induttiva sappiamo che $r - 1 = s - 1$ e che i primi presenti nelle due fattorizzazioni sono a due a due uguali. Questo conclude la dimostrazione.

□

Esercizio 3.9. Alla luce del teorema di esistenza e unicità della fattorizzazione in primi riprendiamo in considerazione il metodo per la ricerca del massimo comune divisore fra due numeri a e b che si basa sulla scomposizione di a e b in fattori primi (descritto nel Capitolo 2, Paragrafo 2). Come mai questo metodo dà effettivamente il $MCD(a, b)$?

Concludiamo queste riflessioni sui numeri primi con il famoso teorema che ci garantisce che i numeri primi sono infiniti.

Teorema 3.10. *L'insieme $\mathcal{P}$ dei numeri primi è infinito.*

Dimostrazione. Supponiamo per assurdo che $\mathcal{P}$ sia finito e siano dunque

$$p_1, p_2, \ldots, p_N$$

tutti i numeri primi. Consideriamo allora il numero

$$a = (p_1 \cdot p_2 \cdots p_N) + 1$$

Per il Teorema 3.6 c'è un numero primo che divide a. Nel nostro caso vuol dire che uno dei p_i deve dividere a. Ma nessuno dei numeri p_i divide a, visto che, per ogni $i = 1, 2, \ldots, N$, da $a = (p_1 \cdot p_2 \cdots p_N) + 1$ si deduce che il resto della divisione euclidea di a per p_i è 1.

□

Curiosità: avete letto il libro del celebre matematico G.H. Hardy *Apologia di un matematico*? Ve lo consiglio. La dimostrazione che abbiamo appena visto compare come esempio di dimostrazione matematicamente "bella" e significativa.

2. Congruenze

Fissiamo un numero m intero positivo, per esempio $m = 12$.

Fare l'aritmetica modulo 12 vuol dire considerare tutti gli altri numeri interi da un punto di vista particolare: di ogni numero n ci interesserà solo il suo resto quando facciamo la divisione euclidea per 12. Per esempio, 38 sarà identificato al numero 2, visto che:

$$38 = 12 \cdot 3 + 2$$

Ma anche 62 sarà identificato al 2:

$$62 = 12 \cdot 5 + 2$$

Altri esempi, dove la freccia indica il resto della divisione per 12:

$$43 \to 7 \qquad 12 \to 0 \qquad -6 \to 6 \qquad -11 \to 1$$

$$15 \to 3 \qquad 27 \to 3 \qquad -8 \to 4 \qquad -12 \to 0$$

Si dirà per esempio che 38, 62 e 2 sono "congrui fra loro" modulo 12, e si scriverà:

$$38 \equiv 62 \equiv 2 \quad (12)$$

Pensandoci bene, questa è una aritmetica molto naturale per le lancette del nostro orologio: se si parte dalla mezzanotte di un certo giorno e si lasciano trascorrere due ore, le lancette indicheranno le 2. Ma anche se facciamo trascorrere 38 ore o 62 ore, le lancette indicheranno sempre le 2. Per le lancette del nostro orologio, i numeri 2, 68 e 38 sono in effetti "identificati"!

Dall'esempio passiamo ad una definizione più generale:

Definizione 3.11. Fissato un numero intero positivo m, diremo che due numeri interi a e b sono "congrui fra loro modulo m" se quando facciamo la divisione euclidea di a per m otteniamo lo stesso resto di quando facciamo la divisione euclidea di b per m. Scriveremo:

$$a \equiv b \qquad (m)$$

oppure

$$a \equiv b \qquad mod\ m$$

Se due numeri a e b sono congrui fra loro modulo m, possiamo scrivere le loro divisioni euclidee per m, che, come sappiamo, hanno lo stesso resto:

$$a = mq + r \qquad b = ms + r$$

Notiamo allora che

$$a - b = mq + r - (ms + r) = mq - ms = m(q - s)$$

Questo significa che m divide $a - b$. Viceversa, se prendiamo due numeri a e b che non sono congrui fra loro modulo m, possiamo facilmente osservare che $a-b$ non è un multiplo di m. Infatti, poniamo $a = mq + r_1$ e $b = ms + r_2$, dove r_1 e r_2 sono diversi fra loro e possiamo supporre $r_1 > r_2$. Scrivendo

$$a - b = mq + r_1 - (ms + r_2) = m(q - s) + (r_1 - r_2)$$

si nota che la divisione euclidea di $a - b$ per m ha resto $r_1 - r_2$, che è diverso da 0. In conclusione, abbiamo dimostrato:

PROPOSIZIONE 3.12. *Dato un numero intero positivo m, due numeri interi a e b sono congrui fra loro modulo m se e solo se m divide $a - b$ (questo equivale anche a dire che m divide $b - a$).*

OSSERVAZIONE 3.13. Dunque, la condizione "m divide $a - b$" poteva essere presa come definizione di congruenza fra i numeri interi a e b.

TEOREMA 3.14. *Le congruenze "rispettano" somme e prodotti, nel senso che se $a \equiv a' \bmod m$ e $b \equiv b' \bmod m$, allora $a + b \equiv a' + b' \bmod m$ e $ab \equiv a'b' \bmod m$.*

DIMOSTRAZIONE. Supponiamo che $a' = a + km$ e $b' = b + k'm$.
Allora $a' + b' = a + b + (k + k')m$, e quindi $a + b \equiv a' + b' \bmod m$.
Inoltre $a'b' = (a + km)(b + k'm) = ab + kmb + k'ma + kk'm^2$, e siccome $kmb + k'ma + kk'm^2$ è un multiplo di m possiamo concludere $a'b' \equiv ab \bmod m$. □

ESEMPIO 3.15. Trovare il resto della divisione euclidea di $1253423 \cdot 134432$ per 5. Visto che $1253423 \equiv 3 \bmod 5$ e che $134432 \equiv 2 \bmod 5$, possiamo sostituire e scrivere: $1253423 \cdot 134432 \equiv 3 \cdot 2 \equiv 6 \equiv 1 \bmod (5)$. Quindi il resto è 1.

ESEMPIO 3.16. Trovare il resto della divisione euclidea di 2^{99} per 7. Soluzione: $2^{99} = 2^{3 \cdot 33} = 8^{33}$. Ora, 8 è congruo a 1 modulo 7 dunque possiamo continuare sostituendo: $8^{33} \equiv 1^{33} \equiv 1 \bmod 7$. Quindi il resto è 1.

ESEMPIO 3.17. Trovare il resto della divisione di 3^{11} per 5. Soluzione: Modulo 5 abbiamo le seguenti congruenze: $3^{11} \equiv 3^2 3^2 3^2 3^2 3^2 3 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 3 \equiv (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot 3 \equiv -3 \equiv 2 \bmod (5)$. Quindi il resto è 2.

3. Calcolo veloce dei resti e basi numeriche

Ricordiamo che quando scriviamo un numero, ad esempio 1234567, implicitamente sottintendiamo che esso è scritto in base 10, ovvero:

$$1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$$

Utilizzando il linguaggio delle congruenze possiamo trovare dei modi rapidi di calcolare il resto della divisione euclidea. I prossimi esempi illustrano il caso in cui il divisore è $3, 9, 11, 4, 7$ (e in particolare ci fanno riottenere i famosi criteri di divisibilità per $3, 4, 7, 11$).

ESEMPIO 3.18. Trovare il resto della divisione di 1234564 per 3. Soluzione: Siccome $10 \equiv 1 \bmod 3$, nel fare le congruenze modulo 3 possiamo sostituire 10 con 1 nell'espansione decimale ottenendo: $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 1 \bmod 3$. Quindi il resto è 1. Se avessimo cercato il resto della divisione di 1234564 per 9, avremmo anche in questo caso sostituito il 10 con 1 ottenendo $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 7 \bmod 9$.

ESEMPIO 3.19. Trovare il resto della divisione di 1234567 per 11. Soluzione: Siccome $10 \equiv -1 \bmod (11)$, nel fare le congruenze modulo 11 possiamo sostituire 10 con -1 nell'espansione decimale ottenendo: $1234567 \equiv 1 - 2 + 3 - 4 + 5 - 6 + 7 \equiv 4$. Quindi il resto è 4.

ESEMPIO 3.20. Trovare il resto della divisione di 1234567 per 4. Soluzione: osserviamo che $100 = 25 \cdot 4 \equiv 0 \bmod (4)$. Quindi $1234567 = 12345 \cdot 100 + 67 \equiv 67 \equiv 3 \bmod (4)$.

ESEMPIO 3.21. Trovare il resto della divisione di 1234567 per 7. Soluzione: osserviamo che $1000 = 7 \cdot 143 - 1 \equiv -1 \bmod (7)$. Quindi $1234567 = 1 \cdot 1000^2 + 234 \cdot 1000 + 567 \equiv 1 - 234 + 567 \equiv 334 \equiv 5 \bmod 7$.

Esempio 3.22. Si dimostri che $\sqrt{1234567}$ non è un intero. Soluzione: per assurdo supponiamo che vi sia un intero x tale che $x^2 = 1234567$. Per l'esercizio precedente $x^2 \equiv 1234567 \equiv 3 \bmod 4$. Quindi basta mostrare che x^2 non può essere congruente a 3 modulo 4. Siccome x è congruo a $0, 1, 2$ o 3 modulo 4, ci sono solo quattro verifiche da fare:

$$\begin{aligned} 0^2 &\equiv 0 \bmod 4 \\ 1^2 &\equiv 1 \bmod 4 \\ 2^2 &\equiv 0 \bmod 4 \\ 3^2 &\equiv 1 \bmod 4 \end{aligned}$$

Esempio 3.23. Cambiamento di base: verifichiamo che la scrittura (12345) in base 10 e la scrittura 30071 in base 8 indicano lo stesso numero. In simboli $(12345)_{\text{base } 10} = (30071)_{\text{base } 8}$. Infatti

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

I resti danno la scrittura in base 8 richiesta: infatti da quanto abbiamo scritto segue che $12345 = 1543 \cdot 8 + 1 = 192 \cdot 8^2 + 7 \cdot 8 + 1 = 24 \cdot 8^3 + 7 \cdot 8 + 1 = 3 \cdot 8^4 + 7 \cdot 8 + 1$.

4. Inverso di un numero modulo un intero positivo

Gli unici numeri interi che ammettono un inverso moltiplicativo in $\mathbb{Z}$ sono $+1$ e -1. Quando si considera l'aritmetica modulo un intero positivo m, invece sarà naturale trovare vari numeri che ammettono un inverso. Naturalmente, in questo caso per dire che un numero è inverso di un altro non pretendiamo che il prodotto dei due numeri faccia 1, ma ci basta che faccia un qualunque numero *congruo* a 1:

Definizione 3.24. Sia m un intero positivo. Un inverso di un intero a modulo m è un intero x tale che $ax \equiv 1 \bmod m$.

Esempio 3.25. 2 è un inverso di 3 modulo 5 in quanto $2 \cdot 3 = 6 \equiv 1 \bmod 5$. Attenzione, anche 7 è un inverso di 3, e anche -3...Come potete facilmente verificare, quando un numero ammette un inverso modulo m non ne ammette uno solo, ma infiniti.

Esempio 3.26. Non ci sono inversi di 2 modulo 4.

Teorema 3.27. *Un numero a ha un inverso modulo m se e solo se $MCD(a, m) = 1$.*

Dimostrazione. Se $MCD(a, m) = 1$ per il teorema di Bezout possiamo trovare u, v interi tali che $au + mv = 1$ con u, v interi. Questa uguaglianza, letta modulo m, diventa $au \equiv 1 \bmod m$. Quindi u è un inverso di a modulo m.

Viceversa supponiamo che a abbia un inverso u modulo m, ovvero $au \equiv 1 \bmod m$; allora per definizione di congruenza esiste k tale che $au + mk = 1$. Questo implica (per il Teorema 2.13) $MCD(a, m) = 1$. □

Non sempre possiamo dividere in una congruenza. Ad esempio $2 \cdot 7 \equiv 2 \cdot 4 \bmod 6$, ma $7 \not\equiv 4 \bmod 6$. In generale, la divisione in una congruenza segue la seguente regola:

Teorema 3.28. *Dato $m \in \mathbb{N} - \{0\}$, per ogni $a \in \mathbb{Z} - \{0\}$, $b_1, b_2 \in \mathbb{Z}$ vale:*

$$a\ b_1 \equiv a\ b_2 \quad (m) \quad \Leftrightarrow \quad b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a, m)}\right)$$

Osservazione 3.29. Quindi, se c'è un numero a che divide entrambi i membri di una congruenza, si può "semplificare", a patto però di dividere anche il modulo m per $MCD(a, m)$. Ad esempio:

$$66 \equiv 42 \quad (8) \quad \Leftrightarrow \quad 11 \equiv 7 \quad (4)$$

dove abbiamo diviso il membro di sinistra e quello di destra per 6 e il modulo per $MCD(6, 8) = 2$. Se non avessimo diviso il modulo per 2 avremmo ottenuto

$$11 \equiv 7 \quad (8)$$

che è **falsa**.

Dimostrazione. Ricordiamo che stiamo considerando $a \in \mathbb{Z} - \{0\}$. Supponiamo che

$$a\ b_1 \equiv a\ b_2 \quad (m)$$

Allora per la definizione di congruenza vale che

$$m \mid ab_1 - ab_2$$

ossia esiste un $q \in \mathbb{Z}$ tale che

$$ab_1 - ab_2 = mq$$

Possiamo dividere per $MCD(a, m)$ e otteniamo

$$\frac{a}{MCD(a,m)}(b_1 - b_2) = \frac{m}{MCD(a,m)}q$$

Da questo, visto che $\frac{a}{MCD(a,m)}$ e $\frac{m}{MCD(a,m)}$ sono coprimi (ricordate il Corollario 2.14), segue, per il Teorema 2.15, che

$$\frac{m}{MCD(a,m)} \mid b_1 - b_2$$

ovvero che

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Supponiamo ora, viceversa, che sia vero

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Allora $\frac{m}{MCD(a,m)} \mid (b_1 - b_2)$, ossia esiste un $t \in \mathbb{Z}$ tale che

$$t\frac{m}{MCD(a,m)} = b_1 - b_2$$

da cui, moltiplicando per $MCD(a, m)$ otteniamo

$$tm = (b_1 - b_2)MCD(a, m)$$

Osserviamo dunque che

$$m \mid (b_1 - b_2)MCD(a, m)$$

da cui a maggior ragione ricaviamo

$$m \mid (b_1 - b_2)a$$

(abbiamo usato il fatto che $MCD(a, m)|a$) che si riscrive come

$$a\ b_1 \equiv a\ b_2 \quad (m)$$

□

COROLLARIO 3.30. *Se* $ac \equiv bc \pmod{m}$ *e* $MCD(c, m) = 1$, *allora* $a \equiv b \pmod{m}$.

5. Esercizi

ESERCIZIO 3.31. Sia $\{a_n\}_{n\in\mathbb{N}}$ la successione definita per ricorrenza da

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 1 \\ a_{n+1} &= 2a_n + 3a_{n-1} \qquad \forall n \geq 1. \end{aligned}$$

Dimostrare che:

(1) $\mathrm{MCD}(a_n, 3) = 1$ per ogni $n \geq 0$.
(2) $\mathrm{MCD}(a_{n+1}, a_n) = 1$ per ogni $n \geq 0$.

ESERCIZIO 3.32. Dimostrare che l'insieme dei numeri primi congrui a 3 modulo 4 è infinito.[2]

ESERCIZIO 3.33. Consideriamo i numeri interi x tali che $10000000 \leq x < 20000000$. Quanti di questi numeri sono congrui a 1 modulo 3?

ESERCIZIO 3.34. Stabilire se è vero o falso che

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot 12 \cdot 13 \equiv 7 \qquad (17)$$

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot 12 \cdot 13 \equiv 0 \qquad (1024)$$

In generale è vero o falso che il prodotto di 13 numeri interi consecutivi è sempre divisibile per 1024 ?

ESERCIZIO 3.35. Consideriamo la successione definita per ricorrenza

$$x_0 = 2,\ x_{n+1} = (x_n^2 + 1)$$

Sia r_n il resto della divisione euclidea di x_n per 5.

1) Calcolare i primi 7 valori di r_n.

2) Si dia una regola generale per calcolare r_n e la si dimostri per induzione.

3) Si calcoli r_{10000}.

ESERCIZIO 3.36 (Tornei all'italiana). Supponiamo di avere n squadre di calcio, con n numero pari, e di voler organizzare un torneo all'italiana[3]. Basta pensare al girone d'andata, quello di ritorno poi è automatico, dunque bisogna organizzare $n-1$ turni. Le congruenze possono aiutarci. Possiamo infatti utilizzare la seguente regola:

[2]Anche l'insieme dei numeri primi congrui a 1 modulo 4 è infinito, ma di questo parleremo più avanti.

[3]Se avessimo un numero dispari di squadre ci potremmo comunque ricondurre a questo caso aggiungendo una squadra fittizia, con la regola che se una squadra deve incontrarla le tocca invece un turno di riposo.

- al turno i la squadra x, con $1 \leq x \leq n-1$, incontrerà la squadra y dove y soddisfa $1 \leq y \leq n-1$ e

$$x + y \equiv i \mod n - 1$$

a meno che questa equazione non dia come soluzione $x = y$. In tal caso la squadra x incontra la squadra n.

Dimostrare che il torneo così preparato è ben organizzato (vedi Tabella 1).

	Turno 1	Turno 2	Turno 3	Turno 4	Turno 5
squadra 1	vs 5	vs 6	vs 2	vs 3	vs 4
squadra 2	vs 4	vs 5	vs 1	vs 6	vs 3
squadra 3	vs 6	vs 4	vs 5	vs 1	vs 2
squadra 4	vs 2	vs 3	vs 6	vs 5	vs 1
squadra 5	vs 1	vs 2	vs 3	vs 4	vs 6
squadra 6	vs 3	vs 1	vs 4	vs 2	vs 5

TABELLA 1. Esempio: il tabellone del torneo nel caso di 6 squadre.

ESERCIZIO 3.37. Dato un numero naturale m, dimostrare che se $2^m + 1$ è primo allora m è una potenza di 2.

ESERCIZIO 3.38 (I numeri di Fermat). Dato $n \in \mathbb{N}$ definiamo:

$$\mathcal{F}_n = 2^{2^n} + 1$$

I numeri $\mathcal{F}_n$ si chiamano *numeri di Fermat*. Fermat[4] aveva congetturato che tali numeri fossero tutti primi..ma, come fu mostrato da Eulero[5], la congettura è falsa. Provate anche voi a confutarla:

- Dimostrare che $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ sono primi. Dimostrare che anche $\mathcal{F}_4$ è primo. [Consiglio: non fatelo davvero, $\mathcal{F}_4$ è un numero troppo grande. La cosa diventerà abbordabile dopo che saprete i risultati degli Esercizi 6.39 e 6.40.]
- Dimostrare che $\mathcal{F}_5$ è divisibile per 641. [Traccia: può essere utile osservare che $641 = 2^4 + 5^4 = 1 + 5 \cdot 2^7$]

[4]Pierre de Fermat, matematico francese, 1601-1665.

[5]Leonhard Euler, matematico svizzero, 1707-1783.

Possiamo comunque utilizzare i numeri di Fermat per dimostrare, in maniera diversa da quella del Teorema 3.10, che i numeri primi sono infiniti:

- Dimostrare che se $n \neq m$ allora $\mathcal{F}_n$ e $\mathcal{F}_m$ sono coprimi.
- Dedurre dal punto precedente che i numeri primi sono infiniti.

CAPITOLO 4

Lezione del 9 ottobre

1. Metodo per risolvere le congruenze lineari in una incognita

In questo paragrafo ci occuperemo della risoluzione di congruenze lineari con una incognita, ossia del seguente problema:

dati $a, b, m \in \mathbb{Z}$ con $m > 0$, trovare tutti i numeri interi che risolvono la congruenza lineare ad una incognita

$$ax \equiv b \bmod (m) \tag{1}$$

Innanzitutto osserviamo che se esiste un intero d che divide a e m ma non divide b, allora l'equazione (1) non ha soluzioni. Infatti se (1) ha una soluzione $\overline{x}$, allora esiste un intero k tali che $a\overline{x} - b = km$. Da questa uguaglianza si ricava subito che se d divide a e m allora deve dividere anche b.

Esempio 4.1. $6x \equiv 3 \bmod 4$ non ha soluzioni perché 2 divide 6 e 4 ma non divide 3.

In particolare dalla osservazione precedente si deduce che una condizione necessaria perchè l'equazione (1) abbia soluzioni è che $MCD(a, m)$ divida b. Sempre riflettendo sulla osservazione precedente, ci si accorge che in realtà il problema di risolvere $ax \equiv b \bmod (m)$ è in sostanza la stessa cosa del problema di risolvere l'equazione diofantea $ax - km = b$ nelle variabili x e k. Dunque potremmo già concludere che la condizione che $MCD(a, m)$ divida b è anche sufficiente per l'esistenza di soluzioni della equazione (1).

Enunceremo però tutto questo nel prossimo teorema, e daremo una dimostrazione che fornirà anche un algoritmo per trovare tutte le soluzioni quando esistono. Prima di enunciarlo, però, è bene fare una osservazione su quando due equazioni sono equivalenti.

Osservazione 4.2. Dato un numero k che divide a e b, l'equazione

$$\frac{a}{k}x \equiv \frac{b}{k} \quad \left(\frac{m}{MCD(k, m)}\right)$$

è equivalente alla equazione (1), ossia *ha le stesse soluzioni*. Questo segue dalla regola di divisione data dal Teorema 3.28, visto che in base a tale regola un intero $\overline{x}$ soddisfa $a\overline{x} \equiv b \quad (m)$ se e solo se soddisfa

$$\frac{a}{k}\overline{x} \equiv \frac{b}{k} \quad \left(\frac{m}{MCD(k, m)}\right)$$

Analogamente (si può vedere in realtà come caso particolare di quanto appena osservato), se s è un numero primo con m, l'equazione

$$sax \equiv sb \quad (m)$$

è equivalente alla (1).

Teorema 4.3. *La congruenza*

$$ax \equiv b \quad (m) \tag{1}$$

ha soluzione se e solo se il massimo comun divisore tra a e m divide b. In questo caso l'equazione ha infinite soluzioni, precisamente $MCD(a, m)$ soluzioni modulo m.

Osservazione 4.4. Quando diciamo "l'equazione ha $MCD(a, m)$ soluzioni modulo m" intendiamo dire che l'insieme delle soluzioni dell'equazione è composto da esattamente $MCD(a, m)$ soluzioni $\overline{x}$ che soddisfano $0 \leq \overline{x} < m$ e tutte le altre soluzioni sono i numeri che si ottengono da queste sommando loro un multiplo di m.

Dimostrazione. Se $MCD(a, m)$ non divide b sappiamo già che la congruenza non ha soluzioni. Quindi consideriamo il caso in cui $MCD(a, m)$ divide b. In questo caso $MCD(a, m)$ è dunque il massimo divisore positivo comune a tutti e tre i numeri a, b, m; dividendo l'equazione data per $MCD(a, m)$ otteniamo l'equazione

$$a'x \equiv b' \quad (m') \tag{$*$}$$

dove $a' = \dfrac{a}{MCD(a,m)}, b' = \dfrac{b}{MCD(a,m)}, m' = \dfrac{m}{MCD(a,m)}$, che è equivalente alla (1) come sappiamo dalla Osservazione 4.2.

A questo punto notiamo che, per costruzione, a' e m' sono coprimi e che, per il Teorema 3.28, a' ha un inverso e' modulo m'. [1] Osserviamo in particolare che, visto che anche e' ha un inverso modulo m', ovvero a', allora per il Teorema 3.28 risulta che e' è primo con m'.

Moltiplicando per e' il membro di sinistra e quello di destra di $(*)$ otteniamo

$$e'a'x \equiv e'b' \quad (m') \tag{$**$}$$

Per l'Osservazione 4.2 sappiamo che l'equazione $(**)$ è equivalente alla $(*)$.

Visto che $e'a' \equiv 1 \quad (m')$ possiamo riscrivere la $(**)$ come

$$x \equiv e'b' \quad (m')$$

A questo punto si osserva subito che le soluzioni di questa equazione (e dunque le soluzioni della (1)) sono tutti e soli gli interi della forma $e'b' + km'$ al variare di k in $\mathbb{Z}$. Visto che $m' = \dfrac{m}{MCD(a,m)}$, ci sono esattamente $MCD(a, m)$ interi di questa forma in ogni sequenza di m numeri consecutivi. □

Esempio 4.5. Data l'equazione

$$195x \equiv 6 \quad (42)$$

trovare:
a) tutte le sue soluzioni,
b) le sue soluzioni modulo 42, ossia quelle comprese fra 0 e 41.

Soluzione: Osserviamo che $MCD(195, 42) = 3 \mid 6$ dunque l'equazione ha soluzione. Per prima cosa possiamo sostituire 195 con il suo resto modulo 42, ossia 27:

$$27x \equiv 6 \quad (42)$$

[1] Ricordiamo che, in concreto, si può applicare l'algoritmo per trovare una combinazione di Bezout per ottenere due interi x', y' tali che $1 = a'x' + m'y'$ e poi si prende $e' = x'$.

Poi possiamo dividere membro di destra, membro di sinistra e modulo per $MCD(195, 42) = 3$, ottenendo l'equazione equivalente:

$$9x \equiv 2 \quad (\frac{42}{MCD(3, 42)} = 14)$$

Un possibile modo di procedere adesso è il seguente: si nota a occhio che $3 \cdot 9 = 27$ è congruo a -1 modulo 14. Dunque ci conviene moltiplicare il membro di sinistra e quello di destra per 3. Visto che 3 è primo con 14, per l'Osservazione 4.2 sappiamo che l'equazione che otteniamo è equivalente:

$$27x \equiv 6 \quad (14)$$

che si può riscrivere

$$-x \equiv 6 \quad (14)$$

Moltiplicando adesso per -1 (anch'esso primo con 14), otteniamo:

$$x \equiv -6 \quad (14)$$

Questa scrittura descrive già con chiarezza l'insieme di tutte soluzioni dell'equazione

$$195x \equiv 6 \quad (42)$$

Possiamo comunque anche scriverlo così:

$$\{x = -6 + 14q \mid q \in \mathbb{Z}\}$$

Per rispondere alla domanda b), dobbiamo indicare le soluzioni x con $0 \leq x \leq 41$. Sono tre: $-6 + 14, -6 + 2 \cdot 14, -6 + 3 \cdot 14$, cioè 8, 22 e 36. □

2. Esempi di risoluzione di una equazione diofantea (usando le congruenze)

Facciamo qualche esempio che illustra la relazione fra le soluzioni di una equazione diofantea e quella delle equazioni lineari con congruenze ad essa associate. Consideriamo l'equazione diofantea:

$$224x + 108y = 700 \qquad (*)$$

Osservazione 4.6. Se esiste una soluzione (X, Y), il numero intero X deve anche soddisfare

$$224X \equiv 700 \quad (108)$$

(infatti $108Y = 700 - 224X$ dunque $108 \mid 224X - 700$). Viceversa, se un certo numero intero X soddisfa la congruenza $224X \equiv 700 \quad (108)$, questo vuol dire che soddisfa $108 \mid 224X - 700$; allora deve esistere un Y tale che $108Y = 700 - 224X$ e dunque

$$224X + 108Y = 700$$

cioè la coppia (X, Y) risolve l'equazione diofantea $(*)$.

In conclusione abbiamo osservato che l'insieme delle soluzioni dell'equazione

$$224x \equiv 700 \quad (108)$$

coincide con l'insieme dato dalle prime componenti ("le X") delle coppie che risolvono l'equazione diofantea $(*)$.

Risolviamo allora la congruenza

$$224x \equiv 700 \quad (108)$$

Osservazione 4.7. Per risolvere una equazione con congruenze o una equazione diofantea, come avete capito, ci sono molte strade diverse. In questi esempi noi presentiamo una possibile soluzione, ma voi potete divertirvi a trovarne altre, magari più rapide.

Per prima cosa osserviamo sostituiamo il 224 e il 700 con dei numeri più piccoli, a loro congrui modulo 108:

$$8x \equiv 160 \quad (108)$$

Ora possiamo dividere per 8, per semplificare[2] :

$$x \equiv 20 \quad (\frac{108}{MCD(108,8)} = 27)$$

Dunque l'insieme delle soluzioni di

$$224x \equiv 700 \quad (108)$$

è

$$\{x = 20 + 27q \mid q \in \mathbb{Z}\}$$

Possiamo sostituire queste soluzioni al posto della x nella equazione diofantea

$$224x + 108y = 700$$

(che comunque per semplificare possiamo dividere per 4=MCD (224, 108), ottenendo l'equazione diofantea equivalente $56x + 27y = 175$):

$$56(20 + 27q) + 27y = 175$$

Svolgiamo i conti:

$$27y = -1120 + 175 - 56 \cdot 27q$$
$$27y = -945 - 56 \cdot 27q$$
$$y = -35 - 56q$$

Abbiamo dunque trovato che l'insieme delle soluzioni di

$$224x + 108y = 700$$

è:

$$\{(20 + 27q \ , \ -35 - 56q) \mid q \in \mathbb{Z}\}$$

Esempio 4.8. Trovare tutte le soluzioni intere della equazione diofantea

$$54 = 252x + 198y.$$

Soluzione: Dividendo tutto per $18 = MCD(252, 198)$ otteniamo l'equazione equivalente:

$$3 = 14x + 11y$$

Risolviamo la congruenza

$$14x \equiv 3 \bmod 11$$

Moltiplicando per 4 e semplificando otteniamo $x \equiv 1 \bmod 11$, quindi x è della forma $x = 1 + 11k$. Sostituendo nella $14x + 11y = 3$ e facendo i conti si trova $y = -1 - 14k$. Dunque l'insieme delle soluzioni della equazione diofantea data è

$$\{(1 + 11k \ , \ -1 - 14k) \mid k \in \mathbb{Z}\}$$

□

Osserviamo che nei due esempi di questo paragrafo abbiamo trovato in un colpo solo tutte le soluzioni della diofantea, senza dividere il problema nella ricerca di una soluzione particolare e poi di tutte le soluzioni della omogenea associata. Di volta in volta potrete scegliere il metodo di risoluzione che vi sembra più conveniente.

[2]La scelta di sostituire il 700 con 160, anzichè per esempio col 52, è stata dettata proprio dal fatto di aver intravisto la possibilità di questa divisione per 8 che rende la soluzione molto rapida; la conclusione dell'esercizio sarebbe abbastanza veloce anche sostituendo con il 52, verificate.

3. Sistemi di congruenze. Il teorema cinese del resto

Proviamo a risolvere un sistema di due equazioni lineari con congruenze:

$$\begin{cases} x & \equiv & a & (m_1) \\ x & \equiv & b & (m_2) \end{cases}$$

Per prima cosa osserviamo che le soluzioni della prima equazione sono tutti e soli i numeri della forma

$$x = a + km_1 \quad \text{con} \quad k \in \mathbb{Z}$$

Ci chiediamo quando un tale numero risolve anche la seconda equazione. Per saperlo sostituiamo $a + km_1$ alla x nella seconda equazione:

$$a + km_1 \equiv b \qquad (m_2)$$

Qui la variabile è k e otteniamo

$$m_1 k \equiv b - a \qquad (m_2)$$

Questa equazione, come sappiamo, ha soluzione se e solo se $MCD(m_1, m_2) \mid (b - a)$. Dunque siamo già arrivati ad una prima conclusione: il sistema di partenza ha soluzione se e solo se $MCD(m_1, m_2) \mid (b - a)$.

Nel caso in cui ci siano soluzioni, come fare a trovarle tutte? Prendiamo una soluzione particolare k_0 della equazione

$$m_1 k \equiv b - a \qquad (m_2)$$

Allora $x_0 = a + k_0 m_1$ è una soluzione del sistema di partenza ossia

$$\begin{cases} x_0 & \equiv & a & (m_1) \\ x_0 & \equiv & b & (m_2) \end{cases}$$

Come differisce da un'altra soluzione del sistema di partenza? Se anche x_1 soddisfa

$$\begin{cases} x_1 & \equiv & a & (m_1) \\ x_1 & \equiv & b & (m_2) \end{cases}$$

sottraendo opportunamente otteniamo

$$\begin{cases} x_0 - x_1 & \equiv & 0 & (m_1) \\ x_0 - x_1 & \equiv & 0 & (m_2) \end{cases}$$

Dunque $x_0 - x_1$ è un numero che deve essere multiplo di m_1 e anche di m_2. Il più piccolo numero intero positivo che soddisfa tale condizione come sapete si chiama minimo comune multiplo di m_1 e di m_2 e si indica come $mcm\ (m_1, m_2)$. Ricordiamo anche che tutti e soli i numeri che sono divisi da m_1 e da m_2 sono i multipli di $mcm\ (m_1, m_2)$.[3]

In conclusione, tornando al nostro sistema, abbiamo dimostrato che due soluzioni x_0 e x_1 del sistema differiscono per un multiplo di $mcm\ (m_1, m_2)$. Viceversa si verifica subito che, dato x_0 che soddisfa il sistema e dato un multiplo $s \cdot mcm\ (m_1, m_2)$ di $mcm\ (m_1, m_2)$, anche

$$x_0 + s \cdot mcm\ (m_1, m_2)$$

soddisfa il sistema.

Possiamo riassumere tutto quel che abbiamo detto fin qui nel seguente:

[3] Infatti se t è diviso da m_1 e anche da m_2, consideriamo la divisione euclidea di t per $mcm\ (m_1, m_2)$:

$$t = q \cdot mcm\ (m_1, m_2) + r$$

dove $0 \leq r < mcm\ (m_1, m_2)$. Ora, siccome m_1 e m_2 dividono t e $q \cdot mcm\ (m_1, m_2)$, entrambi devono anche dividere r. Allora r deve essere 0, altrimenti sarebbe un numero intero positivo diviso da m_1 e da m_2 ma più piccolo di $mcm\ (m_1, m_2)$ (assurdo).

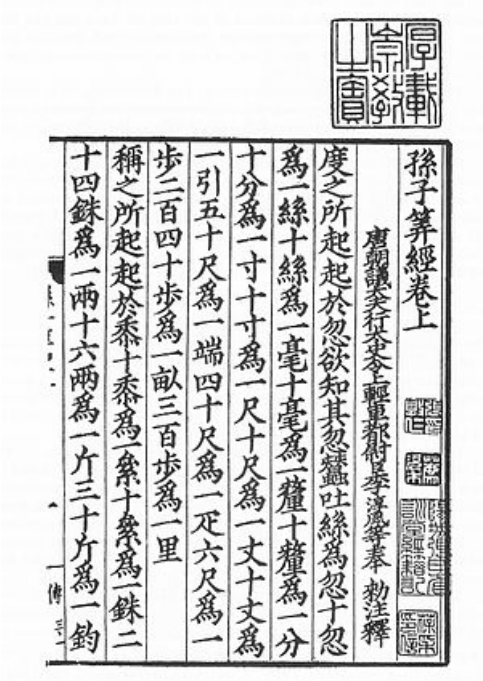

FIGURA 1. Una edizione del trattato Sunzi del V secolo, contenente una formulazione del Teorema Cinese del Resto (immagine da Wikipedia).

TEOREMA 4.9 (Teorema cinese del resto per due equazioni con moduli qualunque). *Dato il sistema di equazioni*

$$\begin{cases} x \equiv a & (m_1) \\ x \equiv b & (m_2) \end{cases}$$

tale sistema ammette soluzione se e solo se $MCD(m_1, m_2) \mid (b-a)$. *In tal caso, presa una soluzione* x_0*, tutte le altre soluzioni del sistema sono i numeri della forma*

$$x_0 + s \cdot mcm\ (m_1, m_2) \quad con \quad s \in \mathbb{Z}$$

OSSERVAZIONE 4.10. Come sappiamo, questo si può esprimere anche dicendo che tutte le soluzioni del sistema sono i numeri x che soddisfano

$$x \equiv x_0 \qquad (mcm\ (m_1, m_2))$$

In particolare osserviamo che esiste un'unica soluzione x con $0 \leq x < mcm\ (m_1, m_2)$.

ESEMPIO 4.11. Si consideri il sistema:

$$\begin{cases} 14x \equiv 4570 & (30) \\ 45x \equiv 231 & (8) \end{cases}$$

Innanzitutto studiamo e risolviamo una per una le due equazioni: la prima ha soluzione perché $MCD(14, 30) = 2 | 4570$ e la possiamo riscrivere sostituendo a 4570 il suo resto modulo 30:

$$14x \equiv 10 \qquad (30)$$

Dividendo per 2 otteniamo:

$$7x \equiv 5 \qquad (15)$$

Se moltiplichiamo entrambi i membri per 2 otteniamo una equazione equivalente perché 2 è primo con il modulo 15 e così arriviamo a

$$14x \equiv 10 \qquad (15)$$

$$-x \equiv 10 \qquad (15)$$

$$x \equiv -10 \qquad (15)$$

$$x \equiv 5 \qquad (15)$$

Per quel che riguarda la seconda equazione, notiamo subito che ha soluzione perché 45 e 8 sono primi fra loro. Sostituiamo ai numeri che compaiono i loro resti modulo 8:

$$5x \equiv 7 \qquad (8)$$

Moltiplicando entrambi i membri per 3 otteniamo l' equazione equivalente

$$15x \equiv 21 \qquad (8)$$

che risolviamo facilmente

$$-x \equiv 5 \qquad (8)$$

$$x \equiv -5 \qquad (8)$$

$$x \equiv 3 \qquad (8)$$

Dunque il sistema dato si può riscrivere come

$$\begin{cases} x \equiv 5 & (15) \\ x \equiv 3 & (8) \end{cases}$$

Ora possiamo applicare il teorema cinese del resto: il sistema ammette soluzione perché $MCD(15, 8) = 1$ e dunque divide $5 - 3$.

A questo punto dobbiamo trovare una soluzione particolare. Ne esisterà una (e una sola) compresa fra 0 e 119 (infatti $120 = 15 \cdot 8$ è il mcm $(15, 8)$). Possiamo cercarla fra i numeri $5, 20, 35, 50, 65, ...$ che sono le soluzioni della prima equazione. Vediamo subito che 35 fa al caso nostro. Dunque, grazie al teorema cinese del resto, possiamo affermare che tutte le soluzioni del sistema sono i numeri della forma

$$35 + 120s \qquad \text{con} \quad s \in \mathbb{Z}$$

Osservazione 4.12. Se non avessimo "visto" subito il 35 avremmo comunque potuto seguire il metodo standard: la prima equazione ci dice che x deve essere del tipo $x = 5 + 15k$. Sostituendo nella seconda abbiamo

$$5 + 15k \equiv 3 \qquad (8)$$

ossia

$$15k \equiv -2 \qquad (8)$$

$$-k \equiv -2 \qquad (8)$$

$$k \equiv 2 \qquad (8)$$

Allora $x = 5 + 15 \cdot 2 = 35$ è una soluzione particolare..e abbiamo "ritrovato" il 35.

Riscriviamo ora il teorema nel caso particolare in cui i moduli delle due equazioni sono primi fra loro, come premessa per poi enunciare il teorema cinese del resto nella sua forma classica.

TEOREMA 4.13 (Teorema cinese del resto per due equazioni con moduli primi fra loro). *Dato il sistema di congruenze*

$$\begin{cases} x & \equiv & a & (m_1) \\ x & \equiv & b & (m_2) \end{cases}$$

con $MCD(m_1, m_2) = 1$*, tale sistema ammette sempre soluzione ed esiste un'unica soluzione* x_0 *tale che* $0 \leq x_0 < m_1 \cdot m_2$*. Tutte le altre soluzioni del sistema sono i numeri della forma*

$$x_0 + q \cdot m_1 \cdot m_2 \quad con \quad q \in \mathbb{Z}$$

La dimostrazione che abbiamo dato si generalizza facilmente al caso di sistemi di n congruenze in cui i moduli siano a due a due coprimi:

TEOREMA 4.14 (Teorema cinese del resto, forma classica). *Dato il sistema di congruenze*

$$\begin{cases} x & \equiv & a_1 & (m_1) \\ x & \equiv & a_2 & (m_2) \\ .. & .. & .. & .. \\ .. & .. & .. & .. \\ x & \equiv & a_{n-1} & (m_{n-1}) \\ x & \equiv & a_n & (m_n) \end{cases}$$

in cui i moduli sono a due a due coprimi (questo vuol dire che per ogni $i \neq j$ *vale* $MCD(m_i, m_j) = 1$*), tale sistema ammette sempre soluzione ed esiste un'unica soluzione* x_0 *tale che* $0 \leq x_0 < m_1 \cdot m_2 \cdots m_{n-1} \cdot m_n$*. Tutte le altre soluzioni del sistema sono i numeri della forma*

$$x_0 + q \cdot m_1 \cdot m_2 \cdots m_{n-1} \cdot m_n \quad con \quad q \in \mathbb{Z}$$

ESERCIZIO 4.15. Dimostrare la forma classica del teorema cinese del resto. (Suggerimento: per induzione sul numero n di equazioni del sistema; il caso di sistemi con due congruenze lo abbiamo già studiato...).

Trovate una discussione del teorema cinese del resto nel libro [**DM**], al Capitolo 4, Paragrafo 7 (in alcuni passaggi viene usata la notazione delle classi di resto, che noi introdurremo presto, ma alcuni esempi ed esercizi sono scritti nella stessa notazione che abbiamo usato noi).

4. Esercizi

ESERCIZIO 4.16. Risolvere l'equazione diofantea

$$40x + 252y = 44$$

Esistono soluzioni (x, y) con $x \equiv 0 \quad (7)$? E con $x \equiv 0 \quad (13)$?

SOLUZIONE: Innanzitutto notiamo che tutti i numeri che compaiono nella equazione sono divisibili per 4. Ci conviene dunque dividere per 4 e studiare l'equazione equivalente:

$$10x + 63y = 11$$

Questa ammette soluzione, visto che 10 e 63 sono primi fra loro e dunque $MCD(10, 63) \mid 11$.

A questo punto, per trovare le soluzioni, sono possibili varie strade. Ne mostriamo una, risolvendo l'equazione lineare con le congruenze:

$$63y \equiv 11 \quad (10)$$

Questa, visto che stiamo lavorando modulo 10, si può riscrivere come:

$$3y \equiv 1 \quad (10)$$

Si nota subito che ha la soluzione $y = -3$. Sappiamo poi, per il Teorema 4.3, che tutte le soluzioni sono gli interi della forma $y = -3 + 10k$ al variare di $k \in \mathbb{Z}$.

A fini puramente didattici, presentiamo in un altro modo l'ultimo passaggio, a partire da

$$3y \equiv 1 \quad (10)$$

Moltiplichiamo per 7 entrambi i membri della equazione (questo produce una equazione equivalente visto che 7 è primo con 10) e otteniamo:

$$21y \equiv 7 \quad (10)$$

ossia

$$y \equiv 7 \quad (10)$$

Da qui "leggiamo" di nuovo lo stesso insieme di soluzioni, presentato nella forma $y = 7 + 10k$ *al variare di* $k \in \mathbb{Z}$.

Sostituendo $y = -3 + 10k$ nella equazione diofantea

$$10x + 63y = 11$$

troveremo il corrispondente valore della x e, al variare di $k \in \mathbb{Z}$, tutte le coppie (x, y) che risolvono il problema posto nel testo:

$$10x + 63(-3 + 10k) = 11$$

$$10x = 200 - 630k$$

$$x = 20 - 63k$$

Dunque l'insieme di tutte le soluzioni della equazione diofantea data è:

$$\{(20 - 63k, -3 + 10k) \in \mathbb{Z} \times \mathbb{Z} \mid k \in \mathbb{Z}\}$$

Rispondiamo ora alle ultime due domande.

Possono esistere soluzioni (x, y) con $x \equiv 0 \quad (7)$? In altre parole, ci chiediamo se per certi valori di $k \in \mathbb{Z}$ può essere vera la congruenza

$$20 - 63k \equiv 0 \quad (7)$$

Ma, visto che stiamo lavorando modulo 7, e $-63k \equiv 0 \quad (7)$ questo equivale a chiedersi se è vera

$$20 \equiv 0 \quad (7)$$

e la risposta è NO.

Possono esistere soluzioni (x, y) con $x \equiv 0 \quad (13)$? Stavolta consideriamo

$$20 - 63k \equiv 0 \quad (13)$$

che si riscrive:

$$-63k \equiv -20 \quad (13)$$

$$63k \equiv 20 \quad (13)$$

$$11k \equiv 7 \quad (13)$$

Questa la si può considerare come una equazione con le congruenze con k come variabile; visto che $MCD(11, 13) = 1$ divide 7 sappiamo che tale equazione ha soluzione. Dunque possiamo rispondere che SÌ, possono esistere soluzioni (x, y) con $x \equiv 0 \quad (13)$.

Notiamo che l'esercizio non chiedeva di trovare le soluzioni, ma solo di dire se potevano esistere, motivando la risposta. Notiamo inoltre che a queste ultime due domande si

poteva rispondere anche prima di calcolare le soluzioni della equazione diofantea. La prima domanda, per esempio, equivale infatti alla seguente: ponendo $x = 7m$, l'equazione diofantea

$$40 \cdot 7\ m + 252y = 44$$

ha soluzione? Per rispondere basta controllare se il massimo comune divisore fra $40 \cdot 7 = 280$ e 252 divide o no 44... □

Esercizio 4.17. Trovare tutte le soluzioni intere dell'equazione

$$341x \equiv 15 \quad (912)$$

Esercizio 4.18. Trovare tutte le soluzioni della congruenza

$$18\ x \equiv 1 \quad (25)$$

Quante sono le soluzioni x con $-10 \leq x \leq 300$?

Esercizio 4.19. a) Trovare tutti i numeri interi che risolvono l'equazione

$$70x \equiv 222 \qquad (24)$$

b) Trovare tutti i numeri interi che risolvono l'equazione

$$(x+1)(x+2) \equiv 0 \qquad (24)$$

Esercizio 4.20. Trovare tutte le soluzioni della congruenza

$$12\ x \equiv 33 \quad (57)$$

Quante sono le soluzioni x con $-10 \leq x \leq 10$?

Esercizio 4.21. Trovare tutte le soluzioni della congruenza

$$1008\ x \equiv 12 \quad (11)$$

Esercizio 4.22. a) Trovare tutte le soluzioni della congruenza

$$546x \equiv 442 \qquad (260)$$

b) Trovare tutte le soluzioni della congruenza

$$7x \equiv -46 \qquad (58)$$

c) Trovare le soluzioni comuni alle due equazioni.

Esercizio 4.23. Trovare tutte le soluzioni della congruenza

$$44\ x \equiv 10 \quad (105)$$

Esercizio 4.24. Trovare per quali $b \in \mathbb{Z}$ e $m \in \mathbb{Z}^+$ si può risolvere la congruenza

$$2\ x \equiv b \quad (m)$$

Esercizio 4.25. a) Risolvere la congruenza

$$168x \equiv 3080 \quad (455)$$

b) Per quali valori del numero intero positivo m la congruenza

$$168x \equiv 1540 \quad (35m)$$

ammette soluzione ?

Esercizio 4.26. Trovare tutte le soluzioni della congruenza

$$420\ x \equiv 91 \quad (119)$$

Quante sono le soluzioni x con $-10 \leq x \leq 300$?

Esercizio 4.27. Trovare tutte le soluzioni della congruenza $42x \equiv 6 \bmod 110$ e stabilire il numero delle soluzioni nell'intervallo $[-1000, 2000]$.

Esercizio 4.28. Trovare tutte le soluzioni della congruenza $9x \equiv 3^{15} \bmod 17$.

Esercizio 4.29. Determinare per quali valori del parametro k la congruenza

$$-6x \equiv 20 \bmod 7k$$

ha soluzione e risolverla per $k = 8$.

Esercizio 4.30. a) Calcolare $MCD(3192, 117)$.
b) Trovare tutti gli $m \in \mathbb{Z}$ che soddisfano

$$3192\ m \equiv 288 \mod 117$$

e tali che $0 \leq m \leq 234$.

Esercizio 4.31. Dire se le seguenti proposizioni sono vere o false e motivare la risposta:

a) per tutti i numeri naturali positivi n, $7^n \equiv n^3 + 3n^2 + 2n + 1 \mod 5$.
b) Per tutti i numeri naturali positivi n, $7^n \equiv n^3 + 3n^2 + 2n + 1 \mod 3$.
c) Per tutti i numeri naturali positivi n, $7^n \geq n^3 + 3n^2 + 2n + 1$.

Esercizio 4.32. a) Trovare tutti gli interi x che soddisfano la congruenza:

$$1386x \equiv 1890 \quad (294)$$

b) Trovare tutti gli interi y che soddisfano la congruenza:

$$1386y^2 \equiv 1890 \quad (294)$$

Esercizio 4.33. a) Risolvere la congruenza

$$396x \equiv 234 \quad (1050)$$

b) Per quali valori dell'intero k la congruenza

$$396x \equiv 234 \quad (105 \cdot k)$$

ha soluzione?

Esercizio 4.34. a) Risolvere la congruenza

$$5920x \equiv 160 \quad (504)$$

b) Per quali valori del numero intero positivo m la congruenza

$$5920x \equiv 160 \quad (56m)$$

ammette soluzione ?

ESERCIZIO 4.35. a) Trovare l'insieme $S_1 \subseteq \mathbb{Z}$ delle soluzioni della congruenza lineare:

$$3315\ x \equiv 816 \qquad \text{mod } 952$$

b) Trovare l'insieme $S_2 \subseteq \mathbb{Z}$ delle soluzioni della congruenza lineare:

$$126x \equiv 42 \qquad \text{mod } 77$$

c) Descrivere $S_1 \cap S_2$

ESERCIZIO 4.36. Trovare tutte le soluzioni di

$$x^2 + 1 \equiv 0 \text{ mod } 65$$

ESERCIZIO 4.37. Dimostrare che, per ogni numero primo p esiste un numero naturale n tale che

$$6n^2 + 5n + 1 \equiv 0 \text{ mod } p$$

CAPITOLO 5

Lezione del 16 ottobre

1. Il piccolo teorema di Fermat

In questa sezione studieremo un importante teorema che riguarda le potenze dei numeri modulo un intero positivo m.

TEOREMA 5.1 (Il piccolo teorema di Fermat). *Se p è un numero primo e a è un numero intero che non è un multiplo di p, allora vale*

$$a^{p-1} \equiv 1 \quad (p)$$

OSSERVAZIONE 5.2. Sia $p = 7$. Il teorema ci garantisce che per ogni $a \in \mathbb{Z}$ che non sia multiplo di 7 vale:

$$a^6 \equiv 1 \quad (7).$$

Avvertiamo subito che può accadere che 6 non sia il più piccolo numero t tale che

$$a^t \equiv 1 \quad (7).$$

Per esempio per $a = 2$ troviamo:

$$2^3 \equiv 1 \quad (7)$$

Invece per $a = 3$ la più piccola potenza che dà un risultato congruo a 1 modulo 7 è effettivamente 6. Infatti le potenze di 3 modulo 7 sono le seguenti:

$$3^1 = 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1$$

Approfondiremo più avanti questa osservazione.

DIMOSTRAZIONE. Dato un intero $a \not\equiv 0 \quad (p)$ consideriamo i numeri

$$a, 2a, \ldots, (p-1)a$$

Questi $p-1$ numeri sono a due a due non congrui fra loro modulo p. Supponiamo infatti, per assurdo, che esistano i e j $(0 \leq i < j \leq p-1)$ tali che $ia \equiv ja \quad (p)$.

Ora sappiamo (per il Teorema 3.27) che a ammette un inverso modulo p. Sia dunque b un inverso di a. Moltiplicando per b otteniamo:

$$iab \equiv jab \quad (p)$$

ossia

$$i \equiv j \quad (p)$$

Poiché avevamo supposto $0 \leq i < j \leq p-1$ abbiamo trovato un assurdo.

Dunque la lista

$$a, 2a, \ldots, (p-1)a$$

comprende $p-1$ numeri i cui resti nella divisione per p sono tutti diversi da 0 e a due a due distinti. Allora i resti dei numeri $a, 2a, \ldots, (p-1)a$ sono esattamente, a meno di riordinarli, i numeri

$$1, 2, \ldots, (p-1)$$

Possiamo dunque scrivere che

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \qquad (p)$$

Questa congruenza, raccogliendo a sinistra i fattori uguali ad a, equivale alla seguente:

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \qquad (p)$$

Ora osserviamo che $p-1$ è invertibile modulo p (sempre per il Teorema 3.27), e moltiplichiamo entrambi i membri per un suo inverso. Otteniamo

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-2) \equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \qquad (p)$$

Poi moltiplichiamo entrambi i membri per un inverso di $p-2$, e così via..

Alla fine troviamo

$$a^{p-1} \equiv 1 \qquad (p)$$

come volevamo dimostrare. □

Diamo adesso una diversa dimostrazione del piccolo teorema di Fermat dovuta ad Eulero. Per un'altra dimostrazione, consultate anche il Paragrafo 8 del Capitolo 4 di [**DM**].

DIMOSTRAZIONE. Per prima cosa dimostriamo che p divide $\left(\begin{array}{c} p \\ i \end{array} \right)$ quando $0 < i < p$. Infatti sappiamo che

$$\left(\begin{array}{c} p \\ i \end{array} \right) i! \, (p-i)! = p!$$

e, per il teorema di decomposizione unica in prodotto di fattori primi, p, che divide il membro di destra, deve dividere il membro di sinistra. Poiché p non può dividere $i!$ $(p-i)!$ (che sono prodotti di numeri positivi strettamente minori di p) possiamo dedurre, per la proprietà caratterizzante dei numeri primi (ossia quella che dice che se p è primo e divide un prodotto ab allora p deve dividere a o p deve dividere b), che p deve dividere $\left(\begin{array}{c} p \\ i \end{array} \right)$.

A questo punto possiamo osservare che, dati due numeri interi a e b, lo sviluppo del binomio $(a+b)^p$ ha, modulo p, una scrittura molto semplificata. Infatti vale

$$(a+b)^p = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) a^i b^{p-i} \equiv a^p + b^p \qquad (p)$$

dato che, appunto, p divide tutti i coefficienti $\left(\begin{array}{c} p \\ i \end{array} \right)$ $(0 < i < p)$.

In particolare, nel caso $b = 1$, abbiamo

$$(a+1)^p \equiv a^p + 1 \qquad (p)$$

Ora proviamo che, per ogni $a \in \mathbb{Z}$ vale

$$a^p \equiv a \quad (p)$$

Questa relazione, nel caso in cui a non è multiplo di p, ci dà (dividendo per a) l'enunciato del teorema.

Ci basta dimostrare che, per ogni $a \in \mathbb{N}$,

$$a^p \equiv a \quad (p)$$

(il caso dei numeri negativi si ricava poi immediatamente).

Lo dimostriamo per induzione su a.

Il caso base, per $a = 0$,

$$0^p \equiv 0 \quad (p)$$

è banale.

Supponiamo ora che questa relazione sia vera fino ad $a = n$ e proviamo a dimostrare che

$$(n+1)^p \equiv n+1 \quad (p)$$

(se ci riusciamo la nostra dimostrazione è terminata).

Ora, per quanto visto sopra possiamo scrivere che

$$(n+1)^p \equiv n^p + 1 \quad (p)$$

Ma, per ipotesi induttiva, $n^p \equiv n \quad (p)$ per cui

$$(n+1)^p \equiv n+1 \quad (p)$$

□

Mostriamo nel seguente esempio una importante applicazione del piccolo teorema di Fermat al calcolo veloce di potenze modulo un numero primo.

Esempio 5.3. Se vogliamo calcolare

$$15^{1443} \equiv ? \quad (17)$$

possiamo utilizzare il piccolo teorema di Fermat che ci dice che

$$15^{16} \equiv 1 \quad (17)$$

Ora $1443 = 16 \cdot 90 + 3$ dunque

$$15^{1443} \equiv (15^{16})^{90}\, 15^3 \equiv 1^{90}\, 15^3 \quad (17)$$

Ma $15 \equiv -2 \quad (17)$ dunque

$$15^{1453} \equiv (-2)^3 \equiv -8 \equiv 9 \quad (17)$$

Esempio 5.4. Attenzione, se il modulo non è primo, l'enunciato del piccolo teorema di Fermat non vale più: non è vero, per esempio, che $2^5 \equiv 1 \quad (6)$. Infatti

$$2^5 = 32 \equiv 2 \quad (6)$$

Dal piccolo teorema di Fermat si ricava subito questo corollario:

Corollario 5.5. *Se p è un numero primo, per ogni numero intero a vale*

$$a^p \equiv a \quad (p)$$

Dimostrazione. Se a non è multiplo di p per il piccolo teorema di Fermat vale

$$a^{p-1} \equiv 1 \quad (p)$$

da cui si ottiene la tesi moltiplicando per a entrambi i membri. È poi immediato verificare che se $a \equiv 0 \quad (p)$ allora la tesi è vera.

□

Questo ci dà un criterio per decidere se un numero non è primo:

Corollario 5.6. *Se $n > 1$ è un numero intero tale che per qualche numero intero a vale*

$$a^n \not\equiv a \quad (n)$$

allora n non è primo.

DIMOSTRAZIONE. Si tratta della contronominale del corollario precedente. □

È interessante capire se con questi ragionamenti si può trovare un criterio per dire con certezza se un numero è primo (non solo per dire se un numero NON è primo). Saremmo infatti tentati di pensare che se prendiamo un numero intero $n > 1$ e scopriamo che per tutti i numeri interi a vale

$$a^n \equiv a \quad (n)$$

allora n è primo. Questo non è vero: ci sono infiniti numeri che soddisfano questa proprietà ma non sono primi. Si chiamano *numeri di Carmichael*[1] o *falsi primi*.

ESERCIZIO 5.7. Dimostrare che 561 è un numero di Carmichael (è il più piccolo esistente).

ESERCIZIO 5.8. Dimostrare che 1105 e 1729 sono numeri di Carmichael (sono il secondo e il terzo nella lista dei numeri di Carmichael).

2. Un interessante risvolto applicativo: il metodo di crittografia RSA

Consideriamo due numeri primi distinti p e q, e prendiamo un numero e che sia primo con $(p-1)(q-1)$. Sappiamo dunque che e è invertibile modulo $(p-1)(q-1)$, e chiamiamo d un suo inverso.

La seguente semplice proposizione è il cuore del metodo di crittografia che vogliamo descrivere:

PROPOSIZIONE 5.9. *Dati p, q, e, d come sopra, per ogni numero m con $0 \leq m < pq$ vale*

$$(m^e)^d \equiv m \quad (pq)$$

DIMOSTRAZIONE. Osserviamo che per il teorema cinese del resto l'equazione

$$x \equiv m \quad (pq)$$

è equivalente al sistema

$$\begin{cases} x \equiv m & (p) \\ x \equiv m & (q) \end{cases}$$

Dunque ci basta dimostrare che $(m^e)^d$ è una soluzione del sistema.

Verifichiamo che $(m^e)^d$ è soluzione della prima equazione (per la seconda equazione si procederà in maniera del tutto analoga), ossia verifichiamo che è vera la congruenza:

$$(m^e)^d \equiv m \quad (p)$$

Ora, se $p|m$ la congruenza appena scritta diventa $0 \equiv 0 \quad (p)$ che è vera.

Se invece $p \nmid m$ allora possiamo applicare il piccolo teorema di Fermat. Infatti per costruzione

$$ed \equiv 1 \qquad ((p-1)(q-1))$$

dunque possiamo scrivere

$$ed = 1 + k(p-1)(q-1)$$

per un certo intero k.

Allora

$$(m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1^{k(q-1)} \equiv m \quad (p)$$

dove abbiamo usato il piccolo teorema di Fermat per dire che $m^{p-1} \equiv 1 \quad (p)$.

□

[1] Robert Carmichael, matematico americano,1878-1967.

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman inventarono un metodo (detto RSA dalle iniziali dei loro cognomi) per scambiarsi messaggi criptati il cui funzionamento può essere schematicamente riassunto nel seguente modo.[2]

Supponiamo che A voglia inviare un messaggio segreto a B (non occorre pensare a chissà quali contesti di spionaggio e controspionaggio, A per esempio potremmo essere noi mentre digitiamo il codice della nostra carta di credito per fare un acquisto online).

Innanzitutto B ha scelto due numeri primi distinti p e q molto grandi (attualmente si scelgono numeri di circa trecento cifre: osserviamo che la ricerca di numeri primi grandi è un problema matematico di per sé interessante, che ha dunque anche una importante applicazione).

Visto che conosce p e q, B conosce anche $p-1$ e $q-1$ e può dunque facilmente scegliere e e d con le caratteristiche illustrate in questo paragrafo.

A questo punto B consegna ad A i numeri pq ed e. Anzi, li può addirittura rendere pubblici, in modo che altri possano inviargli messaggi crittati, non solo A.

Quando A vuole inviare un messaggio, questo messaggio può essere facilmente codificato da un numero m con $0 < m < pq$ (se è un messaggio numerico è già un numero, se è un messaggio con lettere, si può certo trovare un modo di associare ad ogni lettera un numero, dunque il messaggio finale risulterà un numero m, magari molto grande, ottenuto scrivendo uno accanto all'altro tutti i numeri che rappresentano le lettere).[3]

A questo punto A non invia il numero m, ma calcola m^e modulo pq e invia dunque un numero c con $0 < c < pq$ e $c \equiv m^e \pmod{pq}$.

Dunque B riceve il messaggio c. Per decodificarlo calcolerà c^d modulo pq e, per la Proposizione 5.9, ritroverà il messaggio originale m.

Come mai questo sistema è efficace? Ricordiamo che solo B conosce il numero d, e il punto è proprio questo. Il numero d è stato ricavato da e e dalla conoscenza dei numeri $p-1$ e $q-1$, mentre sono pubblici solo i numeri e e il **prodotto** pq. Per ricavare $p-1$ e $q-1$ conoscendo il prodotto pq bisognerebbe saper fattorizzare pq, e questa è una operazione che, al giorno d'oggi, con numeri così grandi, non è possibile eseguire in tempo utile. E non esiste per il momento neppure nessun altro metodo che permetta, dato un numero c che sappiamo essere congruo modulo pq ad una potenza e-esima di un certo numero ignoto, di ritrovare in tempo utile questo numero ignoto.[4]

Nelle poche righe precedenti abbiamo descritto in maniera schematica il metodo RSA, senza discutere le molte accortezze tecniche che occorre usare nella pratica, che non competono a questo corso ma ad un corso di crittografia. Ad ogni modo, una volta che viene applicato con tutte le accortezze del caso, il metodo RSA è ritenuto molto affidabile.

Abbiamo fatto solo un primo accenno alle complesse problematiche della crittografia, ma per voi che intraprendete la carriera di matematici può essere interessante sapere che un teorema di aritmetica elementare, semplice ma profondo, come il piccolo teorema di Fermat, ha ripercussioni applicative così importanti.

---

[2]Per coloro che sono interessati ad una introduzione divulgativa (non tecnica) alla storia della crittografia fin dalle origini, segnalo il libro di S. Singh *Codici e Segreti*.

[3]Ricordiamo che pq è molto grande, dunque c'è spazio per codificare anche messaggi molto lunghi. Altrimenti A dovrà spezzare il suo messaggio e inviare vari numeri m_1, m_2 etc...

[4]Se siete curiosi potete dare un'occhiata all'articolo di Rivest e Kaliski *RSA problem*, https://people.csail.mit.edu/rivest/RivestKaliski-RSAProblem.pdf

3. Le classi di resto modulo un intero positivo. Struttura additiva e moltiplicativa.

Cominciamo con un esempio. Consideriamo i possibili resti della divisione euclidea di un numero intero per 10. Abbiamo 10 possibilità: resto uguale a 0,1,2,3,. . . , 9. Quali sono i numeri che danno resto 1? Eccone alcuni: 1,11,21,31,. . . ....-9,-19,-29,-39, -49. . .

Chiamiamo $[1]_{10}$ l'insieme costituito da questi numeri:

$$[1]_{10} = \{x \in \mathbb{Z} \mid x \equiv 1 \quad (10)\}$$

Analogamente, chiamiamo $[2]_{10}$ l'insieme dei numeri interi la cui divisione per 10 dà resto 2, e in generale, per $i = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, chiamiamo $[i]_{10}$ l'insieme dei numeri interi la cui divisione per 10 dà resto i.

Gli insiemi $[0]_{10}$, $[1]_{10}$, $[2]_{10}$,. . . , $[9]_{10}$ si chiamano "classi di resto modulo 10"; la loro unione è uguale a tutto $\mathbb{Z}$ giacché ogni numero intero appartiene ad una (e ad una sola) delle classi. Chiamiamo ora $\mathbb{Z}_{10}$ l'insieme i cui elementi sono tutte le classi di resto modulo 10:

$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, \ldots, [9]_{10}\}$$

Possiamo arricchire questo insieme definendo due operazioni, una somma e una moltiplicazione.

Prima estendiamo la nostra notazione: fin qui per esempio non abbiamo definito il simbolo $[11]_{10}$. Infatti abbiamo preso in considerazione solo simboli in cui fra le parentesi quadre c'è un resto 0,1,. . . , 9 di una divisione euclidea per 10. Decidiamo di accettare anche $[11]_{10}$ intendendo che $[11]_{10} = [1]_{10}$. E anche, per esempio, $[127]_{10} = [7]_{10}$. Insomma ci mettiamo d'accordo di poter indicare una classe di resto $[i]_{10}$ anche col simbolo $[s]_{10}$ dove s è un qualunque numero intero tale che

$$s \equiv i \quad (10)$$

Ora siamo pronti a definire la somma e la moltiplicazione di elementi di $\mathbb{Z}_{10}$. Poniamo:

$$[a]_{10} \cdot [b]_{10} = [ab]_{10}$$

$$[a]_{10} + [b]_{10} = [a + b]_{10}$$

Per esempio:

$$[7]_{10} \cdot [5]_{10} = [35]_{10} = [5]_{10}$$

$$[6]_{10} + [8]_{10} = [14]_{10} = [4]_{10}$$

Insomma in $\mathbb{Z}_{10}$ "sette" per "cinque" fa "cinque" e "sei" più "otto" fa "quattro".

In realtà, per essere sicuri di aver definito una buona somma e una buona moltiplicazione, bisogna verificare che, se

$$[a]_{10} = [a']_{10}$$

$$[b]_{10} = [b']_{10}$$

allora

$$[a]_{10} \cdot [b]_{10} = [a']_{10} \cdot [b']_{10}$$

$$[a]_{10} + [b]_{10} = [a']_{10} + [b']_{10}$$

insomma che queste operazioni non dipendono dai numeri a e b che mettiamo fra parentesi quadre ma solo dalle loro classi di resto.

ESERCIZIO 5.10. Fate questa verifica. (Suggerimento: visto che $[a]_{10} = [a']_{10}$ allora sarà $a' = a+10k$ e analogamente $b' = b+10t$. Dunque per esempio, per quel che riguarda la moltiplicazione, vale $[a']_{10} \cdot [b']_{10} = [(a+10k)(b+10t)]_{10} = [ab+10bk+10at+100kt]_{10} = [ab]_{10} = [a]_{10}[b]_{10}$.)

Con queste operazioni l'insieme $\mathbb{Z}_{10}$ diventa un "anello commutativo con unità". Discuteremo la definizione formale di anello (anche se la avete già vista a Geometria 1) in uno dei prossimi capitoli.

Intanto osserviamo che la somma e la moltiplicazione che abbiamo definito hanno molte delle buone proprietà a cui "siamo abituati" dalla moltiplicazione e dalla somma in $\mathbb{Z}$ (proprietà commutativa e associativa di entrambe le operazioni, proprietà distributive, esistenza dell'elemento neutro per entrambe operazioni, esistenza dell'opposto rispetto alla somma..).

C'è però una cosa nuova in $\mathbb{Z}_{10}$, rispetto a $\mathbb{Z}$. Vale infatti

$$[2]_{10} \cdot [5]_{10} = [10]_{10} = [0]_{10}$$

ossia il prodotto di due elementi diversi da $[0]_{10}$ ha come risultato $[0]_{10}$ (mentre in $\mathbb{Z}$ il prodotto di due interi diversi da zero è sempre diverso da 0). Si dice a questo proposito che $[2]_{10}$ e $[5]_{10}$ sono due *divisori dello zero* in $\mathbb{Z}_{10}$.

Passiamo al caso generale. Sia m un numero intero positivo.
Per ogni $i = 0, 1, 2, \ldots, m-1$ chiamiamo $[i]_m$ la "classe di resto di i modulo m", ossia l'insieme dei numeri che danno resto i quando si considera la loro divisione euclidea per m:

$$[i]_m = \{x \in \mathbb{Z} \mid x \equiv i \pmod{m}\}$$

Come nell'esempio in cui $m = 10$, osserviamo che l'unione di tutte le classi di resto modulo m dà tutto $\mathbb{Z}$.
Chiamiamo $\mathbb{Z}_m$ l'insieme di tutte le classi di resto modulo m:[5]

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Si tratta dunque un insieme di cardinalità m.

Come sopra adottiamo la convenzione per cui possiamo indicare la classe $[i]_m$ anche col simbolo $[s]_m$ dove s è un qualunque numero intero tale che

$$s \equiv i \pmod{m}$$

Per esempio, con $m = 37$:

$$[5]_{37} = [42]_{37} = [412]_{37}$$

Possiamo allora definire la somma e la moltiplicazione di elementi di $\mathbb{Z}_m$:

$$[a]_m \cdot [b]_m = [ab]_m$$

$$[a]_m + [b]_m = [a+b]_m$$

Anche questa volta si verifica (fate di nuovo il facile esercizio!) che queste operazioni sono ben definite e che non dipendono dai numeri a e b ma solo delle loro classi di resto, e $\mathbb{Z}_m$ risulterà un anello commutativo con unità.

[5] In vari testi, come [**DM**], trovate questo insieme indicato con il simbolo $\mathbb{Z}/m\mathbb{Z}$.

4. Esercizi

ESERCIZIO 5.11. a) Trovare il numero naturale m tale che $0 \leq m < 13$ e

$$[2^{(2^{10})}]_{13} = [m]_{13}$$

b) Trovare il numero naturale k tale che $0 \leq k < 3$ e

$$[(138139140141 \ldots 999)^{1987} - 1]_3 = [k]_3$$

ESERCIZIO 5.12. Consideriamo la funzione $g : \mathbb{Z}_5 \times \mathbb{Z}_5 \to \mathbb{Z}_5 \times \mathbb{Z}_5$ che è definita dalla seguente relazione:

$$\forall\, [a],\ [b] \in \mathbb{Z}_5, \quad g(([a],[b])) = ([a-3b],[a+3b])$$

Dire se g è iniettiva, surgettiva, bigettiva.

ESERCIZIO 5.13. a) Trovare l'insieme delle soluzioni della congruenza lineare:

$$327\ x \equiv 416 \qquad \mod (52)$$

b) Dire se la funzione $f : \mathbb{Z}_{52} \to \mathbb{Z}_{52}$ data da

$$f([x]) = [15x]$$

è iniettiva, surgettiva, bigettiva.

ESERCIZIO 5.14 (Teorema di Wilson[6]). Dimostrare che, se p è primo, vale

$$(p-1)! \equiv -1 \qquad (p)$$

Se invece m è un numero non primo, la congruenza

$$(m-1)! \equiv -1 \qquad (m)$$

è vera o falsa?

ESERCIZIO 5.15. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$, $17^{16^n} \equiv 4 \mod 7$.

ESERCIZIO 5.16. a) Quante sono tutte le possibili funzioni $f : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$?
b) Quanti sono gli elementi invertibili di $\mathbb{Z}_{15}$? E quelli invertibili di $\mathbb{Z}_{20}$?
c) Quante sono le funzioni $g : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$ che mandano elementi invertibili di $\mathbb{Z}_{15}$ in elementi invertibili di $\mathbb{Z}_{20}$?
d) Quante sono le funzioni iniettive $h : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$ che mandano elementi invertibili di Z_{15} in elementi invertibili di $\mathbb{Z}_{20}$?

ESERCIZIO 5.17. Dimostrare che esiste un multiplo di 174 nella cui scrittura decimale appare solo la cifra 6.

[Traccia: $174 = 6 \cdot 29$. C'è un n tale che il numero 66666...66 (il 6 compare n volte) sia divisibile per 174 ? Basta scoprire quando il numero 11111...11 (l'1 compare n volte) è divisibile per 29. Ora, $11111...11 = 1 + 10 + 10^2 + \cdots + 10^{n-1} = \frac{10^n-1}{10-1}$...]

ESERCIZIO 5.18. Qual è l'ultima cifra del numero 3^{13452} scritto in base 10? E del numero 6^{245389}?

ESERCIZIO 5.19. Dimostrare che, per ogni numero naturale n, $n(n^6 - 1)$ è divisibile per 42.

ESERCIZIO 5.20. Dimostrare che, per ogni intero positivo n, $2^{3n+3} - 7n - 8$ è divisibile per 49.

[6]John Wilson, matematico inglese, 1741-1793.

Esercizio 5.21. Dimostrare che non esiste nessuna funzione $f : \mathbb{N} \to \mathbb{N}$ tale che, per ogni $n \in \mathbb{N}$

$$f(f(n)) = n + 2015$$

Esiste una simile funzione se nella formula precedente si sostituisce 2015 con 2016 ?

CAPITOLO 6

Lezione del 23 ottobre

1. Gruppi e sottogruppi: prime proprietà

Cominciamo subito scrivendo la definizione formale di gruppo (la avete in realtà già vista a Geometria 1).

DEFINIZIONE 6.1. Un *gruppo* G è un insieme non vuoto dotato di una operazione che ad ogni coppia di elementi $a, b \in G$ associa un elemento di G indicato con $a \cdot b$ e ha le seguenti proprietà:

(1) dati $a, b, c \in G$ vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (proprietà associativa);
(2) esiste un elemento $e \in G$ tale che $a \cdot e = e \cdot a = a$ per ogni $a \in G$ (esistenza dell'elemento neutro, detto anche identità, in G);
(3) per ogni $a \in G$ esiste un elemento $a^{-1} \in G$ tale che $a \cdot a^{-1} = a^{-1} \cdot a = e$ (esistenza dell'inverso in G).

Un gruppo si dice *commutativo* o *abeliano*[1] se, per ogni $a, b \in G$ vale $a \cdot b = b \cdot a$. Un gruppo G si dice finito se l'insieme G ha cardinalità finita.

ESEMPIO 6.2. Ecco due esempi di gruppi non commutativi.

Consideriamo un insieme con n elementi X. L'insieme $Bij(X, X)$ delle funzioni bigettive da X in X è un gruppo con $n!$ elementi, chiamato S_n, con l'operazione data dalla composizione fra funzioni. Fate fin d'ora la verifica che S_n è un gruppo, e dimostrate anche che non è commutativo se $n \geq 3$. Studieremo più avanti S_n in maniera più approfondita.

Se considerate l'insieme $Mat_{n\times n}(K)^*$ delle matrici $n \times n$ *invertibili* a coefficienti in un campo K, noterete che $Mat_{n\times n}(K)^*$ è un gruppo rispetto all'operazione di prodotto fra matrici. Anche in questo caso si tratta di un gruppo non commutativo (se $n \geq 2$).

ESEMPIO 6.3. Ecco altri esempi, e controesempi, familiari.

L'insieme $\mathbb{Z}$ considerato con l'operazione $+$ è un gruppo commutativo infinito; rispetto alla moltiplicazione, invece, non è un gruppo perché solo gli elementi 1 e -1 hanno un inverso. L'insieme $\mathbb{N}$ non è un gruppo né con l'addizione né con la moltiplicazione. I campi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sono gruppi commutativi rispetto all'addizione, mentre gli insiemi $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$,$\mathbb{C}-\{0\}$ sono gruppi commutativi rispetto alla moltiplicazione.

Ogni spazio vettoriale V è un gruppo commutativo rispetto alla addizione.

D'ora in avanti, quando parleremo di un gruppo, ometteremo, tutte le volte che sarà possibile farlo senza creare ambiguità, il simbolo $\cdot$ per la moltiplicazione; scriveremo dunque ab invece di $a \cdot b$, $a^2 = aa$ invece di $a \cdot a$. Inoltre nel fare il prodotto fra n elementi del gruppo scriveremo spesso $a_1 \cdot a_2 \cdots a_n$ omettendo le parentesi, visto che vale la proprietà associativa (una facile induzione su n ci mostra che il risultato del prodotto non dipende da come erano collocate le parentesi).

[1] In onore di Niels Henrik Abel, matematico norvegese, 1802-1829.

Il seguente teorema, semplice ma importante, mette in luce alcune prime proprietà dei gruppi che derivano immediatamente dalla definizione.

TEOREMA 6.4. *Dimostrare che, se G è un gruppo, allora*

(1) *C'è un solo elemento neutro e.*
(2) *Per ogni $a \in G$ c'è un unico inverso di a.*
(3) *Per ogni $a \in G$ vale $(a^{-1})^{-1} = a$.*
(4) *Per ogni $a, b \in G$ vale $(ab)^{-1} = b^{-1}a^{-1}$.*
(5) *Siano a, b, c elementi di G. Allora l'equazione $axb = c$ ha un'unica soluzione $x = a^{-1}cb^{-1}$ in G.*

DIMOSTRAZIONE.
(1) Supponiamo che ci siano due elementi neutri e ed e'. Allora possiamo scrivere, che $e = ee' = e'$ dove per il primo $=$ abbiamo sfruttato la proprietà di elemento neutro di e' (abbiamo infatti moltiplicato a destra per e') e per il secondo $=$ abbiamo sfruttato la proprietà di elemento neutro di e (abbiamo moltiplicato e' a sinistra per e).
(2) Siano h e k due inversi di a. Allora

$$h = he = h(ak) = (ha)k = ek = k$$

(3) Osserviamo che $(g^{-1})^{-1}g^{-1} = g^{-1}(g^{-1})^{-1} = e$ per definizione di $(g^{-1})^{-1}$. Ma sappiamo anche che $gg^{-1} = g^{-1}g = e$ per definizione di g^{-1}. Dunque osserviamo che sia g sia $(g^{-1})^{-1}$ sono inversi di g^{-1}. Per l'unicitàà dell'inverso stabilita nel punto (2) possiamo concludere che $g = (g^{-1})^{-1}$.
(4) Basta verificare che $b^{-1}a^{-1}$ è un inverso di ab. Lo faremo moltiplicandolo a sinistra (la dimostrazione moltiplicandolo a destra è analoga).

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$$

dove abbiamo usato in maniera sostanziale la proprietà associativa.
(5) Un elemento $\overline{x}$ soddisfa l'equazione $axb = c$ se e solo se vale $a\overline{x}b = c$. Questa uguaglianza è vera se e solo se è vera $\overline{x}b = a^{-1}c$, come si vede moltiplicando ognuno dei due membri, a sinistra, per a^{-1}. Moltiplicando ognuno dei due membri, a destra, per b^{-1} si vede che questa uguaglianza a sua volta è vera se e solo se è vera $\overline{x} = a^{-1}cb^{-1}$. Dunque le soluzioni della equazione $axb = c$ coincidono con le soluzioni della equazione $x = a^{-1}cb^{-1}$, che, come si vede, sono una sola, ossia $a^{-1}cb^{-1}$.

□

Fra i sottoinsiemi di G rivestono un ruolo particolare quelli che, rispetto all'operazione $\cdot$, sono a loro volta dei gruppi:

DEFINIZIONE 6.5. Un *sottogruppo* H di un gruppo G è un sottoinsieme di G che soddisfa le tre seguenti proprietà:

(1) $e \in H$
(2) $a, b \in H \Rightarrow ab \in H$
(3) $a \in H \Rightarrow a^{-1} \in H$

Per indicare che H è un sottogruppo di G si scrive $H < G$.

OSSERVAZIONE 6.6. In particolare, fra i sottogruppi di un gruppo G ci sono sempre G stesso e il sottogruppo banale $\{e\}$.

Indichiamo subito un importante sottogruppo:

DEFINIZIONE 6.7 (Centro di un gruppo). Dato un gruppo G si chiama *centro* di G il sottoinsieme formato dagli elementi che commutano con tutti gli elementi del gruppo:

$$Z(G) = \{g \in G \mid gh = hg \quad \forall h \in G\}$$

ESERCIZIO 6.8. Dimostrare che $Z(G)$ è un sottogruppo di G.

Si osserva subito che se il gruppo G è abeliano allora $Z(G) = G$.

ESEMPIO 6.9. Sia a un elemento di un gruppo G. Consideriamo il sottoinsieme di G

$$(a) = \{a^i \mid i \in \mathbb{Z}\}$$

Spieghiamo bene la notazione. Se $s > 0$ con a^s si intende, come immaginate, il prodotto di a per se stesso s volte. Poi si pone $a^0 = e$. Inoltre se $i > 0$ e scriviamo a^{-i} intendiamo $(a^{-1})^i$. Per il punto (4) del Teorema 6.4 questo è uguale a $(a^i)^{-1}$ (per esempio $a^{-2} = a^{-1}a^{-1} = (a^2)^{-1}$). Il sottoinsieme (a) è un sottogruppo di G e si chiama *sottogruppo ciclico generato da* a.

I sottogruppi ciclici di $\mathbb{Z}$ (con l'operazione $+$) sono, al variare di $m \in \mathbb{Z}$, i sottogruppi

$$(m) = \{km \mid k \in \mathbb{Z}\}$$

che coincidono, usando la notazione della scorsa lezione, con le classi di resto $[0]_m$.

DEFINIZIONE 6.10. Se, per qualche $a \in G$ vale $G = (a)$ allora si dice che G è un *gruppo ciclico*.

2. Laterali destri di un sottogruppo. Il Teorema di Lagrange. Ordine di un elemento

DEFINIZIONE 6.11. Sia G un gruppo, H un sottogruppo di G. Chiameremo *H-laterale destro*, o *laterale destro di H*, o *classe laterale destra di H*, un sottoinsieme di G del tipo:

$$gH = \{gh \mid h \in H\}$$

dove $g \in G$.

L'insieme i cui elementi sono gli H-laterali destri si indica con G/H e la sua cardinalità $|G/H|$ si chiama *indice* di H in G.

In particolare osserviamo che $eH = H$ ossia H è un particolare H-laterale destro. A parte questo caso, i laterali destri di H non sono sottogruppi (come potete facilmente verificare nel caso in cui $G = \mathbb{Z}$ con l'operazione $+$ e $H = (m)$ per un certo intero positivo m), ma solo sottoinsiemi di G.

Gli H laterali destri forniscono però una partizione di G, ossia G è unione disgiunta dei suoi laterali destri, come mostra la seguente:

TEOREMA 6.12. *Ogni elemento w di G è contenuto in uno e un solo H-laterale destro: wH.*

DIMOSTRAZIONE. Osserviamo subito che $w \in wH$ visto che $e \in H$ e allora $w = we \in wH$. Supponiamo ora che w appartenga anche al laterale γH, dove $\gamma \in G$. Allora $w = \gamma h_1$ per un certo $h_1 \in H$. Ora osserviamo che il laterale wH e il laterale γH coincidono. Infatti:

$$\gamma H = \{\gamma h \mid h \in H\} = \{\gamma h_1 h \mid h \in H\} = \{wh \mid h \in H\} = wH$$

Il secondo $=$, quello in blu, va spiegato bene. Il punto è che, al variare di h, gli elementi $h_1 h$ descrivono tutti gli elementi del gruppo H: infatti ogni elemento h_2 appartenente ad H può essere ottenuto come $h_1(h_1^{-1}h_2)$, dove $h_1^{-1}h_2$ appartiene ad H visto che H è un sottogruppo. □

OSSERVAZIONE 6.13. Illustriamo la proposizione precedente nel caso in cui $G = \mathbb{Z}$ con l'operazione $+$ e $H = (12)$. Il numero 5 appartiene al laterale $5 + (12)$ che, se ci si pensa, è l'insieme che nella lezione scorsa abbiamo chiamato $[5]_{12}$, la classe (laterale) di resto di 5 modulo 12. Ora 5 appartiene anche al laterale $17 + (12)$ ma si verifica subito che i laterali $5 + (12)$ e $17 + (12)$ coincidono (questo è in accordo con la convenzione che avevamo scelto per cui $[5]_{12} = [17]_{12}$).

In conclusione abbiamo una partizione di $\mathbb{Z}$ in unione disgiunta delle seguenti classi laterali:

$$[0]_{12}, [1]_{12}, [2]_{12}, \ldots, [10]_{12}, [11]_{12}$$

Segue dal precedente teorema che due laterali gH e bH o sono disgiunti o coincidono. Il seguente corollario illustra la situazione:

COROLLARIO 6.14. *Dato un laterale gH, si consideri un laterale bH. Allora bH coincide con gH se e solo se $b \in gH$. Altrimenti i due laterali sono disgiunti.*

DIMOSTRAZIONE. Se $b \in gH$ allora c'è un elemento in comune fra i due laterali. Dunque poiché sappiamo dal Teorema 6.12 che ogni elemento appartiene ad un solo laterale, questo vuol dire che $gH = bH$. Viceversa, se $bH = gH$ allora è immediato concludere che $b \in bH = gH$. □

Svolgete anche l'Esercizio 6.37 che presenta i laterali come classi di equivalenza rispetto ad una relazione.

La partizione di G in unione disgiunta di classi laterali rispetto ad un sottogruppo H ha una importante conseguenza per quel che riguarda le cardinalità, nel caso in cui G sia finito:

TEOREMA 6.15 (Teorema di Lagrange[2]). *Se G è un gruppo finito e H è un sottogruppo di G allora $|H|$ divide $|G|$.*

DIMOSTRAZIONE. Visto che G è finito, G è l'unione disgiunta di un numero finito, diciamo n_H, di laterali destri di H. Se dimostriamo che ogni laterale ha cardinalità esattamente $|H|$ allora risulta $|G| = n_H\ |H|$ e dunque $|H|$ divide $|G|$.

Contiamo allora quanti elementi ha il laterale gH, per un qualunque $g \in G$. Visto che gli elementi della forma gh ottenuti al variare di $h \in H$ sono tutti diversi fra loro (se vale $gh_1 = gh_2$ allora moltiplicando a sinistra per g^{-1} abbiamo $h_1 = h_2$), vale che $|gH| = |H|$. □

Segnaliamo subito un importante corollario del Teorema di Lagrange.

DEFINIZIONE 6.16. Dato un elemento x di un gruppo G, se esiste un minimo intero positivo n tale che $x^n = e$ allora n si indica con $o(x)$ e si chiama *ordine* di x. Se un tale n non esiste allora si dice che x ha ordine infinito e si scrive $o(x) = \infty$.

COROLLARIO 6.17. *In un gruppo finito G, ogni elemento x ha ordine finito e tale ordine $o(x)$ divide $|G|$.*

DIMOSTRAZIONE. Consideriamo le potenze positive di x di G: $x, x^2, \cdots, x^k, \ldots$. In questa lista ad un certo punto deve comparire e. Infatti, se $x = e$ non c'è nulla da dimostrare. Se $x \neq e$, visto che le potenze sono infinite ma gli elementi del gruppo sono finiti, ad un certo punto deve valere $x^i = x^j$ con $1 \leq i < j$. Allora, moltiplicando per l'inverso di x^i, si ottiene $x^{j-i} = e$.

[2]Joseph-Louis Lagrange, nato Giuseppe Lodovico Lagrangia, matematico italiano, 1736-1813.

Sia ora $o(x)$, come abbiamo definito sopra, il più piccolo n per cui $x^n = e$ e consideriamo gli elementi

$$\{e, x, x^2, \ldots, x^{o(x)-1}\}$$

Tali elementi sono tutti distinti: se fosse $x^i = x^j$ con $1 \leq i < j \leq o(x)$ allora varrebbe $x^{j-i} = e$ ma questo non è possibile perché $j - i < o(x)$.

Inoltre osserviamo che $\{e, x, x^2, \ldots, x^{o(x)-1}\}$ coincide con il sottogruppo ciclico (x) generato da x (infatti si nota che $x^{-1} = x^{o(x)-1}$, $x^{-2} = x^{o(x)-2}$ etc...e si verifica subito che tutte le potenze di x e di x^{-1} sono presenti nella lista, visto che si ripetono ciclicamente).

Dunque la cardinalità del sottogruppo (x) è uguale a $o(x)$, e dal Teorema di Lagrange si ricava che $o(x)$ divide $|G|$.

□

Corollario 6.18. *Se x è un elemento di un gruppo finito G vale*

$$x^{|G|} = e.$$

Dimostrazione. Infatti per il corollario precedente possiamo scrivere $|G| = k \cdot o(x)$ per un certo intero k. Da questo segue che

$$x^{|G|} = x^{k \cdot o(x)} = (x^{o(x)})^k = e^k = e$$

□

3. Una prima applicazione: la funzione di Eulero e il Teorema di Eulero.

Il Teorema di Lagrange e il Corollario 6.17 hanno una immediata applicazione aritmetica. Fissato un numero intero positivo m, consideriamo infatti l'anello $\mathbb{Z}_m$. È immediato verificare che gli elementi invertibili di $\mathbb{Z}_m$ costituiscono un gruppo *rispetto alla moltiplicazione*. Tale gruppo viene indicato con la notazione $\mathbb{Z}_m^*$.

Esempio 6.19. Se p è un numero primo, $\mathbb{Z}_p^*$ ha $p-1$ elementi, visto che tutte le classi (eccetto la [0]) sono invertibili.

Il gruppo Z_{10}^* ha 4 elementi: [1],[3],[7],[9].

Il gruppo Z_{15}^* ha 8 elementi: [1], [2], [4], [7], [8], [11], [13], [14].

Definizione 6.20. *La funzione ϕ di Eulero* è la funzione $\phi : \mathbb{N}^{>0} \to \mathbb{N}^{>0}$ definita ponendo $\phi(1) = 1$ e, per $n > 1$,

$$\phi(n) = \text{numero degli interi positivi minori di } n \text{ e primi con } n$$

Dunque la cardinalità di $\mathbb{Z}_m^*$ è uguale a $\phi(m)$. Questo ci permette già di enunciare un teorema che generalizza il piccolo teorema di Fermat:

Teorema 6.21. *Fissato un intero positivo m, se a è un intero primo con m vale:*

$$a^{\phi(m)} \equiv 1 \bmod m$$

Dimostrazione. Visto che a ed m sono coprimi, sappiamo che $[a]$ appartiene a $\mathbb{Z}_m^*$. Per il Corollario 6.18 in $\mathbb{Z}_m^*$ vale

$$[a]^{\phi(m)} = [1]$$

che equivale a

$$a^{\phi(m)} \equiv 1 \bmod m$$

□

Osservazione 6.22. Se $m = p$ è primo ritroviamo l'enunciato del piccolo teorema di Fermat, visto che $\phi(p) = p - 1$ (abbiamo dunque dato, tramite il Teorema di Lagrange, un'altra dimostrazione del piccolo teorema di Fermat). In questo caso, come vedremo più avanti, vale anche che $\mathbb{Z}_p^*$ è un gruppo ciclico, ossia esiste un elemento in $\mathbb{Z}_p^*$ di ordine esattamente $p - 1$.

Osservazione 6.23. Avremmo potuto dimostrare il Teorema 6.21 anche imitando la dimostrazione del piccolo teorema di Fermat nel caso dei gruppi abeliani finiti, come suggerito dall'Esercizio 6.32. Ma abbiamo preferito introdurre subito il Teorema di Lagrange, che ha valore più generale, e i laterali, che avranno anch'essi grande importanza in seguito.

Alla luce di questo teorema, risulta importante saper calcolare in modo efficiente i valori della funzione ϕ che, al momento, è definita in maniera un po' implicita.

Proposizione 6.24. *Se b e c sono due numeri primi tra loro*

$$\phi(bc) = \phi(b)\phi(c)$$

Dimostrazione. Facciamo una breve osservazione preliminare: dati tre numeri interi s, t, m, con $m > 0$, tali che $s \equiv t \pmod{m}$, allora s è coprimo con m se e solo se t è coprimo con m. Infatti $s \equiv t \pmod{m}$ può essere tradotto nella relazione $s = mq + t$ per un certo intero q, e dal Teorema 2.7 sappiamo che $MCD(s, m) = MCD(m, t)$.

Ora se u è un numero intero positivo coprimo con bc e minore di bc, allora u è in particolare coprimo con b e coprimo con c, ed è dunque soluzione di un sistema di equazioni del tipo:

$$\begin{cases} x \equiv k & (b) \\ x \equiv v & (c) \end{cases}$$

dove k è un intero positivo coprimo con b e $< b$ e v è un intero positivo coprimo con c e $< c$. Viceversa, per il teorema cinese, ogni sistema di equazioni del tipo descritto ha una sola soluzione intera positiva e $< bc$, e tale soluzione, essendo coprima con b e con c, è anche coprima con bc.

Dunque i numeri interi positivi coprimi con bc e minori di bc sono tanti quanti i sistemi del tipo descritto, che sono $\phi(b)\phi(c)$ (il prodotto delle possibile scelte di k e v). □

Teorema 6.25. *Consideriamo un intero positivo m. Se $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ è la sua decomposizione in fattori primi, allora*

$$\phi(m) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1})$$

Dimostrazione. Dalla Proposizione 6.24 segue subito che per calcolare $\phi(m)$ basta fare il prodotto dei numeri $\phi(p_i^{a_i})$. Ci resta dunque da sapere quanto vale $\phi(p^n)$ con p numero primo. Osserviamo che i numeri positivi minori di p^n sono tutti primi con p^n a meno che non siano multipli di p. Un semplice calcolo mostra dunque che $\phi(p^n) = p^n - p^{n-1}$. □

Osservazione 6.26. In particolare, se p e q sono due distinti numeri primi, $\phi(p^2) = p^2 - p$, $\phi(pq) = (p - 1)(q - 1)$. Dunque, come avevamo osservato nell'Esempio 6.19, $\phi(10) = 4 \cdot 1 = 4$, $\phi(15) = 4 \cdot 2 = 8$.

Esempio 6.27. Come applicazione immediata dei risultati precedenti possiamo calcolare subito la classe di resto di 2^{365} modulo 225.

Visto che $\phi(225) = (25-5)(9-3) = 120$, per il Teorema 6.21 sappiamo infatti che

$$2^{120} \equiv 1 \bmod 225$$

Dunque

$$2^{365} \equiv (2^{120})^3 \cdot 2^5 \equiv 2^5 \equiv 32 \bmod 225$$

ESEMPIO 6.28. Il Teorema 6.21 ci dice che

$$2^8 \equiv 1 \bmod 15$$

Osserviamo però che l'ordine di $[2]$ in $\mathbb{Z}_{15}^*$ non è 8, ma 4. L'ordine di un elemento divide l'ordine del gruppo (Corollario 6.17): questo esempio mostra che non è detto che coincida con l'ordine del gruppo. Del resto, $[1]$ ha ordine 1 in ogni gruppo $\mathbb{Z}_m^*$, e, se $m > 1$, 1 è diverso da $\phi(m)$.

Trovate il Teorema di Lagrange e degli esercizi su congruenze con esponenziali a pag. 103 di [**DM**].

4. Esercizi

ESERCIZIO 6.29. Dimostrare che se la cardinalità di un gruppo è un numero primo, allora il gruppo è ciclico.

ESERCIZIO 6.30. Dimostrare che se per due elementi a, b di un gruppo G vale $ab = e$ allora vale anche $ba = e$, e viceversa. Dunque per verificare che b è l'inverso di a basta verificare solo che sia inverso sinistro (o solo che sia inverso destro).

ESERCIZIO 6.31. Quali sono gli elementi di ordine massimo in $\mathbb{Z}_{13}^*$? E in $\mathbb{Z}_{20}^*$?

ESERCIZIO 6.32. Sia G un gruppo abeliano finito di cardinalità n. Dimostrare, senza usare il teorema di Lagrange, e imitando la prima dimostrazione del piccolo teorema di Fermat, che per ogni $g \in G$ vale $g^n = e$. [Nota: seguendo questa strada avremmo potuto dunque dimostrare il teorema di Eulero senza passare per il Teorema di Lagrange.]

ESERCIZIO 6.33. Se H è un sottoinsieme finito non vuoto di un gruppo G e vale che $a, b \in H \Rightarrow ab \in H$, allora H è un sottogruppo di G.

ESERCIZIO 6.34. Sia p un numero primo dispari. Dimostrare che se $[-1]$ è un quadrato in $\mathbb{Z}_p$ allora p è congruo a 1 modulo 4.

ESERCIZIO 6.35. Dimostrare che, preso un numero primo $p \equiv 1 \bmod 4$ allora

$$\left(\left(\frac{(p-1)}{2}\right)!\right)^2 \equiv -1 \bmod p$$

ESERCIZIO 6.36. Dimostrare che esistono infiniti numeri primi congrui a 1 modulo 4.

SOLUZIONE: [Traccia] Se fossero finiti, diciamo $p_1, p_2, \ldots, p_N$, potremmo considerare il numero $4(p_1 p_2 \cdots p_N)^2 + 1$... □

ESERCIZIO 6.37. Dato un sottogruppo H di un gruppo G si consideri la seguente relazione fra gli elementi di G: $x \sim y$ se e solo se $y^{-1}x \in H$.

Dimostrare che si tratta di una relazione di equivalenza e che per due elementi x e y vale $x \sim y$ se e solo se x e y appartengono allo stesso laterale destro $xH = yH$.

ESERCIZIO 6.38. Dimostrare che, per ogni intero positivo n vale:

$$n = \sum_{d|n} \phi(d)$$

Esercizio 6.39. Sia $\mathcal{F}_n$ l'ennesimo numero di Fermat (vedi l'Esercizio 3.38)[3]. Dimostrare che, se q è un primo che divide $\mathcal{F}_n$, allora

$$q \equiv 1 \bmod 2^{n+1}$$

Esercizio 6.40 (Più difficile del precedente). Proviamo a migliorare il risultato dell'esercizio precedente, dimostrando la seguente osservazione[4]: se q è un primo che divide $\mathcal{F}_n$, con $n > 1$, allora

$$q \equiv 1 \bmod 2^{n+2}$$

[3]Il risultato di questo esercizio potrebbe fornire una spiegazione di come mai Eulero ha saputo trovare facilmente il numero primo 641 che divide $\mathcal{F}_5$: per cercare un eventuale primo che divide $\mathcal{F}_5$ basta cercare fra i numeri primi congrui a 1 modulo $2^6 = 64$ o, se dimostrate anche il risultato del prossimo esercizio, addirittura fra i numeri primi congrui a 1 modulo $2^7 = 128$. Chi cerca fra i numeri primi congrui a 1 modulo 128 trova come primo candidato il 257 e poi subito dopo, al secondo tentativo, il 641.

[4]Dovuta al matematico francese Edouard Lucas, 1842-1891.

CAPITOLO 7

Lezioni del 29 ottobre e 30 ottobre

1. Omomorfismi di gruppi

1.1. Definizione di omomorfismo e automorfismo.

DEFINIZIONE 7.1. Dati due gruppi G_1, G_2, una funzione $f : G_1 \to G_2$ si dice *omomorfismo* se per ogni $g, h \in G_1$ vale:

$$f(gh) = f(g)f(h)$$

PROPOSIZIONE 7.2. *Sia $f : G_1 \to G_2$ un omomorfismo. Allora, se chiamiamo e_{G_1} ed e_{G_2} rispettivamente le identità di G_1 e di G_2, vale*

$$f(e_{G_1}) = e_{G_2}$$

Inoltre, per ogni $g \in G_1$ vale

$$f(g^{-1}) = f(g)^{-1}$$

DIMOSTRAZIONE. Osserviamo che possiamo scrivere

$$f(e_{G_1}) = f(e_{G_1}e_{G_1}) = f(e_{G_1})f(e_{G_1})$$

dove per il primo $=$ si è usato il fatto che e_{G_1} è l'identità di G_1 e per il secondo $=$ si è usato il fatto che f è un omomorfismo. Quella che abbiamo ottenuto è una uguaglianza in G_2. Potremmo subito concludere per il punto (5) del Teorema 6.4, visto che la soluzione dell'equazione

$$f(e_{G_1}) = xf(e_{G_1})$$

è unica, e sappiamo che e_{G_2} e $f(e_{G_1})$ entrambi risolvono l'equazione, dunque devono coincidere. Altrimenti (si tratta in realtà dello stessa dimostrazione, ma la presentiamo in due forme così potete scegliere quella a voi più congeniale), possiamo moltiplicare entrambi i membri di

$$f(e_{G_1}) = f(e_{G_1})f(e_{G_1})$$

per l'inverso di $f(e_{G_1})$:

$$f(e_{G_1})^{-1}f(e_{G_1}) = f(e_{G_1})^{-1}f(e_{G_1})f(e_{G_1})$$

ottenendo

$$e_{G_2} = f(e_{G_1})$$

Per quel che riguarda la seconda affermazione che dobbiamo dimostrare, dato $g \in G_1$ possiamo scrivere

$$e_{G_2} = f(e_{G_1}) = f(gg^{-1}) = f(g)f(g^{-1})$$

Dunque, vista l'unicità dell'inverso di un elemento, $f(g^{-1}) = f(g)^{-1}$.

□

DEFINIZIONE 7.3. Dati due gruppi G_1, G_2, se un omomorfismo $f : G_1 \to G_2$ è bigettivo allora è un *isomorfismo*. Se esiste un isomorfismo fra due gruppi G_1 e G_2 si dice che i due gruppi sono *isomorfi* e si scrive

$$G_1 \cong G_2$$

Dato un gruppo G, un isomorfismo $f : G \to G$ si dice anche *automorfismo*. Denoteremo con $Aut(G)$ l'insieme formato dagli automorfismi di un gruppo G.

ESERCIZIO 7.4. Dimostrare che $Aut(G)$ è un gruppo rispetto all'operazione data dalla composizione di funzioni.

ESEMPIO 7.5. La funzione $exp : \mathbb{R} \to \mathbb{R}^{>0}$ definita da $exp(a) = e^a$ per ogni $a \in \mathbb{R}$ è un isomorfismo fra $\mathbb{R}$ pensato come gruppo con l'operazione $+$ e $\mathbb{R}^{>0}$ (con questo simbolo intendiamo i numeri reali positivi) pensato come gruppo con la moltiplicazione.

ESEMPIO 7.6. La funzione $f : \mathbb{Z}_{10} \to \mathbb{Z}_5$ definita da $f([a]_{10}) = [a]_5$ è un omomorfismo surgettivo fra $\mathbb{Z}_{10}$ e $\mathbb{Z}_5$, pensati come gruppi con l'operazione $+$.

ESEMPIO 7.7. Osserviamo che il sottoinsieme $\{1, -1\}$ di $\mathbb{Z}$, visto con l'operazione data dalla moltiplicazione, è un gruppo. Si tratta di un gruppo isomorfo a $\mathbb{Z}_2$, visto come gruppo rispetto all'operazione $+$. L'isomorfismo $f : \{1, -1\} \to \mathbb{Z}_2$ è unico, ed è definito da $f(1) = [0]$ e $f(-1) = [1]$ (verificate nei dettagli quest'ultima affermazione).

ESERCIZIO 7.8. Il sottoinsieme $\{1, -1, \imath, -\imath\}$ di $\mathbb{C}$, visto con l'operazione data dalla moltiplicazione, è un gruppo, isomorfo a $\mathbb{Z}_4$, visto come gruppo con l'operazione $+$. In questo caso ci sono due isomorfismi possibili: quali?

Illustriamo ora un modo per produrre importanti automorfismi di un gruppo:

DEFINIZIONE 7.9. Sia G un gruppo e sia $g \in G$. Consideriamo la funzione $C_g : G \to G$ definita da

$$C_g(h) = ghg^{-1} \qquad \forall h \in G$$

Tale funzione si chiama *coniugio* rispetto all'elemento g.

PROPOSIZIONE 7.10. *Sia G un gruppo e sia $g \in G$. Il coniugio C_g è un automorfismo di G.*

DIMOSTRAZIONE. Per dimostrare che C_g è una funzione bigettiva basta osservare che possiede un'inversa, che è $C_{g^{-1}}$.

Per dimostrare che è un omomorfismo (e dunque un automorfismo), dati $h, k \in G$ si osserva che:

$$C_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = (ghg^{-1})(gkg^{-1}) = C_g(h)C_g(k)$$

□

Osserviamo che nella dimostrazione qui sopra, nel passaggio in cui compare $ghg^{-1}gkg^{-1}$ abbiamo aggiunto nel nostro prodotto il fattore $g^{-1}g$ che è uguale ad e. Si tratta di una tecnica usato molto frequentemente quando si fanno calcoli in un gruppo.

1.2. Nucleo e immagine di un omomorfismo. Ci sono due sottogruppi importanti associati ad un omomorfismo.

DEFINIZIONE 7.11. Dati due gruppi G_1, G_2 e un omomorfismo $f : G_1 \to G_2$ chiamiamo *nucleo* di f l'insieme:

$$Ker f = \{g \in G_1 | f(g) = e_{G_2}\}$$

Denotiamo con Imm f l'immagine di f:

$$\text{Imm } f = \{f(g) | g \in G_1\}$$

ESERCIZIO 7.12. Dimostrare che $Kerf$ è un sottogruppo di G_1 e Imm f è un sottogruppo di G_2.

Illustriamo subito due importanti proprietà di $Kerf$.

TEOREMA 7.13. *Dati due gruppi G_1, G_2, un omomorfismo $f : G_1 \to G_2$ è iniettivo se e solo se $Kerf = \{e_{G_1}\}$.*

DIMOSTRAZIONE. Supponiamo che f sia iniettivo. Se esistesse in $Kerf$ un elemento $u \neq e_{G_1}$ allora varrebbe $f(u) = e_{G_2} = f(e_{G_1})$, dove il secondo $=$ deriva dalla Proposizione 7.2, e questo contraddirebbe l'iniettività.

Viceversa, supponiamo che $Kerf = \{e_{G_1}\}$. Supponiamo per assurdo che f non sia iniettiva. Allora esistono due elementi $g, h \in G_1$, con $g \neq h$ e tali che $f(g) = f(h)$.

Possiamo dunque scrivere, moltiplicando per $f(h)^{-1}$, che $f(h)^{-1}f(g) = e_{G_2}$. A questo punto usando la Proposizione 7.2 e la definizione di omomorfsimo otteniamo

$$e_{G_2} = f(h)^{-1}f(g) = f(h^{-1})f(g) = f(h^{-1}g)$$

Questo significa che $h^{-1}g \in Kerf$. Poiché però $Kerf = \{e_{G_1}\}$ allora $h^{-1}g = e_{G_1}$, da cui si ottiene, moltiplicando entrambi i membri per h (a sinistra), $g = h$ che è assurdo perché contraddice l'ipotesi iniziale $g \neq h$.

□

La proposizione appena dimostrata sicuramente vi ricorda la proprietà del nucleo delle applicazioni lineari che avete visto a Geometria 1. In effetti se si considerano gli spazi vettoriali come gruppi abeliani con l'operazione $+$ allora una applicazione lineare è in particolare un omomorfismo nel senso dei gruppi, e dunque il Teorema 7.13, applicato questo caso, dice appunto che una applicazione lineare è iniettiva se e solo se il suo nucleo è $\{O\}$.

Un'altra importante proprietà di $Kerf$ è la seguente.

PROPOSIZIONE 7.14. *Dati due gruppi G_1, G_2 e un omomorfismo $f : G_1 \to G_2$, vale che per ogni $g \in G_1$ e per ogni $h \in Kerf$*

$$ghg^{-1} \in Kerf$$

Questo si può anche esprimere scrivendo che $C_g(Kerf) \subseteq Kerf$. Più precisamente vale $C_g(Kerf) = Kerf$.

DIMOSTRAZIONE. La prima parte è una immediata verifica. Presi $h \in Kerf$ e $g \in G_1$, usiamo il fatto che $f(h) = e_{G_2}$ e le proprietà degli omomorfismi studiate fin qui:

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e_{G_2}f(g)^{-1} = e_{G_2}$$

Abbiamo dunque dimostrato che $C_g(Kerf) \subseteq Kerf$.

Questo vale per ogni $g \in G_1$. Prendendo in particolare l'elemento g^{-1} abbiamo che $C_{g^{-1}}(Kerf) \subseteq Kerf$. Applicando C_g a questi due insiemi otteniamo dunque l'inclusione $C_g(C_{g^{-1}}(Kerf)) \subseteq C_g(Kerf)$ che, visto che C_g e $C_{g^{-1}}$ sono l'uno l'inverso dell'altro, è l'inclusione $Kerf \subseteq C_g(Kerf)$ che restava da dimostrare.

□

La proprietà appena esposta si può esprimere dicendo che $Kerf$ è un sottogruppo *invariate per coniugio* o *normale*. Discuteremo questa proprietà cruciale in una delle prossime lezioni.

2. Un esempio importante: il gruppo simmetrico

In questo paragrafo presenteremo un importante esempio di gruppo: il gruppo simmetrico.

DEFINIZIONE 7.15. Dato un numero intero positivo n, una *permutazione dei numeri* $1, 2, \ldots, n$ è una funzione f bigettiva dall'insieme $\{1, 2, \ldots, n\}$ in se stesso. Chiamiamo S_n l'insieme di tali permutazioni.

Osserviamo che l'insieme S_n ha $n!$ elementi. Inoltre, poiché sappiamo che la composizione fra funzioni è associativa, e che una funzione è bigettiva se e solo se ammette un'inversa, è immediato verificare che S_n, con il prodotto dato dalla composizione fra funzioni, è un gruppo.

DEFINIZIONE 7.16. Chiameremo S_n il *gruppo simmetrico* su n elementi.

OSSERVAZIONE 7.17. Se consideriamo un insieme X di cardinalità n, e l'insieme $Bij(X, X)$ delle funzioni bigettive da X in sé, le stesse considerazioni esposte sopra ci permettono di dire che $Bij(X, X)$ è un gruppo rispetto al prodotto dato dalla composizione fra funzioni. Si dimostra facilmente (esercizio!) che i gruppi $Bij(X, X)$ e S_n sono isomorfi.

2.1. La rappresentazione di una permutazione mediante la decomposizione in cicli disgiunti. Per descrivere le permutazioni è molto utile avere a disposizione una notazione efficiente. Una prima possibilità è illustrata dal seguente esempio. Sia $n = 9$; allora col simbolo

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 1 & 7 & 2 & 8 & 5 & 9 \end{pmatrix}$$

indichiamo la permutazione che manda ogni numero in quello che sta sotto di lui: per esempio 1 va in 3, 2 in 4, 3 in 6, 4 in 1, 5 in 7, e così via.

Un altro modo di rappresentare la stessa permutazione è la *decomposizione in cicli disgiunti*:

$$f = (1, 3, 6, 2, 4)(5, 7, 8)(9).$$

Questa scrittura va letta così: il primo ciclo (la prima parentesi) ci dice che la f manda 1 in 3, 3 in 6, 6 in 2, 2 in 4 e 4 in 1, ossia ogni elemento viene mandato in quello che lo segue, tranne l'ultimo, che viene rimandato nel primo (ecco perché si chiamano 'cicli'). Il secondo ciclo dice che 5 viene mandato in 7, 7 in 8 e 8 in 5. L'ultimo ciclo dice che 9 viene mandato in se stesso, ossia viene lasciato fisso dalla f.

Di solito quando un elemento viene lasciato fisso non lo indichiamo; dunque possiamo indicare f anche con la scrittura

$$f = (1, 3, 6, 2, 4)(5, 7, 8)$$

OSSERVAZIONE 7.18. È facile dimostrare che, data una permutazione f, la si può sempre scrivere come decomposizione di cicli disgiunti (l'aggettivo 'disgiunti' si riferisce, come avrete intuito, al fatto che ogni numero compare al più in un solo ciclo). Infatti si crea tale decomposizione come risultato di un algoritmo finito: si apre un ciclo, per esempio, come sopra, $(1, 3, 6....$, e i numeri che compaiono, dopo il primo, sono tutte immagini del numero precedente. Per esempio $3 = f(1), 6 = f(3)$ etc.. Poiché f è una funzione iniettiva, nel procedere con l'algoritmo, ogni volta il numero da inserire sarà o un numero 'nuovo', mai comparso prima, oppure il numero da cui eravamo partiti (nell'esempio, 1). Nel primo caso si continua a completare il ciclo, nel secondo caso si

chiude il ciclo e si passa a creare un altro ciclo, finchè non si è descritta completamente la permutazione f.

Osservazione 7.19. Avremmo potuto anche scrivere

$$f = (5, 7, 8)(1, 3, 6, 2, 4)$$

Infatti l'ordine con cui compaiono i cicli non ha influenza nella descrizione della permutazione f. Questo può essere visto anche nel seguente modo. Chiamiamo f_1 la permutazione $f_1 = (1, 3, 6, 2, 4)$ e f_2 la permutazione $f_2 = (5, 7, 8)$. Allora f_1 e f_2 commutano (lo potete verificare pensando che 'muovono' due insiemi di numeri che sono disgiunti fra loro) e vale che $f_1 \circ f_2 = f_2 \circ f_1 = f$ (il simbolo $\circ$ indica il prodotto ovvero la composizione di funzioni). In altre parole, quando scriviamo una permutazione f con la notazione dei cicli disgiunti, in realtà potremmo mettere fra un ciclo e l'altro il simbolo $\circ$, perché f è anche uguale al prodotto delle permutazioni corrispondenti a ciascuno dei cicli.

2.2. Composizione di permutazioni: qualche esempio per fare pratica. Per acquisire maggiore familiarità con il prodotto in S_n, ossia con la composizione di permutazioni, facciamo adesso un esempio.

Consideriamo $n = 10$; se f è la permutazione $f = (1, 3, 6, 2, 4, 7)(5, 8, 10)$ e g è la permutazione

$$g = (1, 3)(2, 9)$$

qual è la decomposizione in cicli di $g \circ f$?

In concreto, scriviamo

$$(1, 3)(2, 9) \circ (1, 3, 6, 2, 4, 7)(5, 8, 10)$$

Comporre le funzioni equivale a seguire il 'cammino' di un numero, applicandogli i cicli da destra a sinistra. Per esempio il ciclo più a destra manda il 5 in 8, il secondo ciclo lascia l'8 fisso, il terzo e il quarto anche. Dunque $g \circ f$ manda il 5 in 8. Seguiamo adesso l'8. Il ciclo più a destra lo manda in 10, il secondo ciclo lascia fisso il 10, e così anche il terzo e il quarto. Dunque per ora abbiamo trovato:

$$g \circ f = (5, 8, 10...$$

Continuiamo: il 10 viene mandato in 5 dal ciclo più a destra, e il 5 vene poi lasciato fisso. Dunque abbiamo chiuso il primo ciclo:

$$g \circ f = (5, 8, 10)...$$

Studiamo adesso l'immagine di un altro numero, per esempio il 2 (in questo momento in realtà siamo liberi di partire da un numero qualunque diverso da 5,8,10). Otteniamo

$$g \circ f = (5, 8, 10)(2, 4...$$

Ora dobbiamo seguire il 4

$$g \circ f = (5, 8, 10)(2, 4, 7...$$

Poi il 7, che viene lasciato fisso dal ciclo più a destra, e viene mandato in 1 dal secondo ciclo. Il terzo ciclo lascia fisso l'1 e il quarto manda 1 in 3. Dunque

$$g \circ f = (5, 8, 10)(2, 4, 7, 3...$$

Continuando così arriviamo a

$$g \circ f = (5, 8, 10)(2, 4, 7, 3, 6, 9)(1) = (5, 8, 10)(2, 4, 7, 3, 6, 9)$$

che è la decomposizione in cicli disgiunti che cercavamo.

Osservazione 7.20. È facile vedere che, se $n \geq 3$, non è detto che $g \circ f = f \circ g$. Basta considerare $f = (1,2)$, $g = (1,3)$; possiamo calcolare:

$$g \circ f = (1,3)(1,2) = (1,2,3)$$

$$f \circ g = (1,2)(1,3) = (1,3,2)$$

e osservare che la permutazione $(1,2,3)$ è diversa da $(1,3,2)$.

2.3. Altri esempi: conto di permutazioni con una certa struttura, inversi, coniugio.

Esempio 7.21 (Conto del numero di elementi con un certa decomposizione ciclica). In S_{17} quanti sono gli elementi la cui decomposizione in cicli è costituita da 3 cicli di lunghezza 4 e da un ciclo di lunghezza 5 ? Insomma gli elementi la cui decomposizione ha questa struttura: $(\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ ,\ )$?

Innanzitutto scegliamo i 4 numeri che vanno nel "primo" ciclo di lunghezza 4: abbiamo $\binom{17}{4}$ scelte. Una volta scelti, come si possono disporre questi 4 numeri? Si possono disporre in 4! modi diversi, però notiamo che il ciclo (a,b,c,d) rappresenta lo stesso elemento del ciclo (b,c,d,a) e dei cicli (c,d,a,b), (d,a,b,c). Insomma possiamo far 'muovere' i numeri circolarmente in un ciclo senza cambiare l'elemento del gruppo che viene rappresentato. Dunque 4 numeri si possono disporre dentro un ciclo di lunghezza 4 in modo da creare $\frac{4!}{4} = 6$ elementi diversi di S_{17}. Poi con $\binom{13}{4}$ scelte scegliamo i numeri che vanno nel secondo ciclo di lunghezza 4, e con $\binom{9}{4}$ scegliamo quelli che vanno nel terzo ciclo. In $\binom{5}{5} = 1$ scelte possiamo decidere quali numeri vanno nel ciclo di lunghezza 5, ossia tali numeri sono 'obbligati'.

Tenendo conto di quanto detto fin qui, potremmo proporre il numero:

$$\binom{17}{4}\frac{4!}{4}\binom{13}{4}\frac{4!}{4}\binom{9}{4}\frac{4!}{4}\binom{5}{5}\frac{5!}{5}$$

Però questo numero è troppo grande. Abbiamo commesso un errore: quando abbiamo preparato i tre cicli di lunghezza 4, li consideravamo "ordinati" (il "primo", il "secondo", il "terzo"). In realtà tali cicli commutano fra loro, perché coinvolgono numeri distinti. Per esempio noi abbiamo contato

$$(1,2,3,4)(5,6,7,8)(9,10,11,12)(13,14,15,16,17)$$

e

$$(5,6,7,8)(1,2,3,4)(9,10,11,12)(13,14,15,16,17)$$

come elementi diversi mentre rappresentano lo stesso elemento di S_{17}.

Siccome ci sono 3! modi di disporre in ordine i tre cicli di lunghezza quattro, il numero delle permutazioni del tipo $(\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ ,\ )$ è:

$$\frac{1}{3!}\left[\binom{17}{4}\frac{4!}{4}\binom{13}{4}\frac{4!}{4}\binom{9}{4}\frac{4!}{4}\binom{5}{5}\frac{5!}{5}\right]$$

dove, usando la formula per il binomio, molti dei fattoriali si possono semplificare e si ottiene

$$17!\frac{1}{3!}\left(\frac{1}{4}\right)^3\frac{1}{5}$$

L'Esercizio 7.33 vi chiederà di ripetere il ragionamento appena esposto per trovare una formula generale.

ESEMPIO 7.22 (L'inverso di un elemento). Come si può scrivere concretamente, data una permutazione f decomposta in cicli disgiunti, l'inversa di f? Osserviamo innanzitutto che, per esempio, in S_7 la permutazione inversa di $f = (2,4,6,1)$ è $f^{-1} = (1,6,4,2)$. Dunque la permutazione inversa di $(2,4,6,1)(3,5,7)$ è $(1,6,4,2)(7,5,3)$. A voi il facile esercizio di generalizzare.

ESEMPIO 7.23 (Il coniugio in S_n). Consideriamo due permutazioni $\sigma, \tau \in S_9$, e sia

$$\sigma = (1,3,5)(2,4,6,8)$$

Vogliamo calcolare il coniugio $C_\tau(\sigma)$, ovvero $\tau\sigma\tau^{-1}$.

Una buona strada è quella di capire quanto vale la permutazione $C_\tau(\sigma)$ applicata al numero $\tau(1)$. Abbiamo

$$C_\tau(\sigma)(\tau(1)) = \tau\sigma\tau^{-1}(\tau(1)) = \tau\sigma(\tau^{-1}\tau(1)) = \tau\sigma(1) = \tau(\sigma(1)) = \tau(3)$$

dove abbiamo composto le permutazioni coinvolte una per una e abbiamo usato $\sigma(1) = 3$. Dunque $C_\tau(\sigma)$ manda $\tau(1)$ in $\tau(3)$. Allo stesso modo possiamo calcolare

$$C_\tau(\sigma)(\tau(3)) = \tau\sigma\tau^{-1}(\tau(3)) = \tau\sigma(\tau^{-1}\tau(3)) = \tau\sigma(3) = \tau(5)$$

dove abbiamo usato $\sigma(3) = 5$. Dunque $C_\tau(\sigma)$ manda $\tau(3)$ in $\tau(5)$. Potete a questo punto continuare il calcolo e scrivere la decomposizione in cicli disgiunti di $C_\tau(\sigma)$:

$$C_\tau(\sigma) = \tau\sigma\tau^{-1} = (\tau(1),\tau(3),\tau(5))(\tau(2),\tau(4),\tau(6),\tau(8))$$

Come avrete notato, può essere ottenuta dalla decomposizione in cicli disgiunti di σ sostituendo ogni numero i con $\tau(i)$.

A voi il compito di generalizzare questo esempio e dimostrare che, date due permutazioni $\tau, \sigma \in S_n$, per ogni $i = 1, ..., n$ vale che

$$C_\tau(\sigma)(\tau(i)) = \tau(\sigma(i))$$

e dunque la decomposizione in cicli disgiunti di $C_\tau(\sigma) = \tau\sigma\tau^{-1}$ si ottiene considerando la decomposizione in cicli disgiunti di σ e sostituendo ad ogni numero i il numero $\tau(i)$.

2.4. Permutazioni pari e dispari. Approfondiamo lo studio del gruppo S_n. Le permutazioni che scambiano due elementi fra di loro lasciando fissi tutti gli altri, ossia quelle della forma (i,j), si chiamano *trasposizioni*.

Notiamo che ogni permutazione si può scrivere come prodotto di trasposizioni, non necessariamente disgiunte. Per esempio, consideriamo in S_{10} la permutazione

$$f = (2,6,3,7,5,9,10).$$

Osserviamo che vale:

$$f = (2,6,3,7,5,9,10) = (2,10) \circ (2,9) \circ (2,5) \circ (2,7) \circ (2,3) \circ (2,6).$$

Questo esempio ci permette subito di intuire come comportarsi nel caso in cui la permutazione sia composta da un solo ciclo. Se invece consideriamo una permutazione che si scrive come prodotto di vari cicli disgiunti, possiamo esprimere ogni ciclo come prodotto di trasposizioni: così facendo, la permutazione risulta prodotto di tutte le trasposizioni che abbiamo usato per ottenere i cicli. Per esempio, in S_8 consideriamo

$$g = (2,6,3,7,5)(4,8,1).$$

Visto che

$$(2,6,3,7,5) = (2,5) \circ (2,7) \circ (2,3) \circ (2,6)$$

e

$$(4,8,1) = (4,1) \circ (4,8)$$

allora vale:

$$g = (2,6,3,7,5)(4,8,1) = (2,5) \circ (2,7) \circ (2,3) \circ (2,6) \circ (4,1) \circ (4,8).$$

Osseviamo subito che, quando scriviamo una permutazione come prodotto di trasposizioni, non c'è un modo solo di farlo. Per esempio in S_3 la trasposizione $h = (1,2)$ si può scrivere in vari modi come prodotto di trasposizioni:

$$h = (1,2) = (2,3)(1,3)(2,3) = (1,3)(1,2)(1,3)(1,3)(2,3).$$

Tutte le scritture di h che abbiamo mostrato contengono un numero *dispari* di trasposizioni. Non si tratta di un caso, come mostra il seguente teorema.

TEOREMA 7.24. *Consideriamo una permutazione $\sigma \in S_n$ ($n \geq 2$). Se σ si può scrivere come prodotto di t trasposizioni e anche come prodotto di k trasposizioni, allora vale $t \equiv k \quad (2)$.*

DIMOSTRAZIONE. Facciamo agire S_n sull'insieme $\mathbb{R}[x_1, ..., x_n]$ dei polinomi a coefficienti reali in n variabili, nel seguente modo: dato $\sigma \in S_n$ e dato $f(x_1, x_2, ..., x_n)$, σ applicato a $f(x_1, x_2, ..., x_n)$ è il polinomio $f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$. Scriveremo:

$$\sigma \cdot f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

In altre parole, l'azione di σ sostituisce nel polinomio f, per ogni $i = 1, ..., n$, la variabile x_i con la variabile $x_{\sigma(i)}$. Osserviamo che l'identità e di S_n lascia invariati tutti i polinomi e anche che per ogni $\sigma, \tau \in S_n$ e per ogni $f(x_1, x_2, ..., x_n) \in \mathbb{R}[x_1, ..., x_n]$ vale

$$(\sigma \circ \tau) \cdot f(x_1, x_2, ..., x_n) = \sigma \cdot (\tau \cdot f(x_1, x_2, ..., x_n))$$

Questo è un esempio di *azione di un gruppo su un insieme*. Discuteremo in un prossimo capitolo questa situazione più in generale. Nel caso presente, consideriamo in particolare il polinomio

$$p(x_1, x_2, ..., x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

Per esempio, nel caso $n = 3$ si tratta del polinomio

$$p(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

Sia ora τ la trasposizione $\tau = (a, b)$ con $1 \leq a < b \leq n$, e studiamo $\tau \cdot p(x_1, x_2, ..., x_n)$. L'azione di τ non modifica i fattori $x_i - x_j$ in cui i e j sono diversi da a e da b. Invece, per quel che riguarda i fattori che contengono x_a o x_b:

- per ogni m che soddisfa $1 \leq m < a$ l'azione di τ scambia fra loro i due fattori $(x_m - x_a)$ e $(x_m - x_b)$
- per ogni m che soddisfa $b < m \leq n$ l'azione di τ scambia fra loro i due fattori $(x_a - x_m)$ e $(x_b - x_m)$;
- per ogni s che soddisfa $a < s < b$ l'azione di τ scambia fra loro i due fattori $(x_a - x_s)$ e $(x_s - x_b)$ ma cambiando anche il segno ad entrambi. Il prodotto $(x_a - x_s)(x_s - x_b)$ resta dunque invariato;
- infine, l'azione di τ cambia il segno del fattore $(x_a - x_b)$.

Risulta dunque dall'analisi precedente che $\tau \cdot p(x_1, x_2, ..., x_n) = -p(x_1, x_2, ..., x_n)$ per ogni trasposizione $\tau \in S_n$.

A questo punto possiamo concludere la dimostrazione del teorema: data una permutazione $\sigma \in S_n$ che si può scrivere come prodotto di t trasposizioni, per sapere come agisce σ su $p(x_1, x_2, ..., x_n)$ basta applicare una dopo l'altra queste t trasposizioni. Dunque vale

$$\sigma \cdot p(x_1, x_2, ..., x_n) = (-1)^t p(x_1, x_2, ..., x_n)$$

Se σ si può scrivere anche come prodotto di k trasposizioni, allora per lo stesso ragionamento vale anche

$$\sigma \cdot p(x_1, x_2, ..., x_n) = (-1)^k p(x_1, x_2, ..., x_n)$$

Per non avere una contraddizione, deve valere $(-1)^t = (-1)^k$, dunque deve valere $t \equiv k \quad (2)$. □

Dal Teorema 7.24 segue che possiamo dividere gli elementi di S_n in due famiglie:

DEFINIZIONE 7.25. Chiameremo una permutazione $\sigma \in S_n$ *pari* se può essere scritta come prodotto di un numero pari di trasposizioni, e *dispari* se può essere scritta come prodotto di un numero dispari di trasposizioni.

COROLLARIO 7.26. *L'insieme delle permutazioni pari di S_n è un sottogruppo di S_n che indicheremo con A_n, il* gruppo alterno *su n elementi. Vale che $|A_n| = \frac{n!}{2}$.*

DIMOSTRAZIONE. Consideriamo la funzione $\epsilon : S_n \to \mathbb{Z}_2$ data da $\epsilon(\sigma) = [0]$ se σ è pari e $\epsilon(\sigma) = [1]$ se σ è dispari. Questa funzione si chiama funzione *segno*, e ci capiterà di usarla più avanti.[1] Come conseguenza del Teorema 7.24 osserviamo che si tratta di un omomorfismo fra il gruppo S_n e il gruppo $\mathbb{Z}_2$. Dunque il suo nucleo, che è proprio A_n, è un sottogruppo di S_n.

Per quel che riguarda la cardinalità di A_n, osserviamo che la classe laterale $(1,2)A_n$ in S_n è costituita da tutte le permutazioni dispari. Infatti ogni permutazione in $(1,2)A_n$ è dispari, visto che si può scrivere come $(1,2)g$ con g pari.[2] Inoltre, data una qualunque permutazione dispari w, possiamo mostrare che appartiene a $(1,2)A_n$: infatti si può scrivere $w = (12)\,((12)w)$ dove $(12)w \in A_n$.

Allora la partizione di S_n data dalle classi laterali di A_n è costituita da due classi, A_n e $(1,2)A_n$ e, come sappiamo, vale che le classi laterali di un sottogruppo hanno tutte la stessa cardinalità. Dunque $|A_n| = \frac{n!}{2}$. □

Possiamo fare anche qualche altra osservazione su A_n: essendo il nucleo di un omomorfismo sappiamo che è un sottogruppo invariante per coniugio (o, con la terminologia che introdurremo nella prossima lezione, un sottogruppo normale).

Inoltre, ricordando che all'inizio del paragrafo abbiamo visto che ogni ciclo di lunghezza j si può scrivere come prodotto di $j-1$ trasposizioni, sappiamo come decidere rapidamente, data la decomposizione in cicli disgiunti di una permutazione, se tale permutazione è pari o dispari. Infatti, consideriamo una permutazione nella cui decomposizione ciclica compaiono r cicli di lunghezza dispari e s cicli di lunghezza pari. Allora tale permutazione è pari se e solo se s è pari.

Per esempio, in S_{11}, $(1,2,3)$ e $(1,2,3)(4,5,6,7)(8,9)$ sono permutazioni pari, mentre $(1,2,3)(4,5,6,7)$ è una permutazione dispari.

3. Esercizi

3.1. Esercizi di ripasso su funzioni iniettive e surgettive.

ESERCIZIO 7.27. Date $f : X \to Y$ e $g : Y \to Z$, è vero o falso che $g \circ f$ iniettiva implica f iniettiva? È vero o falso che $g \circ f$ iniettiva implica g iniettiva?

[1] Conformemente ad una notazione molto diffusa, continueremo a chiamare ϵ anche la funzione con codominio modificato $\epsilon : S_n \to \mathbb{Z}$ data da $\epsilon(\sigma) = 0$ se σ è pari e $\epsilon(\sigma) = 1$ se σ è dispari.

[2] Qui avremmo dovuto scrivere $(12) \circ g$ ma, visto che ormai conosciamo bene il gruppo simmetrico, cominciamo ad adottare la convenzione che usiamo spesso per i gruppi, ovvero quella di non scrivere il simbolo del prodotto.

ESERCIZIO 7.28. Date $f : X \to Y$ e $g : Y \to Z$, è vero o falso che $g \circ f$ surgettiva implica f surgettiva? È vero o falso che $g \circ f$ surgettiva implica g surgettiva?

3.2. Esercizi sul gruppo simmetrico.

ESERCIZIO 7.29. Consideriamo il gruppo simmetrico S_{10}. Qual è l'ordine della permutazione $(2, 3, 4, 5, 6, 7, 8)$? Qual è l'ordine della permutazione $(1, 3, 5, 6)(2, 4, 8)$? E quello della permutazione $(1, 2, 3, 4, 5, 6)(7, 8, 9, 10)$?

ESERCIZIO 7.30. Consideriamo la permutazione $g = (2, 4, 6, 1)(3, 5, 7)(8, 9) \in S_9$. Qual è il suo ordine?

In generale, data una permutazione di $h \in S_n$ la cui decomposizione in cicli disgiunti ha k cicli di lunghezza rispettivamente $l_1, l_2, \ldots, l_k$, qual è l'ordine di h?

ESERCIZIO 7.31. Quante sono in S_{12} le permutazioni di ordine 12?

ESERCIZIO 7.32. Dimostrare, usando l'Esempio 7.23, che, a parte il caso di S_2, il centro del gruppo simmetrico è banale, ossia che per ogni intero positivo $n \neq 2$ vale $Z(S_n) = \{e\}$.

ESERCIZIO 7.33. Generalizzare il risultato dell'Esempio 7.21: quante sono le permutazioni in S_n la cui decomposizione in cicli contiene m_i cicli di lunghezza i (per ogni $i = 1, ..., n$)? Ovviamente alcuni dei numeri m_i possono anche essere uguali a 0 e dovrà valere che $\sum_{i=1}^{n} i\ m_i = n$.

ESERCIZIO 7.34 (Il sottogruppo di Klein[3]). Si consideri il seguente sottoinsieme di S_4:

$$K = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

Dimostrare che K è un sottogruppo invariate per coniugio di S_4 (viene chiamato *sottogruppo di Klein*). È vero o falso che K è isomorfo a $\mathbb{Z}_4$? È vero o falso che K è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$?

ESERCIZIO 7.35. Dimostrare che, per $n \geq 2$, ogni permutazione di S_n può essere ottenuta come prodotto delle seguenti $n - 1$ trasposizioni:

$$(1, 2), (1, 3), ..., (1, n)$$

Qui si intende che nel prodotto ogni trasposizione può comparire anche più volte, o non comparire affatto.

Prima del prossimo esercizio introduciamo una definizione:

DEFINIZIONE 7.36. Dato un gruppo G, e dati $g_1, ..., g_k \in G$, diremo che G *è generato* da $g_1, ..., g_k \in G$ se ogni elemento di g può essere espresso come prodotto degli elementi $g_1, ..., g_k$ e dei loro inversi, eventualmente con ripetizioni. Si dirà che l'insieme $\{g_1, ..., g_k\}$ è un *insieme di generatori* di G.

Sappiamo che l'insieme delle trasposizioni è un insieme di generatori di S_n, per ogni $n \geq 2$. L'esercizio precedente ci mostra che anche l'insieme $\{(1, 2), (1, 3), ..., (1, n)\}$ è un insieme di generatori per S_n. Il prossimo ci chiede di trovare un altro insieme di generatori:

ESERCIZIO 7.37. Dato $n \geq 3$, trovare un insieme di generatori di S_n di cardinalità $n - 1$, in cui non tutti gli elementi sono trasposizioni.

[3]Christian Felix Klein, matematico tedesco, 1849 - 1925.

ESERCIZIO 7.38. Dimostrare che, dato $n \geq 3$, ogni permutazione di A_n può essere ottenuta come prodotto di permutazioni della forma (a, b, c), ossia di permutazioni composte da un unico ciclo di lunghezza 3.

ESERCIZIO 7.39 (L' 'enigma' del gioco del 15). La Figura 1 rappresenta la configurazione di base del famoso gioco del 15: Dimostrare che, seguendo le regole del gioco, ossia

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

FIGURA 1. Configurazione di base del gioco del 15

facendo scorrere i blocchetti nel modo lecito, non è possibile passare dalla configurazione base alla configurazione in cui il blocchetto 15 e il blocchetto 14 sono scambiati fra di loro, mentre tutti gli altri blocchetti sono posti come nella configurazione base.

3.3. Esercizi su omomorfismi e automorfismi.

ESERCIZIO 7.40. Quanti elementi ha il gruppo $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$?

ESERCIZIO 7.41. Dimostrare che $Aut(\mathbb{Z}_m)$ è isomorfo a $\mathbb{Z}_m^*$.

ESERCIZIO 7.42. Dato un omomorfismo $f : G_1 \to G_2$, dimostrare che per ogni $x \in G_1$ vale che $o(f(x))$ divide $o(x)$. Dimostrare inoltre che se f è un isomorfismo allora per ogni $x \in G_1$ vale $o(f(x)) = o(x)$.

ESERCIZIO 7.43. Dimostrare che la funzione 'coniugio' $C : G \to Aut(G)$, che associa ad ogni $g \in G$ l'automorfismo C_g è un omomorfismo (si considera $Aut(G)$ con la sua struttura di gruppo rispetto alla composizione). Qual è il nucleo di C?

ESERCIZIO 7.44. Consideriamo l'insieme delle isometrie del piano che mandano un quadrato in sé. Dimostrare che si tratta di un gruppo di cardinalità 8, con l'operazione di composizione. Viene chiamato *gruppo diedrale* D_4. Descrivere gli elementi di D_4 e indicare un insieme di generatori di cardinalità 2. Descrivere un omomorfismo iniettivo da D_4 a S_4.

ESERCIZIO 7.45. Consideriamo l'insieme delle isometrie del piano che mandano un poligono regolare di n lati in sé. Dimostrare che si tratta di un gruppo di cardinalità $2n$, con l'operazione di composizione. Viene chiamato *gruppo diedrale* D_n. Descrivere gli elementi di D_n e indicare un insieme di generatori di cardinalità 2. Descrivere un omomorfismo iniettivo da D_n a S_n.

CAPITOLO 8

Lezione del 5 novembre

1. Sottogruppi normali e quozienti

DEFINIZIONE 8.1. Sia $H < G$. Diremo che H è un *sottogruppo normale* o semplicemente che è *normale* se per ogni $g \in G$ vale

$$C_g(H) = H$$

In tal caso si scrive $H \triangleleft G$.

OSSERVAZIONE 8.2. L'insieme $C_g(H)$ si indica comunemente anche come gHg^{-1}. È una notazione molto intuitiva e la useremo spesso anche noi, visto che descrive bene l'insieme

$$C_g(H) = \{ghg^{-1} | h \in H\}$$

OSSERVAZIONE 8.3. Come sappiamo dalla Proposizione 7.14, per ogni omomorfisno $f : G_1 \to G_2$, il nucleo $Kerf$ è un sottogruppo normale di G_1.

OSSERVAZIONE 8.4. Rileggendo la dimostrazione della Proposizione 7.14, si osserva che una parte di essa può essere facilmente generalizzata e adattata a dimostrare il seguente fatto: se per un sottogruppo H di G e per ogni $g \in G$ vale $gHg^{-1} \subseteq H$ allora vale anche, per ogni $g \in G$, $gHg^{-1} = H$. Dunque nella definizione di sottogruppo normale avremmo potuto sostituire la richiesta $C_g(H) = H$ con $C_g(H) \subseteq H$.

OSSERVAZIONE 8.5. Se il gruppo G è abeliano, si verifica immediatamente che ogni suo sottogruppo è normale. Infatti, per ogni $g \in G$, vale in questo caso che C_g è l'identità (ossia l'automorfismo che manda ogni elemento in se stesso).

Facciamo subito un esempio di sottogruppo che non è normale. Per questo abbiamo bisogno di un gruppo non abeliano. Consideriamo il sottogruppo $H = \{e, (1, 2)\}$ di S_3. Vale che

$$(1, 3)H(1, 3) = \{e, (3, 2)\} \neq H$$

dunque H non è normale in S_3.

Ora veniamo al punto cruciale di questo paragrafo: mostreremo che se $H \triangleleft G$ allora è possibile definire sull'insieme G/H (i cui elementi sono gli H-laterali) un prodotto rispetto al quale G/H diventa un gruppo.

Innanzitutto premettiamo che, dati due sottoinsiemi A ed B di G, esiste già una definizione 'naturale' del prodotto AB come il seguente sottoinsieme di G:

$$AB = \{ab | a \in A, b \in B\}$$

Proviamo a partire da questa definizione di prodotto fra sottoinsiemi, e prendiamo due classi laterali g_1H e g_2H. Il loro prodotto naturale come sottoinsiemi è dunque il seguente sottoinsieme di G:

$$(g_1H)(g_2H) = \{g_1h_1g_2h_2 | h_1 \in H, h_2 \in H\}$$

Ora ci chiediamo: questo insieme è ancora una classe laterale di H in G?

Osserviamo che

$$g_1h_1g_2h_2 = g_1g_2g_2^{-1}h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2$$

dove abbiamo usato il trucco di inserire $e = g_2g_2^{-1}$ nel prodotto che stavamo considerando. Ora notiamo che $g_2^{-1}h_1g_2$ è un elemento di H (**qui si usa in maniera cruciale il fatto che H è un sottogruppo normale**), che chiameremo $\overline{h}$. In conclusione,

$$g_1h_1g_2h_2 = g_1g_2\overline{h}h_2$$

Il calcolo appena fatto mostra che il sottoinsieme $(g_1H)(g_2H)$ di G definito sopra è contenuto nella classe laterale g_1g_2H. Inoltre è immediato verificare l'inclusione opposta (esercizio!). Dunque la definizione naturale di $(g_1H)(g_2H)$ produce come risultato il sottoinsieme g_1g_2H di G che è ancora una classe laterale.

Questa osservazione, che si è svolta a livello di sottoinsiemi di G, ci suggerisce che siamo sulla buona strada per definire un prodotto in G/H, quando H è normale. Definiamo il seguente prodotto fra due elementi g_1H e g_2H di G/H:

$$g_1Hg_2H = g_1g_2H$$

Bisogna innanzitutto verificare che questa definizione è ben posta, ossia non dipende dai rappresentanti scelti per le classi laterali g_1H e g_2H. Prendiamo dunque degli altri rappresentanti delle stesse classi laterali: il Corollario 6.14 ci dice che saranno del tipo $g_1h_1H = g_1H$ e $g_2h_2H = g_2H$ con h_1, h_2 elementi di H. Secondo la definizione di prodotto in G/H che abbiamo appena dato vale

$$g_1h_1H\ g_2h_2H = g_1h_1g_2h_2H$$

A questo punto rimane solo da controllare che i due laterali $g_1h_1g_2h_2H$ e g_1g_2H coincidono.

Ma, adottando un ragionamento simile a quello visto sopra, possiamo scrivere

$$g_1h_1g_2h_2H = g_1g_2g_2^{-1}h_1g_2h_2H = g_1g_2(g_2^{-1}h_1g_2)h_2H = g_1g_2\overline{h}h_2H$$

dove $\overline{h} \in H$ per la normalità di H, e dunque infine $g_1g_2\overline{h}h_2H = g_1g_2H$ come volevamo.[1]

La classe laterale $eH = H$ si comporta da identità rispetto al prodotto appena definito in G/H, e per ogni classe gH esiste l'inverso, che è la classe $g^{-1}H$. L'associatività del prodotto è una facile conseguenza dell'associatività del prodotto in G.

Definizione 8.6. Dato un gruppo G e un suo sottogruppo normale H chiameremo G/H, munito del prodotto definito sopra, il *gruppo quoziente* di G su H.

Quali sono le proprietà dei gruppi quozienti?

Alcune in qualche modo rispecchieranno le proprietà di G, altre potranno rendere G/H molto diverso da G: basti pensare al caso in cui $G = \mathbb{Z}$ con l'operazione $+$ e $H = (m)$. Osserviamo immediatamente che il gruppo quoziente $G/(m)$ è (isomorfo a) $\mathbb{Z}_m$ con l'operazione $+$. Dunque siamo partiti da un gruppo infinito ($\mathbb{Z}$) e abbiamo ottenuto come quoziente un gruppo finito.

Cominciamo ad esplorare la situazione con il seguente:

[1] Vorremmo rimarcare che il fatto che il prodotto in G/H sia ben definito discende anche direttamente dalla osservazione precedente sul prodotto di sottoinsiemi: sappiamo che il laterale g_1g_2H si può ottenere come prodotto degli insiemi g_1H e g_2H, mentre il laterale $g_1h_1g_2h_2H$ si può ottenere come prodotto degli insiemi dati dai due laterali g_1h_1H e g_2h_2H, che coincidono rispettivamente con g_1H e g_2H. Dunque i laterali $g_1h_1g_2h_2H$ e g_1g_2H coincidono.

Teorema 8.7 (Primo teorema di omomorfismo). *Dati due gruppi G_1, G_2 e un omomorfismo $f : G_1 \to G_2$, vale che*

$$G_1/Kerf \cong \text{Imm}\, f$$

Dimostrazione. Osserviamo innanzitutto che il gruppo quoziente $G_1/Kerf$ è ben definito perché, come sappiamo, $Kerf$ è un sottogruppo normale di G_1. Inoltre abbiamo già osservato che Imm f è un sottogruppo di G_2, dunque in particolare è un gruppo.

Per dimostrare il teorema dobbiamo costruire un isomorfismo $\overline{f} : G_1/Kerf \to \text{Imm}\, f$. Poniamo, per ogni $g_1 \in G_1$,

$$\overline{f}(g_1 Kerf) = f(g_1)$$

Per prima cosa si verifica che $\overline{f}$ è ben definito: se avessimo scelto un altro rappresentante per il laterale $g_1 Kerf$, lo avremmo indicato (in accordo con il Corollario 6.14) come $g_1 k Kerf$, con $k \in Kerf$. Ma allora secondo la definizione di $\overline{f}$ abbiamo

$$\overline{f}(g_1 k Kerf) = f(g_1 k)$$

Dato che f è un omomorfismo e $k \in Kerf$ possiamo scrivere

$$f(g_1 k) = f(g_1)f(k) = f(g_1)e_{G_2} = f(g_1)$$

dunque $\overline{f}$ è ben definito.

A questo punto possiamo verificare che $\overline{f}$ è un omomorfismo. Dati due laterali $g_1 Kerf, g_2 Kerf \in G_1/Kerf$, dobbiamo dimostrare che:

$$\overline{f}(g_1 Kerf)\overline{f}(g_2 Kerf) = \overline{f}(g_1 Kerf\ g_2 Kerf)$$

Ora osserviamo che:

$$\overline{f}(g_1 Kerf\ g_2 Kerf) = \overline{f}(g_1 g_2 Kerf) = f(g_1 g_2)$$

dove per il primo $=$ abbiamo usato la definizione di prodotto nel gruppo quoziente $G_1/Kerf$ e per il secondo $=$ abbiamo usato la definizione di $\overline{f}$. D'altra parte, sempre per la definizione di $\overline{f}$, vale:

$$\overline{f}(g_1 Kerf)\overline{f}(g_2 Kerf) = f(g_1)f(g_2)$$

Visto che f è un omomorfismo, e dunque $f(g_1 g_2) = f(g_1)f(g_2)$, abbiamo dimostrato che $\overline{f}$ è un omomorfismo.

Resta da dimostrare che $\overline{f}$ è bigettivo. Per l'iniettività, dato il Teorema 7.13, basta studiare $Ker\overline{f}$. Ora, quali classi laterali $gKerf$ vengono mandate da $\overline{f}$ in e_{G_2} (che è anche l'identità di Imm f)? Se vale

$$\overline{f}(gKerf) = f(g) = e_{G_2}$$

allora deve essere $g \in Kerf$ dunque la classe $gKerf$ coincide con la classe $eKerf$, che è l'identità di $G_1/Kerf$. Dunque $Ker\overline{f}$ contiene un solo elemento, l'identità di $G_1/Kerf$: questo prova l'iniettività di $\overline{f}$.

Per quel che riguarda la surgettività, preso un qualunque elemento $y \in \text{Imm}\, f$, allora possiamo scegliere $g \in G_1$ tale che $f(g) = y$. A questo punto si osserva che

$$\overline{f}(gKerf) = f(g) = y$$

dunque $\overline{f}$ è surgettivo.

□

Corollario 8.8. *Dati due gruppi G_1, G_2 e un omomorfismo surgettivo $f : G_1 \to G_2$, vale che*

$$G_1/Kerf \cong G_2$$

COROLLARIO 8.9. *Dati due gruppi G_1, G_2 e un omomorfismo iniettivo $f : G_1 \to G_2$, vale che*

$$G_1 \cong \text{Imm } f$$

Concludiamo questo paragrafo con una osservazione sulla relazione fra sottogruppi normali e nuclei di omomorfismi. Come sappiamo, dato un omomorfismo $f : G_1 \to G_2$, il suo nucleo è un sottogruppo normale di G_1. Viceversa, se abbiamo un sottogruppo $H \triangleleft G_1$, possiamo vederlo come nucleo di un omomorfismo. Vale infatti la seguente proposizione:

PROPOSIZIONE 8.10. *Dato un gruppo G_1 e un suo sottogruppo normale H, la funzione $\pi_H : G_1 \to G_1/H$ definita da $\pi(g) = gH$ per ogni $g \in G_1$ è un omomorfismo surgettivo (su G_1/H consideriamo la struttura di gruppo quoziente), con nucleo uguale ad H. Tale omomorfismo si chiama* proiezione al quoziente *di G_1 rispetto ad H.*

DIMOSTRAZIONE. Tutte le proprietà indicate sono di facile dimostrazione. Per esempio, il fatto che π_H sia un omomorfismo richiede la verifica che, dati $g_1, g_2 \in G_1$ vale

$$\pi_H(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \pi_H(g_1)\pi_H(g_2)$$

dove l' $=$ centrale è dato proprio dalla definizione di prodotto in G_1/H. □

Osserviamo infine che il primo teorema di omomorfismo e la proposizione precedente ci permettono di dire che, dato un gruppo G, ogni suo quoziente rispetto ad un sottogruppo normale è isomorfo all'immagine di G tramite un certo omomorfismo, e viceversa, ogni immagine di G tramite un omomorfismo è isomorfa ad un quoziente di G per un suo sottogruppo normale.

2. Qualche esempio

2.1. Quoziente di un gruppo ciclico. Sia C un gruppo ciclico (finito o infinito), generato da un elemento x: $C = (x)$. Se consideriamo un sottogruppo H di C, questo sarà normale visto che C è commutativo. Vogliamo studiare il gruppo quoziente C/H.

Possiamo per questo considerare l'omomorfismo $\pi_H : C \to C/H$.

Poiché x genera C, allora $\pi_H(x) = xH$ genera C/H, vista la surgettività di π_H e il fatto che $\pi_H(x^j) = \pi_H(x)^j$ per le proprietà di omomorfismo. Dunque C/H è ciclico.

Analizziamo vari casi. Se $H = \{e\}$, dalla Proposizione 8.10 ricaviamo che π_H è iniettiva e surgettiva, dunque si tratta di un isomorfismo: vale allora $C \cong C/H$, cosa che del resto avremmo potuto verificare direttamente in questo caso molto semplice.

Se $H = C$ (il che equivale a dire che $x \in H$), C/H contiene un solo elemento, ed è il gruppo banale formato solo dall'identità.

Supponiamo allora che $\{e\} \subsetneq H \subsetneq C$. Visto che $x \notin H$, possiamo considerare il più piccolo intero positivo m tale che $x^m \in H$ (tale intero deve esistere perchè x genera C). Sappiamo già che C/H è ciclico e generato da xH, ora possiamo aggiungere l'informazione che $x^m H = H$ e che l'ordine di xH è proprio m, dunque C/H ha cardinalità m, ed è costituito dai seguenti elementi:

$$H, xH, x^2H, ..., x^{m-1}H$$

2.2. Il quoziente $\mathbb{R}/\mathbb{Z}$. Consideriamo la funzione $g : \mathbb{R} \to \mathbb{C}$ definita da $g(\alpha) = \cos 2\pi\alpha + i \sin 2\pi\alpha$ per ogni $\alpha \in \mathbb{R}$.[2]

[2]Il numero complesso $\cos 2\pi\alpha + i \sin 2\pi\alpha$ viene indicato come $e^{2\pi i\alpha}$ e la funzione g che stiamo considerando è dunque l'esponenziale complesso che manda $\alpha \in \mathbb{R}$ in $e^{2\pi i\alpha}$.

Si osserva subito che Imm g coincide con il sottoinsieme $\mathcal{C}$ di $\mathbb{C}$ dato dagli elementi di norma 1 (ossia dai punti della circonferenza di raggio 1 centrata nell'origine). Se consideriamo $\mathbb{R}$ come gruppo rispetto all'addizione e $\mathcal{C}$ come gruppo con la moltiplicazione 'ereditata' da $\mathbb{C}$ (è un sottogruppo moltiplicativo di $\mathbb{C}$), le regole della moltiplicazione in $\mathbb{C}$ ci permettono di verificare facilmente che g è un omomorfismo.

Qual è il suo nucleo? Si tratta degli elementi $\alpha \in \mathbb{R}$ tali che $g(\alpha) = \cos 2\pi\alpha + i \sin 2\pi\alpha = 1$, e questo accade se e solo se $\alpha \in \mathbb{Z}$. Dunque per il Teorema 8.7 possiamo concludere che $R/\mathbb{Z}$ è isomorfo al gruppo $\mathcal{C}$.

2.3. Un omomorfismo di S_4 su S_3. Ci sono vari modi per costruire un omomorfismo surgettivo da S_4 a S_3. In questa paragrafo ne presentiamo uno, anche con lo scopo di fare un interessante esercizio su questi piccoli gruppi simmetrici.

La prima osservazione interessante è che possiamo costruire un sottogruppo di S_4 di cardinalità 8. L'idea ci viene pensando al gruppo diedrale D_4, che si può vedere come sottogruppo di S_4 mediante un omomorfismo iniettivo (come sa bene chi ha già svolto l'Esercizio 7.44). Ripercorriamo uno dei possibili modi di svolgere quell'esercizio: la Figura 1 mostra (in rosso) le riflessioni presenti nel gruppo diedrale D_4.

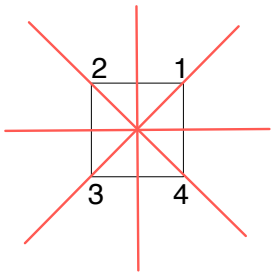

FIGURA 1. Le riflessioni presenti nel gruppo diedrale D_4.

Possiamo associare ad ogni riflessione la permutazione dei vertici da essa indotta. Otteniamo così i seguenti elementi di S_4:

- $(1,2)(3,4)$
- $(1,3)$
- $(1,4)(2,3)$
- $(2,4)$

Inoltre, come sappiamo, gli altri elementi di D_4 sono la rotazione r di 90 gradi (diciamo in senso antiorario, per fissare le idee), e le sue potenze. Queste, pensando sempre alle permutazioni dei vertici da esse indotte, producono i seguenti elementi di S_4:

- e
- $(1,2,3,4)$ (corrisponde a r)
- $(1,3)(2,4)$ (corrisponde a r^2)
- $(4,3,2,1)$ (corrisponde a r^3)

Gli otto elementi che abbiamo elencato costituiscono dunque un sottogruppo $H_1 < S_4$ (possiamo affermarlo pensando che H_1 è l'immagine di un omomorfismo da D_4 a S_4, ma chi vuole continuare a fare pratica con la composizione di permutazioni, può fare una semplice verifica diretta che si tratta davvero di un sottogruppo).

Ora ci chiediamo: dato un elemento $\sigma \in S_4$, chi è il sottogruppo coniugato $\sigma H_1 \sigma^{-1}$?

Sappiamo che il coniugio per σ mantiene la struttura ciclica degli elementi (vedi Esempio 7.23). Visto che H_1 è generato dagli elementi $(1,2,3,4)$ e $(1,2)(3,4)$ (dal punto

di vista geometrico sono la rotazione r e una riflessione), allora $\sigma H_1 \sigma^{-1}$ sarà il sottogruppo di S_4 generato da $(\sigma(1), \sigma(2), \sigma(3), \sigma(4))$ e $(\sigma(1), \sigma(3))(\sigma(2), \sigma(4))$.

Una breve analisi ci mostra che, al variare di $\sigma \in S_4$, otteniamo nella famiglia dei gruppi $\sigma H_1 \sigma^{-1}$ solo altri due gruppi diversi da H_1. Eccoli:

$$H_2 = \{e, (1,3,2,4), (1,2)(3,4), (4,2,3,1), (1,2), (3,4), (1,3)(2,4), (1,4)(2,3)\}$$

$$H_3 = \{e, (1,3,4,2), (1,4)(2,3), (2,4,3,1), (1,4), (2,3), (1,2)(3,4), (1,3)(2,4)\}$$

Osserviamo che tutti e tre i gruppi H_1, H_2, H_3 contengono il sottogruppo di Klein K (vedi esercizio 7.34). Non è una sorpresa: dopo aver notato che $K < H_1$, visto che $K \triangleleft S_4$, ovvero K è invariate per coniugio rispetto agli elementi di S_4, possiamo subito concludere che, per ogni $\sigma \in S_4$, K è contenuto in $\sigma H_1 \sigma^{-1}$.

Dopo questa 'ricognizione' di alcuni sottogruppi di cardinalità 8 di S_4 (in realtà tutti: l'Esercizio 8.17 vi chiederà di dimostrare che i tre sottogruppi H_1, H_2, H_3 sono gli unici sottogruppi di ordine 8 di S_4), possiamo finalmente costruire un omomorfismo surgettivo da S_4 a S_3.

Osserviamo infatti che ogni $\sigma \in S_4$ agisce per coniugio sull'insieme

$$\{H_1, H_2, H_3\}$$

permutandone gli elementi. Infatti $\sigma H_1 \sigma^{-1} \in \{H_1, H_2, H_3\}$ per costruzione dell'insieme $\{H_1, H_2, H_3\}$, e se, per esempio $H_2 = g H_1 g^{-1}$ allora $\sigma H_2 \sigma^{-1} = (\sigma g) H_1 (\sigma g)^{-1}$ appartiene ancora ad $\{H_1, H_2, H_3\}$ (identico il discorso per $\sigma H_3 \sigma^{-1}$). È poi immediato verificare che se per $i \neq j$ valesse $\sigma H_i \sigma^{-1} = \sigma H_j \sigma^{-1}$ ne seguirebbe $H_i = H_j$, assurdo.

Per esempio se $\sigma = (1,2) \in S_4$ vale

$$(1,2) H_1 (1,2) = H_3$$

$$(1,2) H_2 (1,2) = H_2$$

$$(1,2) H_3 (1,2) = H_1$$

e quindi, se guardiamo alla permutazione indotta da $\sigma = (1,2)$ sugli indici degli H_i, ricaviamo che $\sigma = (1,2)$ induce la seguente permutazione: $(1,3) \in S_3$.

Possiamo allora definire $\psi : S_4 \to S_3$ come la funzione che associa ad ogni $\sigma \in S_4$ la permutazione (in S_3) indotta da σ sugli indici dell'insieme $\{H_1, H_2, H_3\}$ come abbiamo visto sopra. La funzione ψ è un omomorfismo, perchè per calcolare $\psi(\tau\sigma)$ bisogna calcolare per ogni $i = 1, 2, 3$

$$(\tau\sigma) H_i (\tau\sigma)^{-1}$$

che è uguale a

$$\tau\sigma H_i \sigma^{-1} \tau^{-1} = \tau(\sigma H_i \sigma^{-1}) \tau^{-1}$$

ovvero a livello di permutazione degli indici si deve applicare prima la permutazione indotta da σ e poi quella indotta da τ. Dunque $\psi(\tau\sigma) = \psi(\tau)\psi(\sigma)$.

Con un breve calcolo scopriamo ora che $\psi((2,3)) = (1,2)$. Dunque nell'immagine di ψ, che è un sottogruppo di S_3, abbiamo trovato sia $(1,2) = \psi((2,3))$ sia $(1,3) = \psi((1,2))$. Allora, poiché $(1,2)$ e $(1,3)$ generano S_3, possiamo concludere che l'immagine di ψ coincide con S_3 e pertanto ψ è surgettivo.

Abbiamo dunque dimostrato che $\psi : S_4 \to S_3$ è un omomorfismo surgettivo. Qual è il suo nucleo? Innanzitutto sappiamo che dovrà avere cardinalià 4. Infatti per il primo teorema di omomorfismo (vedi in particolare il Corollario 8.9) vale

$$S_4 / Ker\psi \cong S_3$$

e dunque

$$|S_4 / Ker\psi| = 6$$

Ma dal Teorema di Lagrange[3] deriva che

$$|S_4/Ker\psi| = \frac{|S_4|}{|Ker\psi|} = \frac{24}{|Ker\psi|}$$

dunque $|Ker\psi| = 4$.

Cominciamo ad avere un sospettato per il 'ruolo' di $Ker\psi$, visto che si tratta di cercare un sottogruppo normale di S_4 di cardinalità 4: il sottogruppo di Klein. Una verifica diretta, che lasciamo a voi, vi permetterà di verificare che è proprio così, e dunque anche che S_4/K è isomorfo a S_3.

L'Esercizio 8.18 vi suggerisce un altro modo per costruire un omomorfismo surgettivo da S_4 in S_3.

3. Esercizi

Esercizio 8.11. Dimostrare che un sottogruppo H di un gruppo G è normale se e solo se gli H-laterali destri coincidono con gli H-laterali sinistri, ossia, per ogni $g \in G$ vale

$$gH = Hg$$

Esercizio 8.12. Sia G un gruppo e siano H_i dei sottogruppi ($i \in I$, dove I è una famiglia di indici, anche infinita).

Dimostrare che $\bigcap_{i\in I} H_i$ è un sottogruppo di G. È vero che se tutti gli H_i sono normali allora $\bigcap_{i\in I} H_i$ è normale?

Esercizio 8.13. Dati $A = \{e, (1,2)\}$ e $B = \{e, (2,3)\}$ sottoinsiemi di S_3, dimostrare che AB non è un sottogruppo.

Esercizio 8.14. Siano A e B sottogruppi di un gruppo finito G. Dimostrare che

$$|AB| = \frac{|A|\,|B|}{|A \cap B|}$$

(questo vale anche se AB non è un sottogruppo).

Esercizio 8.15. Dare un esempio di un gruppo G con due sottogruppi normali H e K tali che $H \cong K$ ma G/H non è isomorfo a G/K. Dimostrare che invece se esiste un $\phi \in Aut(G)$ tale che $\phi(H) = K$ allora G/H è isomorfo a G/K.

Esercizio 8.16. Verificare che il sottogruppo di Klein è sottogruppo di A_4, oltre che di S_4. Dimostrare che $A_4/K \cong \mathbb{Z}_3$.

Esercizio 8.17. Dimostrare che gli unici sottogruppi di cardinalità 8 di S_4 sono i tre sottogruppi H_1, H_2, H_3 costruiti nel Paragrafo 2.3.

Esercizio 8.18. Dimostrare che esiste un omomorfismo surgettivo da S_4 a S_3 utilizzando la seguente traccia: dimostrare che le rotazioni che mandano un cubo in sé costituiscono un gruppo isomorfo a S_4, e osservare che tali rotazioni permutano l'insieme dei tre assi del cubo, ossia le rette che passano per i punti centrali di due facce opposte.

[3]Se riguardate la dimostrazione del Teorema 6.15, osserverete che in particolare viene dimostrato che, dato un qualunque sottogruppo H di un gruppo finito G, vale

$$|G/H| = \frac{|G|}{|H|}$$

Per ulteriori suggerimenti su questo esercizio potete eventualmente guardare la figura che si trova nella prima pagina al link
$https://perso.univ-rennes1.fr/arnaud.girand/pdf/dvp\_agreg/cube.pdf$

CAPITOLO 9

Lezione del 6 novembre

1. Anelli

1.1. Definizioni. In questo paragrafo ricorderemo la definizione di anello con unità, e faremo qualche prima osservazione. Consultate anche il Capitolo 6, Paragrafo 1 di [**DM**].

DEFINIZIONE 9.1. Un anello con unità R è un insieme dove sono definite due operazioni, che chiamiamo addizione $(+)$ e moltiplicazione $(\cdot)$, che soddisfano le seguenti proprietà:

- R è un gruppo commutativo rispetto all'operazione $+$. Indicheremo con 0 l'elemento neutro rispetto alla somma, e per ogni $a \in \mathbb{R}$ indicheremo con $-a$ il suo inverso rispetto alla somma, che chiameremo *opposto*.
- $\forall\ a, b, c \in R$ vale $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (proprietà associativa della moltiplicazione).
- esiste un elemento $1 \in R$ tale che $\forall\ a \in R$ vale $a \cdot 1 = a$ (1 è l'elemento neutro per il prodotto).
- $\forall\ a, b, c \in R$ vale $(a + b) \cdot c = a \cdot c + b \cdot c$ e anche $a \cdot (b + c) = a \cdot b + a \cdot c$ (proprietà distributive).

OSSERVAZIONE 9.2. Come sappiamo dalla teoria dei gruppi (vedi Teorema 6.4), l'elemento 0 è unico e inoltre per ogni $a \in \mathbb{R}$ l'opposto di a è unico. Analogamente si dimostra che l'elemento 1 è unico.

Segnaliamo subito che la definizione include anche l'anello banale $A = \{0\}$, in cui tutte le operazioni sono banali e dunque lo 0 funziona da elemento neutro per la somma e anche per la moltiplicazione (0=1).

OSSERVAZIONE 9.3. In questo corso, quando useremo la parola 'anello', intenderemo sempre un anello con unità (in generale si può dare la definizione di anello senza la richiesta che esista l'elemento 1, e in diversi contesti risulta utile lavorare con anelli senza 1).

DEFINIZIONE 9.4. Un anello R che soddisfa anche la seguente proprietà si dice *commutativo*:

- $\forall\ a, b \in R$ vale $a \cdot b = b \cdot a$ (proprietà commutativa della moltiplicazione).

DEFINIZIONE 9.5. Sia R un anello commutativo. Diciamo che $a \in R$ è un *divisore di zero* se esiste $b \in R$, $b \neq 0$ tale che $ab = 0$. In particolare, 0 è un divisore di 0. Un anello commutativo R in cui $0 \neq 1$ e in cui l'unico divisore di 0 è 0 si chiama *dominio* (o *dominio di integrità*).

DEFINIZIONE 9.6. Un elemento u di un anello R si dice *invertibile* se esiste $v \in R$ tale che $u \cdot v = v \cdot u = 1$ (cioè se esiste un inverso sinistro e destro di u rispetto alla moltiplicazione). Denotiamo con R^* l'insieme degli elementi invertibili di R.

ESERCIZIO 9.7. Sia R un anello. Dimostrare che R^* è un gruppo rispetto alla moltiplicazione.

DEFINIZIONE 9.8. Due elementi a, b di un anello commutativo R si dicono *associati* se $a = bu$ con $u \in R^*$.

DEFINIZIONE 9.9. Un anello R in cui $0 \neq 1$ che soddisfa anche la seguente proprietà è detto *corpo*:

- ogni $a \in R - \{0\}$ è invertibile (esistenza dell'inverso rispetto alla moltiplicazione per tutti gli elementi diversi da 0).

Un corpo commutativo viene detto *campo*.

1.2. Primi esempi. Sono esempi di anelli commutativi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_m$ per ogni $m > 1$. Gli anelli $\mathbb{Q}$ ed $\mathbb{R}$ sono anche dei campi mentre $\mathbb{Z}$ non è un campo (non esiste in $\mathbb{Z}$ l'inverso rispetto alla moltiplicazione degli elementi diversi da 1 e -1, per esempio non esiste in $\mathbb{Z}$ l'inverso di 8). Come esempio di un anello non commutativo, avete già visto nel corso di Geometria 1 l'anello $Mat_{n\times n}(K)$ delle matrici $n \times n$ a coefficienti in un campo K. Si può sostituire a K un anello R, e si ottiene l'anello non commutativo $Mat_{n\times n}(R)$.

Per avere un esempio di corpo che non è un campo, si può ricorrere al corpo $\mathbb{H}$ dei quaternioni (vedi Esercizio 9.34).
Per quel che riguarda gli anelli $\mathbb{Z}_m$ osserviamo che se il numero m non è primo, $\mathbb{Z}_m$ ha dei divisori dello zero diversi da $[0]_m$, dunque non è un dominio. Infatti in tal caso m si fattorizza come $m = k \cdot s$ con $1 < k < m$ e $1 < s < m$ e vale che

$$[k]_m[s]_m = [ks]_m = [m]_m = [0]_m$$

Come conseguenza, se m non è primo, $\mathbb{Z}_m$ non è un campo (vedremo fra poco, nell'Osservazione 9.13, che un campo è automaticamente un dominio, comunque potete fin d'ora mostrare -facile esercizio- che non può esistere l'inverso degli elementi $[k]_m$ e $[s]_m$...). Vale invece il seguente importante teorema:

TEOREMA 9.10. *Se p è un numero primo, $\mathbb{Z}_p$ è un campo.*

DIMOSTRAZIONE. Se prendiamo una classe $[a]_p \neq [0]_p$ in $\mathbb{Z}_p$, visto che p non divide a, vale che $MCD(a, p) = 1$. Allora la congruenza $ax \equiv 1 \quad (p)$ ha soluzione, dunque esiste $b \in \mathbb{Z}$ tale che $ab \equiv 1 \quad (p)$. Come conseguenza in $\mathbb{Z}_p$ vale $[a]_p[b]_p = [ab]_p = [1]_p$. Abbiamo allora dimostrato che $[a]_p$ è invertibile in $\mathbb{Z}_p$ e che $[b]_p$ è il suo inverso.

□

1.3. Prime osservazioni. Il seguente lemma ci rassicura sul fatto che, a partire dalla definizione di anello, possiamo ricavare alcune proprietà a noi molto familiari (se si moltiplica un elemento per 0 si ottiene 0, 'meno' per 'meno' fa più...etc...).

LEMMA 9.11. *Sia A un anello, allora per ogni a, b in A vale:*

(1) $a \cdot 0 = 0$ *e* $0 \cdot a = 0$
(2) *l'opposto di a è unico e* $-(-a) = a$
(3) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$, *in particolare* $(-1) \cdot a = a \cdot (-1) = -a$.
(4) $(-a) \cdot (-b) = a \cdot b$, *in particolare* $(-1) \cdot (-1) = 1$.

DIMOSTRAZIONE. (1) Dimostriamo che $a \cdot 0 = 0$ (l'altra uguaglianza si dimostra in maniera analoga). Per prima cosa scriviamo $a \cdot (0 + 0) = a \cdot 0$ utilizzando il fatto che 0 è l'elemento neutro per la somma. A questo punto per la proprietà distributiva abbiamo $a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Dunque abbiamo ottenuto $a \cdot 0 + a \cdot 0 = a \cdot 0$. Sottraendo a destra e a sinistra l'opposto di $a \cdot 0$ (che esiste appunto perché A è un anello), otteniamo

$$a \cdot 0 = 0$$

(2) Queste proprietà sono state già dimostrate per i gruppi (Teorema 6.4), dunque non vanno ridimostrate. Le abbiamo inserite in questo lemma per comodità, per presentarle nella notazione additiva.
(3) Per dimostrare che $a \cdot (-b) = -(a \cdot b)$, dobbiamo mostrare che $a \cdot b + a \cdot (-b) = 0$. Utilizzando la proprietà distributiva, si scrive $a \cdot b + a \cdot (-b) = a \cdot (b + (-b))$. Ora, visto che $-b$ è l'opposto di b possiamo proseguire:
$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$$
dove l'ultima uguaglianza segue dal punto (1) appena dimostrato.
(4) Applichiamo due volte il punto (3):
$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b))$$
Come sappiamo dal punto (2), $-(-(a \cdot b)) = a \cdot b$ e questo conclude la dimostrazione.

□

D'ora in avanti, visto che l'opposto e lo 0 ubbidiscono alle regole a noi familiari, saremo liberi di scrivere $a - b$ invece di $a + (-b)$. Inoltre, ometteremo spesso il segno $\cdot$ della moltiplicazione.

Osservazione 9.12. Dalla proprietà (1) segue in particolare che se in un anello abbiamo $0 = 1$ allora per ogni elemento a possiamo scrivere la $a \cdot 0 = 0$ come $a = a \cdot 1 = a \cdot 0 = 0$ e dunque risulta che l'anello A è l'anello banale. Dunque l'unico anello con unità in cui $0 = 1$ è l'anello banale.

Osservazione 9.13. Un campo è anche automaticamente un dominio: infatti, se in un campo K per assurdo valesse $b \cdot r = 0$ per due elementi b, r diversi da 0 allora potremmo moltiplicare a sinistra per l'inverso di b, che chiameremo c, ottenendo
$$c \cdot (b \cdot r) = c \cdot 0$$
da cui, tenendo conto della proprietà associativa, del fatto che $c \cdot b = 1$ e del fatto che $c \cdot 0 = 0$ (punto (1) del Lemma 9.11), abbiamo $r = 0$, assurdo.

Osservazione 9.14. In ogni dominio R vale la *legge di cancellazione*, ossia, se $a \in R$ è diverso da 0, l'uguaglianza
$$ab = ac$$
implica
$$b = c$$
Infatti la $ab = ac$ si può riscrivere come $ab - ac = 0$ e, per la proprietà distributiva, come $a(b - c) = 0$. A questo punto, visto che $a \neq 0$ e che R è un dominio e dunque non ha divisori di 0 diversi da 0, deve valere $b - c = 0$, ovvero $b = c$.
La legge di cancellazione non è vera in generale per gli anelli. Basti pensare per esempio a $\mathbb{Z}_{12}$, dove abbiamo $[3][4] = [3][8]$ ma non è vero che $[4] = [8]$.[1]

Chiudiamo il paragrafo dando la definizione di sottoanello.

Definizione 9.15. Dato un anello R, un *sottoanello* di R è un sottoinsieme $T \subseteq R$ tale che valgano le seguenti tre condizioni:

- $1 \in T$;
- T è un sottogruppo di R rispetto alla operazione $+$;

[1]Come avete visto, abbiamo scritto [4] e non $[4]_{12}$. Ometteremo l'indice per alleggerire la notazione tutte le volte in cui sarà ben chiaro in quale anello stiamo lavorando.

- per ogni $a, b \in T$ vale $ab \in T$.

Se $T \neq R$ si dice che T è un sottoanello *proprio*.

2. Omomorfismi

DEFINIZIONE 9.16. Siano R e S due anelli. Una funzione $\phi : R \to S$ si dice *omomorfismo di anelli* se e solo se, per ogni $a, b \in R$

1) $\phi(a+b) = \phi(a) + \phi(b)$;
2) $\phi(ab) = \phi(a)\phi(b)$;
3) $\phi(1_R) = 1_S$.

Se un omomorfismo ϕ è sia iniettivo che surgettivo si dice *isomorfismo*.

DEFINIZIONE 9.17. Se $\phi : R \to S$ è un omomorfismo di anelli, definiamo *nucleo* di ϕ l'insieme $\ker \phi = \{a \in R | \phi(a) = 0_S\}$, dove 0_S è l'elemento neutro rispetto alla somma in S.

LEMMA 9.18. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora $\ker \phi$ è un sottogruppo additivo di R. Inoltre, se $a \in \ker \phi$ e $r \in R$ allora $ar \in \ker \phi$ e $ra \in \ker \phi$.*

DIMOSTRAZIONE. Dal momento che ϕ è, in particolare, un omomorfismo di gruppi additivi, la prima parte è già per noi nota.
Siano ora $a \in \ker \phi$ e $r \in R$. Vediamo che $\phi(ar) = \phi(a)\phi(r) = 0_S\phi(r) = 0_S$, e quindi $ar \in \ker \phi$. Allo stesso modo si dimostra che $ra \in \ker \phi$. □

OSSERVAZIONE 9.19. Sia $\phi : R \to S$ un omomorfismo di anelli. Visto che in particolare ϕ è anche un omomorfismo di gruppi abeliani, il Teorema 7.13 ci dice che ϕ è iniettivo se e solo se $\ker \phi = \{0_R\}$.

L'Esercizio 9.31 vi inviterà a riflettere sul fatto che in generale il nucleo di un omomorfismo di anelli $\phi : R \to S$ non è un sottoanello di R. Infatti nella definizione di omomorfismo fra anelli è inclusa la richiesta che $\phi(1_R) = 1_S$, dunque $1_R \notin Ker\phi$ a meno che S non sia l'anello banale.

Nessuna sorpresa invece per quel che riguarda l'immagine di un omomorfismo fra anelli:

ESERCIZIO 9.20. Sia $\phi : R \to S$ un omomorfismo. Dimostrare che $\phi(R)$ è un sottoanello di S.

3. Ideali di un anello e anelli quoziente

Lo studio dei nuclei degli omomorfismi ha messo in luce che in un anello ci sono alcuni sottoinsiemi notevoli che non sono sottoanelli. La seguente definizione li individua:

DEFINIZIONE 9.21. Un *ideale* I di un anello R è un sottogruppo additivo tale che per ogni $r \in R$ e per ogni $h \in I$ allora $rh \in I$ e $hr \in I$. Se $I \neq R$ si dice che I è un *ideale proprio*.

La proprietà moltiplicativa che caratterizza gli ideali ci dice che I 'assorbe' la moltiplicazione a destra e a sinistra per elementi arbitrari dell'anello (sottolineiamo che la definizione che abbiamo dato è dunque quella di ideale *bilatero*: in questo corso, visto che lavoreremo quasi esclusivamente con anelli commutativi, non avremo bisogno di approfondire il concetto di ideale non bilatero).

OSSERVAZIONE 9.22. Un ideale I non è un sottoanello di R, a parte il caso $I = R$. Infatti se $1 \in I$ allora $I = R$, per la proprietà di 'assorbimento'.

Esempio 9.23. Sia $R = \mathbb{Z}$. L'insieme $6\,\mathbb{Z} = (6)$ composto da tutti i multipli di 6 ci fornisce l'esempio di un ideale. In generale, dato un anello commutativo R e un elemento $a \in R$, denoteremo (a) l'insieme di tutti gli elementi dell'anello che si possono scrivere come ak per un certo $k \in R$. Si verifica facilmente che (a) è un ideale, e si chiama l'*ideale generato da a*.

Osservazione 9.24. Abbiamo visto nel Lemma 9.18 che il nucleo di un omomorfismo $\phi : R \to S$ è un ideale di R.

Esercizio 9.25. Dimostrare che se I e J sono due ideali dell'anello R allora anche $I + J = \{i + j \mid i \in I, j \in J\}$ e $I \cap J$ sono ideali di R.

Esercizio 9.26. Dimostrare che se I e J sono due ideali dell'anello R allora anche IJ, l'insieme degli elementi che si possono scrivere come somme finite di elementi della forma ij, con $i \in I$ e $j \in J$, è un ideale di R. Dimostrare inoltre che $IJ \subset I \cap J$ e che l'inclusione può essere stretta.

Dato un ideale I in un anello R denotiamo con R/I l'insieme dei laterali di I in R, considerando I come sottogruppo additivo di R. Possiamo scrivere gli elementi di R/I con la notazione additiva $a + I$, con $a \in R$, e per quanto abbiamo visto nel Paragrafo 1 del Capitolo 8 sappiamo che possiamo dare a R/I una struttura di gruppo additivo, con la somma definita da: $(a + I) + (b + I) = (a + b) + I$.

Per dotare R/I di una struttura di anello dobbiamo definire ora una moltiplicazione. La cosa più naturale è definire $(a + I)(b + I) = ab + I$. Dobbiamo però assicurarci che si tratti di una buona definizione, ovvero dobbiamo verificare che se $a + I = a' + I$ e se $b+I = b'+I$ allora vale $ab+I = a'b'+I$. Dal Corollario 6.14 riformulato con la notazione additiva, sappiamo che se $a + I = a' + I$ allora $a = a' + i_1$ con $i_1 \in I$; analogamente se $b + I = b' + I$ allora $b = b' + i_2$ con $i_2 \in I$. Ne segue

$$ab = (a' + i_1)(b' + i_2) = a'b' + a'i_2 + b'i_1 + i_1i_2,$$

ed essendo I un ideale di R abbiamo che per la proprietà di assorbimento $a'i_2$, $b'i_1$, $i_1i_2 \in I$, e inoltre per il fatto che un ideale è in particolare un sottogruppo additivo abbiamo $a'i_2 + b'i_1 + i_1i_2 \in I$, dunque $ab + I = a'b' + I$. Quindi l'operazione di moltiplicazione è ben definita.

Esercizio 9.27. Verificare che R/I, con le operazioni somma e prodotto definite sopra, è un anello.

Osservazione 9.28. Abbiamo appena *definito* la moltiplicazione nel quoziente con l'uguaglianza $(a + I)(b + I) = ab + I$. Questa è una definizione in cui le classi laterali sono pensate come elementi del quoziente R/I.,

Pensiamole invece adesso come sottoinsiemi di R. Osserviamo che in R vale, dal punto di vista insiemistico,

$$(a + I)(b + I) = \{(a + i_1)(b + i_2) \mid i_1, i_2 \in I\} \subseteq ab + I$$

dove l'ultima inclusione può essere stretta. Prendiamo come esempio $\mathbb{Z}$ e l'ideale $I = 6\,\mathbb{Z}$: si ha $(2 + 6\,\mathbb{Z})(4 + 6\,\mathbb{Z}) \subsetneq 8 + 6\,\mathbb{Z}$. Infatti 14 appartiene al laterale $8 + 6\,\mathbb{Z}$, ma non può essere scritto come $(2 + 6k)(4 + 6h)$ con h, k interi.

Compiuta la costruzione dell'anello quoziente di un anello rispetto ad un suo ideale possiamo ora enunciare per gli anelli il primo teorema di omomorfismo, analogo a quello per i gruppi. Lasciamo a voi la dimostrazione come utile esercizio di ripasso, visto che è semplicemente una traduzione parola per parola nel linguaggio degli anelli della dimostrazione già vista per i gruppi:

TEOREMA 9.29. *Siano R e S due anelli, e sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

$$R/\ker\phi \cong \text{Imm } \phi$$

ESERCIZIO 9.30. Dimostrare il teorema appena enunciato.

4. Esercizi

ESERCIZIO 9.31. Si consideri la funzione $f : \mathbb{Z} \to \mathbb{Z}_{10}$ definita da $f(x) = [x]_{10}$ per ogni $x \in \mathbb{Z}$. Dimostrare che si tratta di un omomorfismo di anelli e descrivere $Kerf$. Il nucleo $Kerf$ è un sottoanello di $\mathbb{Z}$?

ESERCIZIO 9.32. Se $R = \mathbb{Z}$ e $I = m\,\mathbb{Z} = (m)$ con m intero positivo, dimostrare che l'anello quoziente R/I è isomorfo a $\mathbb{Z}_m$.

ESERCIZIO 9.33. Dato un anello R ed un ideale I, dimostrare che se R è commutativo allora è commutativo anche R/I. Mostrare invece un esempio di un anello R non commutativo e di un ideale I tali che R/I sia commutativo. [Ovviamente l'ideale $I = R$ funziona per questo esempio. Risucite a immaginare un esempio con I ideale proprio?]

ESERCIZIO 9.34 (Il corpo dei quaternioni di Hamilton[2]). Il corpo dei quaternioni estende il campo dei numeri complessi. Come insieme è definito così:

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

dove $\mathbf{i}, \mathbf{j}, \mathbf{k}$ sono simboli. La somma è definita da :

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = a + a' + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$$

mentre la moltiplicazione è definita facendo la moltiplicazione come la fareste intuitivamente e raccogliendo poi i termini utilizzando le relazioni:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k},\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i},\ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$$

Qual è l'unità rispetto alla moltiplicazione? Trovare l'inverso di $1 + 2\mathbf{i} + 3\mathbf{j} + 4\mathbf{k}$.

ESERCIZIO 9.35. Siano R e S due anelli, e sia $\phi : R \to S$ un omomorfismo di anelli. Dato un ideale I di S dimostrare che il sottoinsieme Γ di R definito da

$$\Gamma = \{x \in R \mid \phi(x) \in I\}$$

è un ideale di R che contiene $Ker\phi$. [Di solito Γ viene indicato come $\phi^{-1}(I)$.]

ESERCIZIO 9.36. Dimostrare che un dominio di integrità finito è un campo.

[2]William Rowan Hamilton, fisico e matematico irlandese, 1805-1865.

CAPITOLO 10

Lezione del 13 novembre

1. Ancora su ideali e anelli quoziente

La domanda che ci poniamo è la seguente: sia R un anello e I un suo ideale, sotto quali condizioni l'anello quoziente R/I è un dominio oppure un campo?

DEFINIZIONE 10.1. Sia R un anello e I un suo ideale diverso da R (ossia $1 \notin I$). L'ideale I si dice *primo* se per ogni $r, s \in R$, $rs \in I$ implica $r \in I$ o $s \in I$.

DEFINIZIONE 10.2. Sia R un anello. Un ideale $I \neq R$ (ossia $1 \notin I$) si dice *massimale* se, quando un ideale J verifica $I \subseteq J \subseteq R$ allora $J = I$ o $J = R$.

Dato un elemento a di un anello commutativo R indicheremo con (a) l'ideale *generato* da a, ossia

$$(a) = \{ar \mid r \in R\}$$

Si tratta di una notazione simile a quella usata in teoria dei gruppi per il sottogruppo generato da un elemento, ma la coincidenza non creerà confusione.

ESEMPIO 10.3. Sia $R = \mathbb{Z}$ l'anello degli interi e sia I un ideale di R. Si dimostra facilmente che tutti e soli gli ideali di $\mathbb{Z}$ sono delle forma (n) per un certo intero n (fatelo per adesso come esercizio, torneremo poi su questo punto). Non è difficile dimostrare che tutti e soli gli ideali massimali sono quelli in cui n è un numero primo e che gli ideali primi sono quelli massimali più l'ideale $\{0\}$.

Vediamo cosa accade al quoziente R/I quando I è primo o massimale.

TEOREMA 10.4. *Sia R un anello commutativo e I un ideale di R. L'anello R/I è un dominio di integrità se e solo se I è un ideale primo.*

DIMOSTRAZIONE. Sia I un ideale primo, mostriamo che R/I è un dominio. Sia

$$(a + I)(b + I) = 0 + I$$

Il nostro scopo è mostrare che vale $a + I = 0 + I$ oppure $b + I = 0 + I$. Osserviamo che $(a + I)(b + I) = 0 + I$ equivale a dire, per la definizione del prodotto in R/I, che $ab \in I$: allora vale $a \in I$ oppure $b \in I$ perché l'ideale I è primo; quindi $a + I = 0 + I$ oppure $b + I = 0 + I$.

Supponiamo adesso che R/I sia un dominio e dimostriamo che I è primo. Sia $ab \in I$: se $a \in I$ abbiamo finito; se $a \notin I$ allora consideriamo nel quoziente il prodotto

$$(a + I)(b + I) = ab + I = 0 + I.$$

Essendo R/I un dominio, visto che $a + I \neq 0 + I$, deve essere $b + I = 0 + I$ ossia $b \in I$. □

TEOREMA 10.5. *Sia R un anello commutativo e I un ideale di R. L'anello R/I è un campo se e solo se I è un ideale massimale.*

DIMOSTRAZIONE. Supponiamo che I sia massimale. Sia $a + I \neq I$, ossia $a \notin I$. Per dimostrare che R/I è un campo dobbiamo mostrare che esiste in R/I l'inverso di $a + I$.

Consideriamo in R l'ideale $I+(a)$: vale $I \subsetneq I+(a) \subseteq R$ (non potendo essere $I+(a) = I$ perché $a \notin I$). Ma allora per la massimalità di I deve essere $I + (a) = R$. Dunque in particolare possiamo scrivere $1 = j + ra$ per certi $j \in I$ e $r \in R$. Vogliamo mostrare che nell'anello quoziente R/I l'elemento $r + I$ è l'inverso di $a + I$. Infatti vale:

$$(r + I)(a + I) = ra + I = (1 - j) + I = 1 + I$$

dove l'uguaglianza $(1 - j) + I = 1 + I$ deriva dal fatto che $j \in I$ e dunque $1 - j$ e 1 sono rappresentanti della stessa classe laterale di I.

Supponiamo adesso che R/I sia un campo e dimostriamo che I è massimale. Consideriamo un ideale J di R tale che $I \subseteq J \subseteq R$. Supponiamo che $J \neq I$: questo significa che esiste $j \in J$ tale che $j \notin I$. Allora $j + I \neq I$ e quindi ammette inverso perché R/I è un campo. Sia $r + I$ tale inverso; vale:

$$rj + I = (r + I)(j + I) = 1 + I.$$

Quindi $1 = rj + i$ con $i \in I$; allora $1 \in J$ poiché $rj, i \in J$. Possiamo dunque concludere che $J = R$.

□

TEOREMA 10.6. *Sia R un anello commutativo. Un ideale massimale di R è primo.*

DIMOSTRAZIONE. Sia I un'ideale massimale, allora per il Teorema 10.5 R/I è un campo e quindi, in particolare, un dominio di integrità. Di conseguenza, per il Teorema 10.4, I è un ideale primo. □

L'Esercizio 10.16 vi mostrerà un anello non commutativo dove il teorema precedente non vale.

2. Due esempi

2.1. I numeri complessi come quoziente di $\mathbb{R}[x]$. Consideriamo l'*omomorfismo di valutazione* $\psi : \mathbb{R}[x] \to \mathbb{C}$ definito nel modo seguente: per ogni $f(x) \in \mathbb{R}[x]$ si pone $\psi(f(x)) = f(\imath)$, ossia l'immagine di $f(x)$ è il numero complesso che si ottiene sostituendo $\imath$ alla variabile x (o, come anche si dice, *valutando* la x in $\imath$).

Visto che incontrerete spesso omomorfismi di valutazione, vale la pena svolgere una volta per tutte il seguente esercizio.

ESERCIZIO 10.7. Sia A un anello commutativo, sia B un anello che contiene A e sia $\alpha \in B$. Dimostrare che la funzione $\theta : A[x] \to B$ definita da $\theta(f(x)) = f(\alpha)$ è un omomorfismo di anelli.

Si osserva subito che l'omomorfismo $\psi : \mathbb{R}[x] \to \mathbb{C}$ definito sopra è surgettivo: per ogni numero complesso $a + \imath b$, il polinomio $bx + a$ è tale che $\psi(bx + a) = a + \imath b$.

Diventa interessante capire qual è il nucleo di ψ. Certamente l'ideale (x^2+1) generato da $x^2 + 1$ è incluso in $Ker\psi$: un generico elemento $f(x)$ dell'ideale si può scrivere come $f(x) = (x^2 + 1)g(x)$ con $g(x) \in \mathbb{R}[x]$, dunque quando lo valutiamo in $\imath$ si ottiene

$$f(\imath) = (\imath^2 + 1)g(\imath) = 0g(\imath) = 0$$

Usando la divisione euclidea di $\mathbb{R}[x]$ si dimostra che vale anche l'inclusione inversa, e che dunque $Ker\psi = (x^2 + 1)$. Infatti consideriamo un polinomio $\lambda(x) \in Ker\psi$ e mostriamo che $\lambda(x) \in (x^2 + 1)$. Dividiamo $\lambda(x)$ per $x^2 + 1$:

$$\lambda(x) = (x^2 + 1)q(x) + r(x)$$

dove il resto $r(x)$ è uguale a 0 oppure è un polinomio di grado < 2, dunque in ogni caso si può scrivere $r(x) = cx + d$ con $c, d \in \mathbb{R}$. Mostriamo che $r(x) = 0$. Valutando in $\imath$ si ricava:

$$\lambda(\imath) = (\imath^2 + 1)q(\imath) + r(\imath)$$

ovvero, visto che $\lambda(x) \in Ker\psi$,

$$0 = 0q(\imath) + r(\imath)$$

da cui si ottiene che $r(\imath) = c\imath + d = 0$, e pertanto $c = d = 0$.

Ora che abbiamo individuato $Ker\psi$, per il primo teorema di omomorfismo per anelli (Teorema 9.29) possiamo scrivere

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$$

Abbiamo dunque presentato il campo $\mathbb{C}$ come quoziente dell'anello $\mathbb{R}[x]$. Per il Teorema 10.5 in particolare ricaviamo che l'ideale $(x^2 + 1)$ è massimale in $\mathbb{R}[x]$.

In generale accade spesso che, per capire se un ideale è massimale, sia conveniente studiare il quoziente e cercare di capire se è un campo.

In questo caso osserviamo che avremmo comunque potuto dimostrare anche per altra via che $(x^2 + 1)$ è massimale.[1]

Visto che $x^2 + 1$ è un polinomio irriducibile, se consideriamo un ideale J di $\mathbb{R}[x]$ che contiene strettamente $(x^2 + 1)$, allora in J c'è un polinomio $g(x) \notin (x^2 + 1)$. Osserviamo che $MCD(x^2 + 1, g(x)) = 1$, dato che un divisore comune di questi due polinomi deve in particolare dividere $x^2 + 1$ e dunque ha solo due possibilità (a meno di associati): 1 e $x^2 + 1$. Ma, visto che $g(x) \notin (x^2 + 1)$ la seconda possibilità va scartata.

Ora, per il Teorema di Bezout per polinomi sappiamo che 1 si può scrivere come combinazione

$$1 = \lambda(x)(x^2 + 1) + \mu(x)g(x)$$

e dunque $1 \in J$, il che dimostra la massimalità di $(x^2 + 1)$.

2.2. La 'nascita' di un campo finito con 4 elementi. Consideriamo l'anello $\mathbb{Z}_2[x]$ dei polinomi sul campo $\mathbb{Z}_2$. Osserviamo che il polinomio $x^2 + x + 1$ è irriducibile in $\mathbb{Z}_2[x]$: infatti se esistesse una fattorizzazione non banale allora si potrebbe scrivere

$$x^2 + x + 1 = (ax + b)(cx + d)$$

con a e c diversi da 0.[2] Da questo seguirebbe che $x^2 + x + 1$ ha radici in $\mathbb{Z}_2$ (le radici di $ax + b$ e di $cx + d$, che potrebbero anche coincidere), mentre un semplice controllo mostra che questo è assurdo perché né 0 né 1 (che sono gli unici due elementi di $\mathbb{Z}_2$) sono radici di $x^2 + x + 1$.

Dalla irriducibilità di x^2+x+1 segue che l'ideale (x^2+x+1) di $\mathbb{Z}_2[x]$ è massimale (vedi il ragionamento del paragrafo precedente, che l'Esercizio 10.17 vi chiederà di ripetere in generale).

Dunque il quoziente $\mathbb{Z}_2[x]/(x^2 + x + 1)$ è un campo per il Teorema 10.5. Ma quanti elementi ha? Una classe laterale in $\mathbb{Z}_2[x]/(x^2+x+1)$ si può scrivere come $f(x)+(x^2+x+1)$

[1] Nelle righe che seguono useremo alcune informazioni sugli anelli di polinomi $K[x]$ (K campo) e sul Teorema di Bezout che discuterete a esercitazioni giovedì 19 novembre e che trovate nelle pagine da 168 a 180 di [**DM**]. In particolare ricordiamo qui la definizione di polinomio *irriducibile*: un polinomio $p(x) \in K[x]$ è irriducibile se ammette solo fattorizzazioni banali, ossia se $p(x) = f(x)g(x)$ implica che $f(x)$ è una costante o che $g(x)$ è una costante.

[2] Qui, e nel seguito in casi simili, per alleggerire la notazione non usiamo la notazione con le parentesi quadre $[a]_2$ per gli elementi di $\mathbb{Z}_2$.

per un certo polinomio $f(x) \in \mathbb{Z}_2[x]$, ma se facciamo la divisione euclidea fra $f(x)$ e x^2+x+1 troviamo

$$f(x) = q(x)(x^2+x+1) + ax + b$$

Da questo si ricava che la classe $ax+b+(x^2+x+1)$ coincide con la classe $f(x)+(x^2+x+1)$. In conclusione ogni classe si può rappresentare come $ax+b+(x^2+x+1)$ con $a, b \in \mathbb{Z}_2$. Si osserva facilmente che per ogni scelta di $a, b \in \mathbb{Z}_2$ abbiamo in effetti una classe diversa, dunque le classi, ossia gli elementi di $\mathbb{Z}_2[x]/(x^2+x+1)$, sono 4 in tutto.

Abbiamo costruito un campo con 4 elementi, che chiameremo $\mathbb{F}_4$. Come potete intuire, questa costruzione si potrà generalizzare, e lo faremo nelle prossime lezioni.

3. Anelli euclidei

Come sappiamo, nell'anello $K[x]$ dei polinomi a coefficienti in un campo K si può fare la divisione col resto, che ha molte analogie con la divisione euclidea in $\mathbb{Z}$.

La seguente definizione di anello euclideo raccoglie tutti gli anelli in cui esiste una divisione con le caratteristiche delle due divisioni ricordate qui sopra. Scopriremo alcune proprietà comuni a tutti questi anelli, e descriveremo un anello euclideo il cui studio ci darà interessanti applicazioni aritmetiche.

DEFINIZIONE 10.8. Un dominio di integrità D si dice *anello euclideo* se esiste una funzione *grado*

$$g : D \setminus \{0\} \to \mathbb{N}$$

tale che

(1) per ogni $a, b \in D$, entrambi non zero, vale $g(a) \leq g(ab)$;
(2) per ogni $a, b \in D$ con $b \neq 0$, esistono $q, r \in D$ tali che $a = qb + r$, dove $r = 0$ o $g(r) < g(b)$.

OSSERVAZIONE 10.9. Osserviamo che la funzione grado non è definita su 0. L'anello $\mathbb{Z}$ è un esempio di anello euclideo (possiamo prendere come g la funzione valore assoluto, e ignorare il fatto che tale funzione è definita anche su 0). L'anello dei $K[x]$ dei polinomi a coefficienti in un campo K è euclideo (in questo caso possiamo prendere come g la funzione *deg* che associa ad un polinomio il suo grado, e non è definito il grado del polinomio 0).

LEMMA 10.10. *In un anello euclideo D siano $a, b \neq 0$. Se $b \mid a$ e $a \nmid b$ allora $g(b) < g(a)$.*[3]

DIMOSTRAZIONE. Sia $a = bc$. Se a non divide b possiamo scrivere che $b = aq + r$ con $r \neq 0$ e $g(r) < g(a)$. Ma d'altra parte $r = b - aq = b - bcq = b(1 - cq)$ e dunque $g(r) \geq g(b)$. Si conclude che $g(a) > g(b)$.

□

LEMMA 10.11. *In un anello euclideo D vale che $g(1) \leq g(b)$ per ogni $b \in D$ e $g(b) = g(1)$ se e solo $b \in D^*$.*

DIMOSTRAZIONE. Per la prima affermazione è sufficiente osservare che, per ogni $b \in D$, vale $g(b1) \geq g(1)$, e questo mostra che $g(1)$ è il minimo dei gradi degli elementi dell'anello. Per la seconda parte utilizzeremo il fatto che b è invertibile se e solo se $(b) = D$.
($\Longrightarrow$) Supponiamo che $g(b) = g(1)$. Sia $a \in D$, allora $a = qb + r$ con $r = 0$ o $g(r) < g(b)$,

[3]Il concetto di divisibilità negli anelli commutativi è quello ovvio: a divide c se e solo se esiste b tale che $ab = c$.

ma b ha il grado minimo fra tutti i gradi degli elementi dell'anello e quindi $r = 0$. Quindi $a \in (b)$ per ogni $a \in D$ e dunque $D = (b)$.
($\Longleftarrow$) Supponiamo che $b \in D^*$. Allora $(b) = D$ e quindi per ogni $a \in D$ esisterà $r \in D$ tale che $a = rb$. Si deduce che, per ogni $a \in D$, $g(a) \geq g(b)$ e quindi $g(b)$ è il minimo fra tutti i gradi degli elementi dell'anello: allora $g(b) = g(1)$.

□

Introduciamo un importante esempio di anello euclideo, di cui parleremo in maniera più approfondita nella prossima lezione.

Definizione 10.12. L'insieme $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, viene chiamato *anello degli interi di Gauss.*[4]

Esercizio 10.13. Mostrare che $\mathbb{Z}[i]$ è un anello.

Proposizione 10.14. *L'anello $\mathbb{Z}[i]$ è euclideo.*

Dimostrazione. L'anello $\mathbb{Z}[i]$ è un dominio di integrità visto che è un sottoanello del campo $\mathbb{C}$. Scegliamo come grado g il quadrato del modulo:

$$\begin{array}{rccc} g: & \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ & a+bi & \longmapsto & |a+bi|^2 = a^2+b^2. \end{array}$$

Se $z, w \in \mathbb{Z}[i]$ allora $g(zw) \geq g(z)$: infatti $|zw|^2 \geq |z|^2$ poiché $|w| \geq 1$ ($w = a + bi$ con a e b interi). Adesso siano $z, w \in \mathbb{Z}[i]$ con $w \neq 0$. Dimostriamo che esiste la divisione euclidea di z per w. Consideriamo tutti i multipli di w in $\mathbb{Z}[i]$: questi individuano nel piano complesso un reticolo dato dai vertici di quadrati di lato $|w|$ e ogni punto del piano è in uno di questi quadrati (o in più di uno, se si trova al bordo). In particolare z starà in uno di questi quadrati. Sia $Q = w_0 w$ un vertice del quadrato che ha distanza minima da z. Stimiamo questa distanza: nel peggiore dei casi z è nel centro del quadrato, dunque,

$$|z - w_0 w| \leq \frac{|w|}{\sqrt{2}}.$$

Da questo segue che $g(z - w_0 w) \leq \frac{g(w)}{2} < g(w)$ e quindi possiamo prendere w_0 come quoziente della divisione e $z - w_0 w$ come resto. In altre parole

$$z = w w_0 + (z - w_0 w)$$

è la divisione euclidea che cercavamo.

□

Esercizio 10.15. Dimostrare che gli elementi invertibili di $\mathbb{Z}[i]$ sono quattro: 1,-1, i, $-i$. [Si può fare velocemente in maniera diretta, ma ricordiamo che si può usare il Lemma 10.11.]

4. Esercizi

Esercizio 10.16. Sia $Mat_{n\times n}(K)$ l'anello (non commutativo...) delle matrici $n \times n$ a coefficienti nel campo K. Dimostrare che gli unici ideali bilateri sono $\{0\}$ e $Mat_{n\times n}(K)$ e che l'ideale $\{0\}$ è massimale ma non è primo.

Esercizio 10.17. Sia K un campo e consideriamo un polinomio irriducibile $f(x) \in K[x]$. Dimostrare che l'ideale $(f(x))$ è massimale in $K[x]$.

Esercizio 10.18. I due anelli $\mathbb{Z}[i]/(3)$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$ sono isomorfi?

[4]Carl Friedrich Gauss, matematico tedesco, 1777-1855.

Esercizio 10.19. È vero o falso che l'anello $\mathbb{Z}[i]/(1+i)$ è isomorfo a $\mathbb{Z}_2$?

Esercizio 10.20. Determinare gli elementi che sono divisori di zero e gli elementi invertibili in $\mathbb{Q}[x]/(x^2-1)$.

Esercizio 10.21. Dimostrare che un anello commutativo che ha come soli ideali $\{0\}$ e se stesso è un campo.

Esercizio 10.22. Sia R un dominio e sia $a \in R$. Dimostrare che $R[x]/(x-a) \cong R$.

Esercizio 10.23. Si consideri in $\mathbb{Z}[x]$ l'ideale I generato da $x-2$ e da 3. Dimostrare che $\mathbb{Z}[x]/I \cong \mathbb{Z}_3$.

Esercizio 10.24. Si può definire sull'anello $K[[x]]$ (le *serie* formali nella variabile x sul campo K) una funzione grado che lo rende un anello euclideo?

Esercizio 10.25 (L'anello degli interi di Eisenstein[5]). Sia $\omega \in \mathbb{C}$ una radice cubica di 1 diversa da 1. È possibile dare una struttura euclidea all'*anello degli interi di Eisenstein* $\mathbb{Z}[\omega]$?

[5]Gotthold Max Eisenstein, matematico tedesco, 1823-1852

CAPITOLO 11

Lezione del 20 novembre

1. Un anello euclideo è un dominio a ideali principali

DEFINIZIONE 11.1. Un ideale I di un anello commutativo A si dice *principale* se è generato da un solo elemento, ossia se esiste $a \in A$ tale che $I = (a)$.[1]

DEFINIZIONE 11.2. Un dominio di integrità si dice a *dominio a ideali principali* (PID) se tutti i suoi ideali sono principali.

OSSERVAZIONE 11.3. Consideriamo $K[x, y]$, anello dei polinomi a coefficienti in un campo K e nelle variabili x e y. Questo anello non è a ideali principali: è facile mostrare (esercizio!) che l'ideale $I = (x, y)$ generato dalle variabili x e y non può essere generato da un solo elemento.

TEOREMA 11.4. *Sia D un anello euclideo. Allora tutti i suoi ideali sono principali, ossia D è un PID.*

DIMOSTRAZIONE. Sia I un ideale di D. L'ideale $I = \{0\}$ è principale, generato da 0. Supponiamo dunque $I \neq \{0\}$, e consideriamo il numero naturale m definito da:

$$m = \min\{g(a) \mid a \in I - \{0\}\}$$

Questo minimo esiste per il principio del buon ordinamento. Sia $d \in I$, $d \neq 0$, tale che $g(d) = m$; vogliamo mostrare che $I = (d)$.
È ovvio che $(d) \subseteq I$, dato che $d \in I$. Viceversa sia $y \in I$, allora esistono $q, r \in D$ tali che $y = qd + r$ con $r = 0$ oppure $r \neq 0$ e $g(r) < g(d)$. Osserviamo che $y - qd \in I$, e dunque $r \in I$. Se fosse $r \neq 0$ allora $g(r) < g(d)$ sarebbe in contraddizione con la minimalità del grado di d; dunque $r = 0$ e allora $y \in (d)$. Questo mostra che $(d) \supseteq I$. □

OSSERVAZIONE 11.5. Questo teorema implica in particolare che ogni ideale di $\mathbb{Z}$ è della forma (n) per un certo intero n, e che ogni ideale di $K[x]$ (K campo) è della forma $(f(x))$ per un certo polinomio $f(x)$.
La dimostrazione vi avrà forse ricordato una delle dimostrazioni del Lemma di Bezout. In effetti la dimostrazione del Teorema 2.10 può adesso essere vista come un caso particolare di quella del Teorema 11.4: in sostanza si mostrava che l'ideale $I = (a, b)$, con a e b non entrambi nulli, è uguale all'ideale principale $(MCD(a, b))$. Torneremo sul Lemma di Bezout nel prossimo paragrafo.

OSSERVAZIONE 11.6. Non è vero il viceversa del Teorema 11.4: un anello che è PID ma non è euclideo è

$$\mathbb{Z}[\frac{1}{2} + \frac{1}{2}i\sqrt{19}] = \{a + b(\frac{1}{2} + \frac{1}{2}i\sqrt{19}) \mid a, b \in \mathbb{Z}\}$$

Per una dimostrazione di questo fatto chi è interessato può leggere l'articolo di O. Campoli in American Mathematical Monthly, Vol 95, n. 9, 1988, pagg. 868-871.

[1] Questa è la definizione per anelli commutativi, quella che servirà in questo corso. Nel caso in cui l'anello non sia commutativo, si distinguono gli ideali principali sinistri, destri e bilateri.

2. Questioni di divisibilità nei PID. Ideali primi e massimali nei PID.

DEFINIZIONE 11.7. In un anello A, dati $a, b \in A$ non entrambi nulli, se esiste un divisore $d \in A - \{0\}$ di a e b tale che ogni altro divisore comune di a e b divide d si dice che d è un *massimo comun divisore* di a e b.

TEOREMA 11.8 (Esistenza di un MCD e Lemma di Bezout nei PID). *Dati $a, b \in D$, dominio a ideali principali, con a e b non entrambi nulli, esiste un massimo comun divisore $d \in D$ di a e b. Inoltre si può scrivere $d = a\lambda + b\mu$ per certi μ e λ in D.*

DIMOSTRAZIONE. Si consideri in D l'ideale $I = (a, b)$ generato da a e da b: visto che siamo in un PID tale ideale è principale e dunque si può scrivere $I = (d)$ per un certo $d \in D$. Questo d è un massimo comun divisore di a e b. Si ha infatti $a \in (d)$ e $b \in (d)$ e quindi $d \mid a$ e $d \mid b$. Inoltre $d \in (a, b)$ dunque si può scrivere $d = a\lambda + b\mu$ per certi μ e λ in D. Allora se c è un divisore comune di a e b questo c divide anche $a\lambda + b\mu = d$. □

OSSERVAZIONE 11.9. Nella definizione di massimo comun divisore e nel teorema precedente abbiamo scritto *un* massimo comun divisore. In effetti il massimo comun divisore non è unico ma si può dire che è unico a meno di moltiplicazione per invertibili, come avete già osservato a esercitazioni parlando dell'anello dei polinomi. Dimostriamolo in generale per un dominio D a ideali principali: siano d, d' due massimi comuni divisori di a e b, non entrambi nulli; allora vale sia $d \mid d'$ che $d' \mid d$, ossia $d' = dk$ e $d = d'h$. Quindi

$$d' = d'hk \Longrightarrow d'(hk - 1) = 0 \Longrightarrow hk = 1,$$

dove l'ultima implicazione è dovuta al fatto che D è un dominio di integrità e che $d' \neq 0$. Questo mostra che h e k sono entrambi invertibili.

Nel caso dell'anello $\mathbb{Z}$, stando alla Definizione 11.7, dati a, b non entrambi nulli, abbiamo dunque due massimi comuni divisori di a e b. Per tradizione però in questo caso si usa scegliere quello positivo e chiamarlo "il massimo comuni divisore", come abbiamo fatto anche noi nella Definizione 2.5.

OSSERVAZIONE 11.10. Se D è un anello euclideo, per determinare un massimo comun divisore di due elementi a e b non entrambi nulli, possiamo utilizzare l'algoritmo di Euclide. E possiamo utilizzare l'algoritmo di Euclide 'alla rovescia' per trovare la combinazione lineare $d = a\lambda + b\mu$. La dimostrazione che conoscete per gli interi può essere ripetuta in modo del tutto analogo, come avete visto anche ad esercitazioni per l'anello dei polinomi.

Torniamo ora ad approfondire il tema, accennato nell' Osservazione 3.5, di cosa sono in un dominio di integrità gli elementi irriducibili e gli elementi primi. Cominciamo ripartendo dalle definizioni.

DEFINIZIONE 11.11. Un elemento $p \neq 0$, $p \notin D^*$, di un dominio di integrità D si dice *primo* se per ogni $a, b \in D$, $p \mid ab$ implica $p \mid a$ o $p \mid b$.

OSSERVAZIONE 11.12. Questo equivale a dire che p è un elemento primo se e solo se $p \neq 0$ e (p) è un ideale primo.

DEFINIZIONE 11.13. Un elemento $\pi \neq 0$, $\pi \notin D^*$, di un dominio di integrità D si dice *irriducibile* se, per ogni $\gamma, \delta \in D$, $\pi = \gamma\delta$ implica $\gamma \in D^*$ o $\delta \in D^*$.

OSSERVAZIONE 11.14. Come potete notare, la definizione di elemento irriducibile applicata all'anello dei polinomi $K[x]$ coincide con la definizione vista ad esercitazioni.

Osservazione 11.15. Nel caso di $\mathbb{Z}$ le due definizioni sono equivalenti, come sappiamo. In generale però questo non è vero, come mostreremo nel Paragrafo 5.

Cominciamo comunque con l'osservare che:

Proposizione 11.16. *Sia D un dominio di integrità. Se $p \in D$ è primo allora p è irriducibile.*

Dimostrazione. Sia p primo e sia $p = \gamma\delta$. Dobbiamo dimostrare che $\gamma \in D^*$ o $\delta \in D^*$. Dato che p è primo vale $p \mid \gamma$ o $p \mid \delta$. Supponiamo che $p \mid \gamma$, ossia $\gamma = pk$. Dunque $p = \gamma\delta = pk\delta$, e da questo segue $p(1 - k\delta) = 0$. Visto che D è un dominio e $p \neq 0$, vale $k\delta = 1$, ossia $\delta \in D^*$. □

Perché sia vera l'implicazione inversa non basta che l'anello sia un dominio. Comunque se l'anello è un dominio a ideali principali allora i concetti di elemento primo ed elemento irriducibile sono equivalenti.

Teorema 11.17. *Sia D un dominio a ideali principali. Se $p \in D$ è un elemento irriducibile allora l'ideale (p) è massimale.*

Dimostrazione. Sia p irriducibile e consideriamo un ideale J tale che $(p) \subseteq J \subseteq D$. Dato che D è un PID, vale $J = (\gamma)$ per un certo $\gamma \in D$. Dunque possiamo scrivere $p = \gamma\delta$ per un $\delta \in D$. Poiché p è irriducibile, vale che uno fra γ o δ è invertibile. Se γ è invertibile allora $J = (\gamma) = (1) = D$, se δ è invertibile allora $J = (\gamma) = (\gamma\delta) = (p)$.
□

Corollario 11.18. *Sia D un dominio a ideali principali. Se $p \in D$ è irriducibile allora è primo.*

Dimostrazione. Sia p irriducibile, allora (p) è massimale per il teorema precedente, dunque (p) è primo per il Teorema 10.6, dunque p è un elemento primo per l'Osservazione 11.12. □

Osservazione 11.19. Il Teorema 11.17 ribadisce un fatto che avete già osservato lavorando nell'anello dei polinomi $K[x]$, e che sarà alla base delle nostra prossime lezioni: in $K[x]$ l'ideale generato da un polinomio irriducibile $f(x)$ è massimale. Per esempio una delle conseguenze è che il quoziente $K[x]/(f(x))$ è un campo.

3. Un anello euclideo è un dominio a fattorizzazione unica

Chiariamo innanzitutto cosa è un dominio a fattorizzazione unica.

Definizione 11.20. Un dominio di integrità D si dice *dominio a fattorizzazione unica* (UFD) se ogni elemento di $D - \{0\}$ che non è invertibile si scrive come prodotto di un numero finito di elementi irriducibili di D e tale decomposizione è unica a meno dell'ordine e di elementi associati.

L'anno prossimo ad Algebra 1 verrà dimostrato che un PID è un UFD. Per il momento osserviamo che la dimostrazione che l'anello $\mathbb{Z}$ è un UFD (Teorema 3.6) può essere adesso ripetuta praticamente parola per parola per gli anelli euclidei.

La dimostrazione dell'esistenza di una fattorizzazione in irriducibili può essere svolta per induzione sulla falsariga di quella per $\mathbb{Z}$, utilizzando la funzione grado.

Nella dimostrazione dell'unicità della fattorizzazione si utilizzava in maniera cruciale il fatto che in $\mathbb{Z}$ gli elementi primi e gli elementi irriducibili coincidono. Ora questo lo sappiamo anche per i PID e in particolare per gli anelli euclidei, grazie ai risultati del paragrafo precedente. Vi lascio allora come utile esercizio di ripasso la dimostrazione del seguente:

TEOREMA 11.21. *Un anello euclideo è un UFD.*

OSSERVAZIONE 11.22. Il risultato del teorema ci rassicura in particolare sul fatto che anche $K[x]$ (con K campo) e $\mathbb{Z}[i]$ sono UFD.

4. Gli elementi primi nell'anello degli interi di Gauss

In questo paragrafo studieremo l'anello $\mathbb{Z}[i]$ degli interi di Gauss; in particolare individueremo quali sono gli elementi primi (che coincidono con gli elementi irriducibili, visto che l'anello è euclideo) e scopriremo che questo è collegato ad una interessante osservazione aritmetica.

LEMMA 11.23. *Sia $p \in \mathbb{Z}$ un numero primo dispari che non è un elemento irriducibile in $\mathbb{Z}[i]$; allora p si può scrivere come somma di due quadrati di numeri interi.*

DIMOSTRAZIONE. Supponiamo che p non sia un elemento irriducibile in $\mathbb{Z}[i]$, allora $p = (a+bi)(c+di)$ con $a+bi$ e $c+di$ appartenenti a $\mathbb{Z}[i]$ non invertibili, e dunque tali che $a^2+b^2 > 1$ e $c^2+d^2 > 1$ (vedi Lemma 10.11).

Osserviamo che, essendo $\overline{p} = p$, si ha anche $p = (a-bi)(c-di)$. Allora moltiplicando membro a membro le due relazioni abbiamo $p^2 = (a^2+b^2)(c^2+d^2)$; visto che $a^2+b^2 > 1$ e $c^2+d^2 > 1$ deve valere $a^2+b^2 = p$ e $c^2+d^2 = p$. □

LEMMA 11.24. *Sia $p \in \mathbb{Z}$ un primo della forma $4n+1$. Allora la congruenza $x^2 \equiv -1 \pmod{p}$ ammette soluzione in $\mathbb{Z}$.*

DIMOSTRAZIONE. Per coloro che non hanno già risolto l'Esercizio 6.35: sia $x = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$. Essendo $p-1 = 4n$, nel prodotto precedente compare un numero pari di termini, per cui $x = (-1)(-2)(-3)\cdots\left(-\frac{p-1}{2}\right)$. A questo punto osserviamo che

$$\begin{aligned} x^2 &= 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot (-1) \cdot (-2) \cdot (-3) \cdots \left(-\frac{p-1}{2}\right) \equiv \\ &\equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \equiv (p-1)! \equiv -1 \pmod{p}, \end{aligned}$$

dove l'ultimo passaggio segue dal teorema di Wilson (Esercizio 5.14). □

Siamo pronti per enunciare un famoso teorema che riguarda i primi $p \equiv 1 \pmod 4$.

TEOREMA 11.25. *Sia $p \in \mathbb{Z}$ un numero primo della forma $4n+1$. Allora p non è irriducibile in $\mathbb{Z}[i]$ ed esistono $a, b \in \mathbb{Z}$ tali che $p = a^2+b^2$.*

DIMOSTRAZIONE. Basta dimostrare che p non è irriducibile in $\mathbb{Z}[i]$, il resto dell'enunciato segue poi dal Lemma 11.23. Scegliamo $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \pmod{p}$ (tale x esiste per il Lemma 11.24). Dunque $p \mid x^2+1 = (x-i)(x+i)$, e se p fosse irriducibile in $\mathbb{Z}[i]$ sarebbe anche un elemento primo di $\mathbb{Z}[i]$ (visto che $\mathbb{Z}[i]$ è euclideo), pertanto dovrebbe valere $p \mid (x+i)$ per esempio. Questo vorrebbe dire che esistono $c, d \in \mathbb{Z}$ tali che $p(c+di) = x+i$. Uguagliando le parti immaginarie, dovrebbe valere $pd = 1$, che è assurdo. □

OSSERVAZIONE 11.26. Possiamo per esempio scrivere: $5 = 1^2+2^2$, $13 = 2^2+3^2$, $17 = 1^2+4^2$, $29 = 2^2+5^2$, $37 = 1^2+6^2$, $41 = 4^2+5^2$ e così via...

Il fatto che un numero primo del tipo $4n+1$ si possa scrivere come somma di due quadrati di numeri interi fu enunciato da Fermat, senza dimostrazione, in una lettera a Mersenne datata 25 Dicembre 1640: perciò viene talvolta chiamato 'Fermat's Christmas

Theorem'. La prima dimostrazione fu poi scritta da Eulero, mentre quella che usa gli interi di Gauss è dovuta a Dedekind.[2]

Completiamo il quadro mostrando che il risultato non è vero per i numeri primi congrui a 3 modulo 4.

TEOREMA 11.27. *Sia p un primo dispari della forma $4n+3$. Allora p non può essere scritto come somma di due quadrati.*

DIMOSTRAZIONE. Supponiamo che $p = a^2+b^2$ con $a, b \in \mathbb{Z}$. Dato che p è dispari deve essere che a e b sono uno pari e l'altro dispari; senza perdita di generalità supponiamo a pari e b dispari. Allora $a^2 \equiv 0 \pmod 4$ e $b^2 \equiv 1 \pmod 4$ (verificate!) e

$$p = a^2 + b^2 \equiv 1 + 0 \equiv 1 \pmod 4,$$

Ma questo è assurdo perché $p \equiv 3 \pmod 4$. □

COROLLARIO 11.28. *I primi della forma $4n+3$ sono irriducibili in $\mathbb{Z}[i]$.*

DIMOSTRAZIONE. Sappiamo dal Lemma 11.23 che se un primo dispari non è irriducibile in $\mathbb{Z}[i]$ allora può essere scritto come somma di due quadrati. Non potendo i primi della forma $4n+3$ essere scritti in tal modo, ne segue che devono essere irriducibili in $\mathbb{Z}[i]$. □

TEOREMA 11.29. *Tutti e soli gli irriducibili di $\mathbb{Z}[i]$ sono (a meno di associati) i primi di $\mathbb{Z}$ della forma $4n+3$ e gli $z \in \mathbb{Z}[i]$ tali che $g(z) = |z|^2$ è un primo di $\mathbb{Z}$.*

DIMOSTRAZIONE. ($\Longleftarrow$) Se p è un primo della forma $4n+3$ il corollario precedente ci dice che è irriducibile in $\mathbb{Z}[i]$. Se $g(z) = p$, con p primo, allora z è irriducibile perché se scriviamo $z = w_1 w_2$ allora, passando ai quadrati delle norme abbiamo $p = |w_1|^2|w_2|^2$ e quindi una delle due norme deve essere uguale a 1, dunque uno dei fattori di z è invertibile. ($\Longrightarrow$) Sia $z \in \mathbb{Z}[i]$ irriducibile. Intanto $z \mid z\overline{z} = g(z) = q_1 \dots q_s$ dove i q_i sono primi in $\mathbb{Z}$ (ossia abbiamo fattorizzato $g(z)$ in $\mathbb{Z}$). Essendo z un elemento primo in $\mathbb{Z}[i]$ si ha che $z \mid q_i$ per un certo i. Deve essere dunque $zw = q_i$ per un certo $w \in \mathbb{Z}[i]$. Se w è invertibile allora z è associato a q_i in $\mathbb{Z}[i]$, e dunque q_i è irriducibile in $\mathbb{Z}[i]$. Ma allora, per quanto visto in questo paragrafo, q_i è un primo della forma $4n+3$. Quindi z, a meno di associati, è un primo di tale tipo. Se invece w non è invertibile allora $|w|^2 \neq 1$; passando ai quadrati delle norme, si osserva che

$$|z|^2|w|^2 = q_i^2.$$

da cui si deduce $|w|^2 = q_i$ e $|z|^2 = q_i$. □

5. Complementi (facoltativo): esempio di un dominio non UFD, in cui esistono elementi irriducibili ma non primi

La nostra attenzione adesso si sposta sugli anelli del tipo $\mathbb{Z}[\sqrt{n}]$ e $\mathbb{Z}[i\sqrt{n}]$. Gli interi di Gauss appartengono a questa famiglia di anelli.
Intanto osserviamo che se n è un quadrato allora $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$, quindi in questo paragrafo n non sarà un quadrato e anzi sarà un elemento in $\mathbb{Z}$ 'squarefree', ovvero uguale ad un prodotto di primi distinti, tutti con esponente uguale a 1. Inoltre adotteremo la notazione per cui per esempio $\mathbb{Z}[\sqrt{-14}]$ significa $\mathbb{Z}[i\sqrt{14}]$.

[2]Richard Dedekind, matematico tedesco, 1831-1916.

Questi anelli, come vedremo, in generale non sono euclidei. È possibile comunque definire su di essi una "seminorma" nel modo seguente

$$\begin{array}{rccc} \ell: & \mathbb{Z}[\sqrt{n}] & \longrightarrow & \mathbb{Z} \\ & a+b\sqrt{n} & \longmapsto & a^2-nb^2 \end{array}.$$

LEMMA 11.30. *L'applicazione ℓ è moltiplicativa.*

DIMOSTRAZIONE. Consideriamo $\mathbb{Z}[\sqrt{n}]$ e due elementi $a+b\sqrt{n}$ e $c+d\sqrt{n}$ dell'anello. Intanto

$$\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right) = ac+bdn+(ad+bc)\sqrt{n},$$

da cui

$$\begin{aligned} \ell\left(\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right)\right) &= (ac+bdn)^2-n(ad+bc)^2 \\ &= a^2c^2+2abcdn+b^2d^2n^2-a^2d^2n-2abcdn-b^2c^2n = \\ &= c^2(a^2-nb^2)-nd^2(a^2-nb^2) = (a^2-nb^2)(c^2-nd^2) = \\ &= \ell\left(a+b\sqrt{n}\right)\ell\left(c+d\sqrt{n}\right), \end{aligned}$$

□

LEMMA 11.31. *Un elemento $z \in \mathbb{Z}[\sqrt{n}]$ è invertibile se e solo se $\ell(z) \in \{1,-1\}$.*

DIMOSTRAZIONE. ($\Longrightarrow$) Se $z \in \mathbb{Z}[\sqrt{n}]$ ed è invertibile allora $zw = 1$ per qualche $w \in \mathbb{Z}[\sqrt{n}]$. Per il lemma precedente si ha $\ell(z)\ell(w) = \ell(1) = 1$ e dunque $\ell(z) \in \{1,-1\}$. ($\Longleftarrow$) Sia $z = a+b\sqrt{n}$ con $|\ell(z)| = 1$, allora $|a^2-nb^2| = 1$. Ma allora possiamo scrivere $(a+b\sqrt{n})(a-b\sqrt{n}) = 1$ o $(a+b\sqrt{n})(-a+b\sqrt{n}) = 1$, e in ogni caso z è invertibile. □

Studiando gli anelli di questo tipo ci possiamo imbattere per esempio in anelli che non sono a fattorizzazione unica.

LEMMA 11.32. *L'anello $\mathbb{Z}[\sqrt{10}]$ non è un dominio a fattorizzazione unica. Inoltre in $\mathbb{Z}[\sqrt{10}]$ non è vero che ogni irriducibile è primo.*

DIMOSTRAZIONE. Per esempio osserviamo che 6 possiamo scriverlo nei due modi che seguono:

$$(4+\sqrt{10})(4-\sqrt{10}) = 6 = 2\cdot 3,$$

ma per concludere che $\mathbb{Z}[\sqrt{10}]$ non è UFD dobbiamo essere sicuri che gli elementi che appaiono nelle due fattorizzazioni siano irriducibili. Mostriamo che 2 e 3 sono elementi irriducibili; se $2 = (a+b\sqrt{10})(c+d\sqrt{10})$ fosse una fattorizzazione senza invertibili allora

$$\ell(a+b\sqrt{10})\ell(c+d\sqrt{10}) = \ell(2) = 4$$

e quindi le due norme a primo membro dovrebbero essere entrambe uguali a 2 o a -2 (non potrebbe essere che una delle due è uguale a ± 1, perché in tal caso l'elemento sarebbe invertibile). Ma ciò non è possibile perch $a^2-10b^2 = \pm 2$ non ha soluzioni intere. Procedendo in modo analogo per il 3 si ottiene che anche 3 è irriducibile, visto che $a^2-10b^2 = \pm 3$ non ha soluzioni intere. L'irriducibilità di $(4+\sqrt{10})$ e $(4-\sqrt{10})$ è una conseguenza dei conti già svolti. Infatti tali elementi hanno seminorma 6: dunque per esempio se $(4+\sqrt{10})$ avesse una fattorizzazione senza invertibili, i due fattori dovrebbero avere seminorma rispettivamente uguale a 2 e a 3, ma abbiamo già visto che nell'anello non ci sono elementi di questo tipo.

Infine osserviamo che 2 è irriducibile ma non è primo. Infatti $2 \mid (4+\sqrt{10})(4-\sqrt{10})$ ma non divide nessuno dei due fattori: uno dei tanti modi per vederlo è che se fosse $2(a+b\sqrt{10}) = 4+\sqrt{10}$ allora varrebbe $\ell(2)|\ell(4+\sqrt{10})$ che è falso perché 4 non divide 6. □

6. Esercizi

Esercizio 11.33. Consideriamo $\mathbb{Z}[x]$, l'anello dei polinomi a coefficienti in $\mathbb{Z}$. Chiamiamo I l'insieme dei polinomi $p(x)$ tali che $p(0)$ è pari. Dimostrare che I è un ideale di $\mathbb{Z}[x]$ e che non può essere generato da un solo elemento. Dunque $\mathbb{Z}[x]$ non è PID.

Esercizio 11.34. Sia D un dominio a ideali principali. Un ideale $I \neq \{0\}$ di D è primo se e solo se è massimale.

Esercizio 11.35. Sia $A = \mathbb{Z}_{10}$: mostrare che esiste in A un elemento primo che non è irriducibile. [La definizione di elemento primo e di elemento irriducibile la abbiamo data per domini, ma immaginate come potreste estenderla a tutti gli anelli.]

Esercizio 11.36. Fattorizzare come prodotto di irriducibili l'elemento 2 in $\mathbb{Z}[i]$.

Esercizio 11.37. Decidere se 5 è irriducibile in $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}[i]$ (e se volete provate anche in $\mathbb{Z}[i\sqrt{2}]$).

Esercizio 11.38. Fattorizzare $43i - 19$ in prodotto di irriducibili in $\mathbb{Z}[i]$.

Esercizio 11.39. Dimostrare che in un UFD un elemento è irriducibile se e solo se è primo.

Esercizio 11.40. Utilizzando i risultati sugli anelli euclidei e quelli del Paragrafo 4 possiamo anche dimostrare che un numero primo della forma $4n + 1$ può essere scritto *in modo unico* come somma di due quadrati di numeri interi?

Esercizio 11.41. Trovare tutte le rappresentazioni di 2425 come somma di due quadrati.

Esercizio 11.42. Consideriamo in $\mathbb{R}[x]$ i polinomi $f(x) = x^4+x^3-x-1$, $g(x) = x^{10}-x^7$ e sia I l'ideale $(f(x), g(x))$. Determinare gli ideali massimali di $\mathbb{R}[x]$ che contengono I.

CAPITOLO 12

Lezione del 26 novembre

1. 'Inventare' radici di polinomi

Consideriamo un campo K e un polinomio $f(x) \in K[x]$ irriducibile e di grado ≥ 2. Tale polinomio non ha radici in K, altrimenti per il teorema di Ruffini[1] si potrebbe fattorizzare in $K[x]$. Poniamoci il seguente problema: è possibile trovare un campo E che contiene K, tale che il polinomio $f(x)$ abbia una radice in E?

Abbiamo tutti gli elementi per rispondere. Consideriamo l'ideale $(f(x))$ e il quoziente $K[x]/(f(x))$. Poiché $f(x)$ è irriducibile in $K[x]$ sappiamo, per il Teorema 11.17, che $(f(x))$ è massimale, e dunque il quoziente $K[x]/(f(x))$ è un campo, che chiameremo E. Osserviamo che il campo E contiene K, o, più esattamente, contiene un sottocampo isomorfo a K. Infatti nella proiezione al quoziente

$$\pi \, : \, K[x] \to E = K[x]/(f(x))$$

i polinomi costanti $k \in K[x]$ hanno come immagine le classi $k + (f(x))$ e, visto come sono state definite le operazioni nel quoziente, l'insieme di tali classi costituisce un sottocampo di E isomorfo a K: per non appesantire la notazione chiameremo tale sottocampo ancora K e nel futuro indicheremo spesso solo con k la classe $k + (f(x))$.

Visto che $K \subset E$, il polinomio $f(x) \in K[x]$ può essere pensato anche come un polinomio in $E[x]$. Mostreremo che $f(x)$ ha una radice in E.

Per 'trovare' una radice basta considerare in E l'elemento $\overline{x} = x + (f(x))$.

Infatti, poniamo che $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, con i coefficienti a_i appartenenti a K. e proviamo a valutare quale elemento di E è $f(\overline{x})$. Si tratta di fare un conto nel quoziente, e per migliorare la notazione chiameremo $I = (f(x))$:

$$f(\overline{x}) = a_n (x + I)^n + a_{n-1} (x + I)^{n-1} + \cdots + a_1 (x + I) + a_0$$

Ora, ricordando come sono state definite le operazioni nel quoziente, sviluppando il conto troviamo

$$f(\overline{x}) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 + I = f(x) + I$$

Ma, visto che $f(x) \in I$, l'elemento $f(x) + I$ è uguale a $0 + I$, dunque $\overline{x}$ è una radice di $f(x)$.

Concludiamo facendo una osservazione sulla dimensione di $K[x]/(f(x))$ visto come spazio vettoriale su K.

TEOREMA 12.1. *Consideriamo un campo K e un polinomio $f(x) \in K[x]$ irriducibile. Allora il campo $E = K[x]/(f(x))$ è uno spazio vettoriale su K di dimensione deg f.*

DIMOSTRAZIONE. L'osservazione che si tratta di uno spazio vettoriale è una semplice conseguenza del fatto che $K \subseteq E$ è una estensione di campi: la somma in E è ben definita ed è ben definita anche la moltiplicazione per gli 'scalari', che sono gli elementi di K.

[1] Lo avete visto a esercitazioni, è una conseguenza dell'esistenza della divisione euclidea in $K[x]$: $\alpha \in K$ è una radice di un polinomio $f(x) \in K[x]$ se e solo se $x - \alpha$ divide $f(x)$ in $K[x]$.

Per quello che riguarda la dimensione, basta osservare che gli elementi

$$1 + (f(x)), x + (f(x)), x^2 + (f(x)), \ldots\ldots, x^{deg\ f-1} + (f(x))$$

sono una base.

□

2. Approfondimenti sulle estensioni semplici di campi

Nel paragrafo precedente abbiamo visto come sia possibile, dato un campo K e un polinomio $f(x) \in K[x]$ irriducibile e di grado ≥ 2, 'creare' un nuovo campo, che contiene K, dove $f(x)$ ammette una radice. Ma talvolta noi conosciamo già un campo che contiene K e in cui il polinomio ha una radice: per esempio, nel caso del polinomio $x^3 - 2 \in \mathbb{Q}[x]$, noi sappiamo che tale polinomio non ha radici razionali ma che in $\mathbb{R}$ esiste una radice, cioè $\sqrt[3]{2}$. Che relazione c'è fra il campo $\mathbb{Q}[x]/(x^3 - 2)$ costruito nel paragrafo precedente e la presenza di una radice di $x^3 - 2$ in $\mathbb{R}$?

Per rispondere, affrontiamo la situazione da un punto di vista generale. Premettiamo intanto la definizione di sottocampo:

Definizione 12.2. Dati un campo E ed un sottoanello A di E, si dice che A è un *sottocampo* di E se per ogni $a \in A$ diverso da 0 l'inverso di a appartiene ad A.

Sia K un campo e sia L un campo che è una *estensione* di K, ossia vale $K \subseteq L$. Dato $\alpha \in L$, consideriamo adesso tutti i sottocampi di L che contengono K e α. La loro intersezione è ancora un sottocampo di L (facile esercizio) che contiene K e α. Per costruzione, si tratta del minimo sottocampo di L (minimo rispetto all'inclusione) che contiene K e α. Visto che questo minimo sottocampo esiste, lo valorizziamo con una notazione apposita:

Definizione 12.3. Dati due campi $K \subseteq L$ e un elemento $\alpha \in L$, indicheremo con $K(\alpha)$ il minimo sottocampo (rispetto all'inclusione) di L che contiene K e α. Si dice che $K(\alpha)$ è una *estensione semplice* di K.

Dati $K \subseteq L$ e $\alpha \in L$, come sopra, possiamo considerare l'omomorfismo di valutazione

$$\psi : K[x] \to L$$

tale che, per ogni $f(x) \in K[x]$, $\psi(f(x)) = f(\alpha)$.

Indicheremo anche con il simbolo $K[\alpha]$ l'immagine di ψ. Possiamo in effetti vedere gli elementi di Imm ψ come i polinomi in α a coefficienti in K.

Qual è il nucleo di ψ? I suoi elementi sono tutti i polinomi $g(x) \in K[x]$ tali che $g(\alpha) = 0$. Sappiamo che $\operatorname{Ker}\psi$ è un ideale e, visto che $K[x]$ è euclideo e dunque PID, $\operatorname{Ker}\psi$ è un ideale principale.

Possiamo allora scrivere

$$\operatorname{Ker}\psi = (f(x))$$

per un certo polinomio $f \in K[x]$.

Ci sono due casi. Il primo è che $\operatorname{Ker}\psi = \{0\}$. Ovvero α non è radice di nessun polinomio a coefficienti in K (a parte ovviamente il polinomio 0). Si dice in tal caso che $\alpha \in L$ è un elemento *trascendente su* K. Per il primo teorema di omomorfismo sappiamo che $K[x] \cong K[\alpha] = \operatorname{Imm}\psi$. In particolare $K[\alpha]$ non è un campo e dunque $K[\alpha] \subsetneq K(\alpha)$.

Osservazione 12.4. Come è noto (ma non lo dimostreremo in questo corso) i numeri reali π ed e, il numero di Eulero base dei logaritmi, sono due esempi di numeri trascendenti su $\mathbb{Q}$.[2]

L'altro caso è che $\operatorname{Ker}\psi = (f(x)) \neq \{0\}$. In tal caso si dice che α è algebrico su K, nel senso della seguente definizione:

Definizione 12.5. Dati due campi $K \subseteq L$ si dice che un elemento $\alpha \in L$ è *algebrico su* K se esiste un polinomio non nullo in $K[x]$ di cui α è radice, ossia se il nucleo $\operatorname{Ker}\psi$ della valutazione definita sopra è diverso da 0. Un generatore $f(x)$ di $\operatorname{Ker}\psi$ si chiama *polinomio minimo di* α *su* K.

Osservazione 12.6. Come avrete subito notato, un polinomio minimo non è unico, ma è unico a meno di associati. L'aggettivo 'minimo' si riferisce al fatto che tale polinomio ha grado minimo fra tutti i polinomi di $K[x]$ che hanno α come radice. Talvolta viene usata la convenzione per cui fra tutti i polinomi associati che sono polinomi minimi quello che ha coefficiente direttore uguale a 1 viene chiamato *il* polinomio minimo di α su K.

Continuiamo a studiare il caso in cui α è algebrico su K e pertanto $\operatorname{Ker}\psi = (f(x)) \neq \{0\}$. Osserviamo che allora $f(x)$ è irriducibile in $K[x]$. Si può vedere in molti modi: per esempio se $f(x) = h_1(x)h_2(x)$ fosse una fattorizzazione in $K[x]$ con $h_1(x), h_2(x)$ non costanti, e dunque $deg\ h_1(x) < deg\ f(x)$ e $deg\ h_2(x) < deg\ f(x)$, valutando in α avremmo $f(\alpha) = 0 = h_1(\alpha)h_2(\alpha)$. Allora deve valere $h_1(\alpha) = 0$ oppure $h_2(\alpha) = 0$, ossia $h_1(x) \in \operatorname{Ker}\psi$ oppure $h_2(x) \in \operatorname{Ker}\psi$, che è assurdo perché $f(x)$, generatore dell'ideale $\operatorname{Ker}\psi$, ha grado maggiore di $h_1(x)$ e $h_2(x)$.

Dunque l'ideale $(f(x))$ è massimale, per il Teorema 11.17

Osservazione 12.7. Anche usando l'Esercizio 11.34 che dice che in un PID ogni ideale primo non zero è massimale si può dimostrare rapidamente che $\operatorname{Ker}\psi = (f(x))$ è massimale, perché dal fatto che il quoziente $K[x]/\operatorname{Ker}\psi$ è isomorfo al sottoanello $\operatorname{Imm}\psi$ di L si ricava che $K[x]/\operatorname{Ker}\psi$ è un dominio e dunque $\operatorname{Ker}\psi$ è primo.

Torniamo a studiare il nostro omomorfismo di valutazione ψ nel caso che α sia algebrico su K. Dal fatto che $(f) = \operatorname{Ker}\psi$ è massimale e dal primo teorema di isomorfismo ricaviamo che $\operatorname{Imm}\psi = K[\alpha]$ è un campo: più esattamente è un sottocampo di L che contiene K e α, dunque contiene il campo $K(\alpha)$. Si osserva subito anche che tutti i polinomi in α devono appartenere a $K(\alpha)$, dunque $K[\alpha] \subseteq K(\alpha)$, per cui vale $K[\alpha] = K(\alpha)$.

Questo potrebbe suscitare un dubbio.

Per esempio se $K = \mathbb{Q}$, $L = \mathbb{R}$ e $\alpha = \sqrt[3]{2}$, sappiamo che sia $1 + \sqrt[3]{2}$ sia il suo inverso $\dfrac{1}{1+\sqrt[3]{2}}$ devono appartenere al campo $\mathbb{Q}(\sqrt[3]{2})$.

Però abbiamo appena visto che in realtà $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$: vogliamo renderci conto come sia possibile che $\dfrac{1}{1+\sqrt[3]{2}}$ appartenga a $\mathbb{Q}[\sqrt[3]{2}]$.

Per la verità questo caso è semplice, e potremmo subito esibire un polinomio in $\sqrt[3]{2}$ uguale a $\dfrac{1}{1+\sqrt[3]{2}}$, ma sviluppare nei dettagli questo esempio potrà essere illuminante.

Consideriamo dunque l'omomorfismo di valutazione $\psi : \mathbb{Q}[x] \to \mathbb{R}$ che valuta ogni polinomio in $\sqrt[3]{2}$. Si nota subito che il polinomio minimo di $\sqrt[3]{2}$ è $x^3 - 2$, ossia che

[2]Osservazione per gli amanti dell'infinito: i numeri algebrici sono un sottoinsieme infinito numerabile di $\mathbb{R}$ (potreste provare a dimostrarlo per esercizio), dunque i numeri trascendenti sono in realtà 'di più' dei numeri algebrici (se fossero un infinito numerabile allora $\mathbb{R}$ sarebbe numerabile...).

$\operatorname{Ker}\psi = (x^3-2)$. Infatti (x^3-2) è incluso in $\operatorname{Ker}\psi$ ma si può vedere facilmente che x^3-2 è irriducibile in $\mathbb{Q}[x]$,[3] dunque (x^3-2) è massimale. Questo significa che ci sono solo due possibilità per $\operatorname{Ker}\psi$: $\operatorname{Ker}\psi = \mathbb{Q}[x]$ oppure $\operatorname{Ker}\psi = (x^3-2)$. La prima di queste possibilità va scartata perché vorrebbe dire che la valutazione ψ è l'omomorfismo che manda ogni elemento in 0, cosa falsa (per esempio $\psi(1) = 1$).[4]

Dunque

$$\mathbb{Q}[\sqrt[3]{2}] \cong Q[x]/(x^3-2)$$

Ora riflettiamo sul quoziente $\mathbb{Q}[x]/(x^3-2)$. Ogni elemento di $\mathbb{Q}[x]/(x^3-2)$ si può rappresentare come

$$ax^2+bx+c+(x^3-2)$$

con $a, b, c \in \mathbb{Q}$. Per esempio consideriamo l'elemento

$$x+1+(x^3-2)$$

Visto che il massimo comun divisore fra $x+1$ e x^3-2 è 1, per il Lemma di Bezout per polinomi è possibile scrivere 1 come combinazione lineare di $x+1$ e x^3-2 a coefficienti in $\mathbb{Q}[x]$. Nel caso in questione è semplicissimo trovare questa combinazione lineare, perchè l'algoritmo di Euclide è molto breve:

$$x^3-2 = (x^2-x+1)(x+1)-3$$

dunque dopo una divisione possiamo scrivere

$$1 = -\frac{1}{3}(x^3-2)+\frac{1}{3}(x^2-x+1)(x+1)$$

Una immediata verifica ci mostra a questo punto che le due classi $x+1+(x^3-2)$ e $\frac{1}{3}(x^2-x+1)+(x^3-2)$ sono una l'inversa dell'altra in $\mathbb{Q}[x]/(x^3-2)$.

D'altra parte, se valutiamo l'uguaglianza fra polinomi

$$1 = -\frac{1}{3}(x^3-2)+\frac{1}{3}(x^2-x+1)(x+1)$$

ponendo $x = \sqrt[3]{2}$, otteniamo

$$1 = -\frac{1}{3}((\sqrt[3]{2})^3-2)+\frac{1}{3}((\sqrt[3]{2})^2-\sqrt[3]{2}+1)(\sqrt[3]{2}+1)$$

ossia

$$1 = \frac{1}{3}((\sqrt[3]{2})^2-\sqrt[3]{2}+1)(\sqrt[3]{2}+1)$$

Questo ci dice che in $\mathbb{R}$

$$\frac{1}{\sqrt[3]{2}+1} = \frac{1}{3}((\sqrt[3]{2})^2-\sqrt[3]{2}+1)$$

Abbiamo mostrato che l'inverso di $\sqrt[3]{2}+1$ può essere scritto come polinomio in $\sqrt[3]{2}$ ed appartiene pertanto a $\mathbb{Q}[\sqrt[3]{2}]$.

Questo ragionamento, ripetuto per ogni elemento non zero, ci mostra concretamente come mai $\mathbb{Q}[\sqrt[3]{2}]$ è un campo e ci indica come trovare gli elementi inversi.

---

[3]Questo si può fare osservando che il polinomio ha grado 3 e se fosse riducibile dovrebbe avere un fattore di grado 1, dunque dovrebbe avere una radice razionale. Ma si verifica facilmente che x^3-2 non ammette radici razionali. Comunque ad esercitazioni imparerete vari criteri che possono essere usati per dimostrare che un polinomio è irriducibile, e fra questi il criterio di Eisenstein adatto al nostro caso.

[4]Questa osservazione ci fa riflettere sul fatto che, in generale, se abbiamo un omomorfismo di anelli con unità $g : A \to B$, il nucleo di g è uguale ad A se e solo se B è l'anello banale $B = \{0\}$.

Una ulteriore domanda che potremmo porci è la seguente. Sappiamo che il polinomio $x^3 - 2$ ammette altre due radici in $\mathbb{C}$, ovvero $\sqrt[3]{2}\omega$ e $\sqrt[3]{2}\omega^2$, dove $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\imath$ è una radice cubica di 1.

Analogamente a quanto visto per $\mathbb{Q}[\sqrt[3]{2}]$, utilizzando l'omomorfismo di valutazione

$$\psi' : \mathbb{Q}[x] \to \mathbb{C}$$

tale che per ogni $g(x) \in \mathbb{Q}[x]$ $\psi(g(x) = g(\sqrt[3]{2}\omega)$, possiamo concludere che $\mathbb{Q}[\sqrt[3]{2}\omega]$ è isomorfo a $\mathbb{Q}[x]/(x^3 - 2)$.

Dunque abbiamo la seguente situazione

$$\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}\omega]$$

Se chiamiamo $\theta : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}\omega]$ l'isomorfismo che si ottiene, è facile osservare che θ lascia fissi gli elementi di $\mathbb{Q}$ e $\theta(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ (infatti nell'isomorfismo a sinistra $\sqrt[3]{2}$ viene mandato in $\overline{x}$ e in quello a destra $\overline{x}$ viene mandato in $\sqrt[3]{2}\omega$).

La stessa cosa si può dire di $\mathbb{Q}[\sqrt[3]{2}\omega^2]$. Abbiamo dunque individuato tre sottocampi di $\mathbb{C}$ isomorfi fra loro.

La cosa si può esporre in generale attraverso il seguente teorema:

Teorema 12.8. *Dati due campi $K \subseteq L$, sia $f(x)$ un polinomio irriducibile in $K[x]$ che ha due radici distinte α e β in L. Allora esiste un isomorfismo $\theta : K[\alpha] \to K[\beta]$ fra i campi $K[\alpha]$ e $K[\beta]$ tale che $\theta(\alpha) = \beta$ e θ ristretto a K sia l'identità.*

Dimostrazione. La dimostrazione ricalca esattamente quella illustrata nell'esempio, dunque la lascio a voi come esercizio. □

Talvolta può capitare che i campi $K[\alpha]$ e $K[\beta]$ che appaiono nel teorema precedente siano uguali, oltre che isomorfi: per esempio se si considera $K = \mathbb{Q}$, $L = \mathbb{C}$ e $f(x) = x^2+1$, si trova che $\mathbb{Q}(\imath) = \mathbb{Q}(-\imath)$.

In generale però $K[\alpha]$ e $K[\beta]$ non coincidono. Tornando al caso di $x^3 - 2$ che stavamo studiando, osserviamo infatti che i tre sottocampi di $\mathbb{C}$ sono tutti distinti: $\mathbb{Q}[\sqrt[3]{2}]$ certamente non coincide né con $\mathbb{Q}[\sqrt[3]{2}\omega]$ né con $\mathbb{Q}[\sqrt[3]{2}\omega^2]$ visto che $\mathbb{Q}[\sqrt[3]{2}]$ è contenuto in $\mathbb{R}$ e gli altri due invece non lo sono. Inoltre non può valere $\mathbb{Q}[\sqrt[3]{2}\omega] = \mathbb{Q}[\sqrt[3]{2}\omega^2]$ altrimenti a tale campo, come si verifica subito, dovrebbero appartenere gli elementi ω (ottenuto dividendo $\sqrt[3]{2}\omega^2$ per $\sqrt[3]{2}\omega$) e $\sqrt[3]{2}$ (ottenuto dividendo $\sqrt[3]{2}\omega$ per ω).

Dunque $\mathbb{Q}[\sqrt[3]{2}\omega] = \mathbb{Q}[\sqrt[3]{2}\omega^2]$ conterrebbe strettamente $\mathbb{Q}[\sqrt[3]{2}]$ e questo creerebbe problemi di dimensione: per il Teorema 12.1 sappiamo che gli spazi vettoriali $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[\sqrt[3]{2}\omega]$ e $Q[\sqrt[3]{2}\omega^2]$ hanno tutti dimensione 3 su $\mathbb{Q}$, pertanto se fosse $\mathbb{Q}[\sqrt[3]{2}\omega] = \mathbb{Q}[\sqrt[3]{2}\omega^2]$ tale spazio vettoriale avrebbe dimensione 3 su $\mathbb{Q}$ ma conterrebbe strettamente lo spazio vettoriale $\mathbb{Q}[\sqrt[3]{2}]$ che ha anch'esso dimensione 3 su $\mathbb{Q}$.

3. Creare un campo con tutte le radici di un polinomio

Iterando il procedimento che 'aggiunge' una radice di un polinomio, è possibile, dato un campo K e un polinomio $f(x) \in K[x]$, costruire un campo E che estende K e tale che in $E[x]$ il polinomio $f(x)$ si fattorizza nel prodotto di polinomi di grado 1.

Teorema 12.9. *Sia K un campo e sia $f(x) \in K[x]$ un polinomio di grado $n \geq 0$. Allora esistono un campo E tale che $K \subseteq E$ ed elementi $e_1, e_2, ..., e_n$ (eventualmente con ripetizioni) appartenenti ad E tali che $f(x)$ si fattorizza nel seguente modo in $E[x]$:*

$$f(x) = \lambda(x - e_1)(x - e_2)\cdots(x - e_n)$$

dove $\lambda \in E$ è una costante.

DIMOSTRAZIONE. Per induzione su $n = deg\ f(x)$. Il passo base ($deg\ f(x) = 0$) è una immediata verifica. Supponiamo ora che $n = deg\ f(x) \geq 1$ e sia $f_1(x)$ un fattore irriducibile di $f(x)$. Costruiamo il campo $F = K[x]/(f_1(x))$: come sappiamo dal paragrafo precedente, in tale campo esiste una radice $\overline{x}$ di $f_1(x)$, e poniamo $e_1 = \overline{x}$. A questo punto in $F[x]$ abbiamo la seguente fattorizzazione:

$$f(x) = (x - e_1)g(x)$$

dove $g(x)$ è un polinomio di grado $n - 1$. Per ipotesi induttiva sappiamo che esiste un campo E che estende F ed elementi $e_2, ..., e_n$ in E tali che $g(x)$ si fattorizza nel seguente modo in $E[x]$:

$$g(x) = \lambda(x - e_2) \cdots (x - e_n)$$

con $\lambda \in E$. Per concludere osserviamo che E estende K in quanto $K \subseteq F \subseteq E$ e in $E[x]$ il polinomio $f(x)$ si fattorizza come

$$f(x) = \lambda(x - e_1)(x - e_2) \cdots (x - e_n)$$

□

4. Esercizi

ESERCIZIO 12.10. Consideriamo $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\imath$, radice cubica di 1, e l'estensione semplice $\mathbb{Q}(\omega)$. Qual è la dimensione di $\mathbb{Q}(\omega)$ come spazio vettoriale su $\mathbb{Q}$? Qual è il polinomio minimo di $\sqrt[3]{2}$ sul campo $\mathbb{Q}(\omega)$?

ESERCIZIO 12.11. Trovare il polinomio minimo di $\imath + \sqrt{2}$ su $\mathbb{Q}$.

ESERCIZIO 12.12. Calcolare la dimensione su $\mathbb{Q}$ di $\mathbb{Q}(\sqrt{5})(\imath) = \mathbb{Q}(\sqrt{5}, \imath)$.[5]

ESERCIZIO 12.13. Sia $\alpha \in \mathbb{C}$ una radice di $x^4 + 1$. Qual è la dimensione di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$? È vero o falso che $x^4 + 1$ si fattorizza come prodotto di fattori di grado 1 in $\mathbb{Q}(\alpha)$?

[5]In seguito, dato un campo K incluso in un campo L, e dati degli elementi $\alpha, \beta, \gamma... \in L$, useremo spesso la notazione $K(\alpha, \beta, \gamma, ...)$ per indicare il campo $K(\alpha)(\beta)(\gamma)$ costruito per estensioni successive. È facile mostrare che tale campo è il più piccolo sottocampo di L che contiene K e $\alpha, \beta, \gamma, ...$, dunque la notazione scelta è una naturale generalizzazione di quella per le estensioni semplici.

CAPITOLO 13

Lezione del 27 novembre

1. Alcune considerazioni sul grado delle estensioni di campi

Dati due campi $F \subseteq K$ diremo che K è una estensione di F. Come abbiamo già osservato nei casi di estensioni studiati nelle lezioni precedenti, K si può vedere anche come uno spazio vettoriale su F. La struttura di spazio vettoriale è quella indotta dal fatto che K è un campo: è già definita la somma fra due elementi di K e anche anche la moltiplicazione per 'scalare' γk, per ogni $\gamma \in F$ e per ogni $k \in K$.

In questa lezione vogliamo discutere alcune informazioni che possiamo ricavare da questa struttura di spazio vettoriale.

DEFINIZIONE 13.1. Dati due campi $F \subseteq K$, il *grado* di K su F è la dimensione di K come spazio vettoriale su F e si indica con il simbolo $[K : F]$. Se la dimensione è infinita si scrive $[K : F] = \infty$. Se il grado è finito, si dice che K è una estensione finita di F, altrimenti si dice che è una estensione infinita.

TEOREMA 13.2. *Se L è una estensione finita di K e K è una estensione finita di F, allora L è una estensione finita di F e*

$$[L : F] = [L : K][K : F]$$

DIMOSTRAZIONE. Un modo per calcolare $dim_F L$ è quello di esibire una base di L su F e contarne gli elementi.

Sia $v_1, ..., v_m$ una base di L su K, e sia inoltre $w_1, ..., w_n$ una base di K su F. Allora l'enunciato del teorema segue dall'osservazione che l'insieme $\{v_i w_j\}$ (dove l'indice i varia fra 1 e m e l'indice j varia fra 1 e n) è una base di L su F costituita da mn elementi.

Infatti, per ogni vettore $v \in L$ possiamo scrivere

$$v = a_1 v_1 + \cdots + a_m v_m$$

con i coefficienti $a_i \in K$. Ma ciascuno degli a_i si può scrivere come

$$a_i = b_{i1} w_1 + \cdots + b_{in} w_n$$

con i coefficienti $b_{ij} \in F$. In conclusione possiamo scrivere

$$v = \sum_{\substack{i = 1, ..., m \\ j = 1, ..., n}} b_{ij} v_i w_j$$

Questo dimostra che gli elementi $v_i w_j$ generano L su F.

D'altra parte se abbiamo l'uguaglianza

$$\sum_{\substack{i = 1, ..., m \\ j = 1, ..., n}} b_{ij} v_i w_j = 0$$

con i coefficienti $b_{ij} \in F$, allora raggruppando i termini possiamo scrivere

$$\sum_{\substack{i=1,...,m \\ j=1,...,n}} b_{ij} v_i w_j = \sum_{i=1,...,m} (b_{i1} w_1 + \cdots + b_{in} w_n) v_i = 0$$

dove le somme fra parentesi $(b_{i1} w_1 + \cdots + b_{in} w_n)$ appartengono a K, e dal fatto che $v_1, ..., v_m$ è una base di L su K si deduce che sono tutte uguali a 0, ovvero

$$b_{i1} w_1 + \cdots + b_{in} w_n = 0$$

per ogni $i = 1, ..., m$. Visto che $w_1, ..., w_m$ è una base di K su F si deduce che i coefficienti b_{ij} che compaiono in queste uguaglianze sono tutti uguali a 0. Questo prova la lineare indipendenza dell'insieme $\{v_i w_j\}$. □

COROLLARIO 13.3. *Se L è una estensione finita di F e $F \subseteq K \subseteq L$ allora K è una estensione finita di F e L è una estensione finita di K. Inoltre $[L : F] = [L : K][K : F]$.*

DIMOSTRAZIONE. Consideriamo L come spazio vettoriale su F. Visto che questo spazio vettoriale ha dimensione finita e che K è un suo sottospazio vettoriale, allora anche K ha dimensione finita su F.

L'altra cosa da dimostrare è che L ha dimensione finita su K, ma questo segue immediatamente dal fatto che una base di L su F è anche un insieme (finito) di generatori di L su K.

Una volta stabilito che le due estensioni $F \subseteq K$ e $K \subseteq L$ sono finite si conclude applicando il Teorema 13.2. □

TEOREMA 13.4. *Dati due campi $F \subseteq K$, un elemento $a \in K$ è algebrico su F se e solo se $F(a)$ è una estensione finita di F.*

DIMOSTRAZIONE. Se $[F(a) : F] = m \in \mathbb{N}$ allora l'insieme $\{1, a, a^2, ..., a^m\}$, visto che contiene $m + 1$ elementi, è un insieme di elementi linearmente dipendenti sul campo F, dunque esistono $\gamma_0, \gamma_1, ..., \gamma_m \in F$ non tutti nulli tali che

$$\gamma_m a^m + \cdots + \gamma_1 a + \gamma_0 = 0$$

e allora a è algebrico su F perché è radice del polinomio $\gamma_m x^m + \cdots + \gamma_1 x + \gamma_0 \in F[x]$.

Viceversa se a è algebrico su F sappiamo, per quanto visto nel Paragrafo 2 del Capitolo 12, che $F(a) = F[a] \cong F[x]/(f(x))$ dove $f(x)$ è il polinomio minimo di a su F. Per il Teorema 12.1 allora il grado $[F(a) : F]$ è finito ed è uguale a *deg* f. □

DEFINIZIONE 13.5. Dati due campi $F \subseteq K$, un elemento $a \in K$ si dice algebrico di grado n su F se $[F(a) : F] = n$, ovvero se il suo polinomio minimo su F ha grado n.

TEOREMA 13.6. *Dati due campi $F \subseteq K$, se $a \in K$ e $b \in K$ sono algebrici su F rispettivamente di grado m e n, allora $a \pm b$, ab e $\frac{a}{b}$ (se $b \neq 0$) sono algebrici su F di grado $\leq mn$.*

DIMOSTRAZIONE. Per prima cosa osserviamo che $[F(a) : F] = m$. Ora b, essendo algebrico su F, a maggior ragione è algebrico su $F(a)$. Sia f il polinomio minimo di b su F: dalle ipotesi sappiamo che *deg* $f = n$.

Il polinomio f potrebbe non essere irriducibile in $F(a)[x]$: in tal caso il polinomio minimo di b su $F(a)$ sarà uno dei fattori irriducibili di f in $F(a)[x]$. Dunque possiamo concludere che il grado di b su $F(a)$ è $\leq n$, ovvero che $[F(a)(b) : F(a)] \leq n$. Per il Teorema 13.2 concludiamo che

$$[F(a)(b) : F] = [F(a)(b) : F(a)][F(a) : F] \leq nm$$

Osserviamo a questo punto che il campo $F(a)(b)$ (possiamo indicarlo anche come $F(a,b)$) è il più piccolo sottocampo di K che contiene F, a e b, dunque in particolare contiene anche $a \pm b$, ab e $\dfrac{a}{b}$ (se $b \neq 0$).

Tali elementi sono allora algebrici su F, in base al seguente ragionamento: per esempio $F(a+b) \subseteq F(a,b)$, dunque per il Corollario 13.3 sappiamo che $F(a+b)$ ha grado finito $\leq mn$ su F; allora, per il Teorema 13.4, $a+b$ è algebrico su F di grado $\leq mn$.

□

Corollario 13.7. *Dati due campi $F \subseteq K$, gli elementi di K algebrici su F formano un sottocampo di K.*

Esempio 13.8. Per illustrare come si possono utilizzare i teoremi sul grado visti in questa lezione, consideriamo l'elemento $c = \sqrt{2} + \sqrt[3]{2} \in \mathbb{R}$, dimostriamo che è algebrico su $\mathbb{Q}$ di grado 6 e troviamo il suo polinomio minimo.

Osserviamo innanzitutto che il polinomio x^2-2 è irriducibile in $\mathbb{Q}[x]$ (se fosse riducibile, essendo di grado 2, dovrebbe avere una radice in $\mathbb{Q}$; ma allora, visto che conosciamo già due radici, $\sqrt{2}$ e $-\sqrt{2}$, che appartengono a $\mathbb{R}-\mathbb{Q}$, il polinomio avrebbe almeno tre radici reali, assurdo). Dunque per quanto visto nella lezione precedente $\mathbb{Q}[\sqrt{2}] \cong Q[x]/(x^2-2)$ e $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Analogamente si osserva che x^3-2 è irriducibile in $\mathbb{Q}[x]$, dunque $\mathbb{Q}[\sqrt[3]{2}] \cong Q[x]/(x^3-2)$ e $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

Per quanto osservato nella dimostrazione del Teorema 13.6 sappiamo che

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 6$$

D'altra parte, pensando alla catena di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ deduciamo per il Teorema 13.2 che $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$, cioè 2, divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$.

Analogamente, pensando alla catena di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ deduciamo che 3 divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. Dunque deve essere $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

Consideriamo ora $c = \sqrt{2} + \sqrt[3]{2}$. Possiamo scrivere:

$$(c - \sqrt{2})^3 = 2$$

e sviluppando i calcoli

$$c^3 + 6c - 2 = \sqrt{2}(3c^2 + 2)$$

Da questa uguaglianza ricaviamo intanto che $\sqrt{2} \in \mathbb{Q}(c)$. Elevando al quadrato entrambi i membri otteniamo poi

$$(c^3 + 6c - 2)^2 = 2(3c^2 + 2)^2$$

Abbiamo dunque trovato che c è radice del polinomio $x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$. Per decidere se questo polinomio è irriducibile, e dunque per decidere se è il polinomio minimo di c su $\mathbb{Q}$, possiamo adesso ricorrere ad una osservazione sui gradi delle estensioni coinvolte. Infatti per il Teorema 13.2 vale

$$[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = [\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}]$$

Ora $\mathbb{Q}(c, \sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ (la dimostrazione delle due inclusioni è immediata), dunque sappiamo che

$$[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = 6$$

Inoltre, visto che abbiamo già osservato che che $\sqrt{2} \in \mathbb{Q}(c)$, vale $[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)] = 1$. In conclusione $[\mathbb{Q}(c) : \mathbb{Q}] = 6$, dunque il polinomio minimo di c su $\mathbb{Q}$ ha grado 6, e allora $x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$ è proprio il polinomio minimo.[1]

2. Estensioni algebriche

Consideriamo estensioni di campi in cui tutti gli elementi sono algebrici sul campo base.

DEFINIZIONE 13.9. Dati due campi $F \subseteq K$, si dice che K è una estensione algebrica di F se ogni elemento di K è algebrico su F.

OSSERVAZIONE 13.10. Una estensione finita $F \subseteq K$ è algebrica. Infatti dato $a \in K$, possiamo considerare la catena di estensioni $F \subseteq F(a) \subseteq K$ e per il Corollario 13.3 vale che $F(a)$ è una estensione finita di F. Dunque a è algebrico su F per il Teorema 13.4.

Esistono però, come vedremo, estensioni algebriche che non sono finite.

TEOREMA 13.11. *Se L è una estensione algebrica di K e K è una estensione algebrica di F, allora L è una estensione algebrica di F.*

DIMOSTRAZIONE. Sia $u \in L$, vogliamo dimostrare che è algebrico su F. Visto che L è una estensione algebrica di K, sappiamo che u è radice di un polinomio

$$x^n + \gamma_{n-1}x^{n-1} + \cdots + \gamma_1 x + \gamma_0$$

con i coefficienti $\gamma_j \in K$.

Ora, K è algebrico su F e dunque $[F(\gamma_0) : F]$ è finito. Inoltre anche $[F(\gamma_0, \gamma_1) : F]$ è finito: infatti vale che $[F(\gamma_0, \gamma_1) : F(\gamma_0)]$ è finito visto che γ_1 è algebrico su F, e dunque lo è anche su $F(\gamma_0)$. Allora $[F(\gamma_0, \gamma_1) : F]$ è finito per il Teorema 13.2 sulle catene di estensioni.

Procedendo in questo modo in al più n passi si dimostra che $[F(\gamma_0, \gamma_1, ..., \gamma_{n-1}) : F]$ è finito.

Ora il grado $[F(u, \gamma_0, \gamma_1, ..., \gamma_{n-1}) : F(\gamma_0, \gamma_1, ..., \gamma_{n-1})]$ è finito perché u è algebrico su $F(\gamma_0, \gamma_1, ..., \gamma_{n-1})$ (infatti u è radice del poinomio $x^n + \gamma_{n-1}x^{n-1} + \cdots + \gamma_1 x + \gamma_0$ che appartiene a $F(\gamma_0, \gamma_1, ..., \gamma_{n-1})[x]$). Quindi per il Teorema 13.2 sulle catene di estensioni si deduce che $[F(u, \gamma_0, \gamma_1, ..., \gamma_{n-1}) : F]$ è finito. Visto che $F(u) \subseteq F(u, \gamma_0, \gamma_1, ..., \gamma_{n-1})$, per il Corollario 13.3 risulta che $F(u)$ è una estensione finita di F e dunque u è algebrico su F per il Teorema 13.4.

□

Facciamo infine una osservazione nel caso in cui $F = \mathbb{Q}$.

DEFINIZIONE 13.12. Si dice che un numero complesso z è un *numero algebrico* se z è algebrico su $\mathbb{Q}$.

I numeri algebrici formano un sottocampo $\mathcal{A}$ di $\mathbb{C}$, come sappiamo per il Corollario 13.7, e per come è stato definito $\mathcal{A}$ è algebrico su $\mathbb{Q}$. L'Esercizio 13.14 vi chiederà di verificare che $[\mathcal{A} : \mathbb{Q}] = \infty$. Le radici di un polinomio in $\mathcal{A}[x]$ sono ancora numeri algebrici, per una immediata applicazione del Teorema 13.11. Quindi, come conseguenza del Teorema Fondamentale dell'Algebra[2], osserviamo che ogni polinomio in $\mathcal{A}[x]$ ha una radice in $\mathcal{A}$ e dunque si fattorizza come prodotto di polinomi di grado 1 in $\mathcal{A}[x]$.

[1] Come vedete scriviamo 'il polinomio minimo' ma non dimenticate che questo va sempre inteso 'a meno di associati'.

[2] È stato enunciato a esercitazioni, ed è stato dimostrato nel corso di Analisi 1: ogni polinomio in $\mathbb{C}[x]$ ammette una radice in $\mathbb{C}$, e dunque si fattorizza come prodotto di fattori lineari in $\mathbb{C}[x]$.

3. La caratteristica di un campo

Concludiamo questa lezione studiando i campi da un altro punto di vista, ossia studiando se contengono un sottoanello isomorfo a $\mathbb{Z}$ o no.

Osserviamo innanzitutto che, dato un campo F, c'è un solo omomorfismo di anelli $\phi : \mathbb{Z} \to F$, determinato dalla condizione $\phi(1) = 1$.[3]

Visto che $\mathbb{Z}$ è un anello a ideali principali, vale che $Ker\ \phi = (d)$, per un intero $d \geq 0$. Inoltre, poichè $\operatorname{Imm} \phi$ è un dominio (essendo un sottoanello del campo F), allora $Ker\ \phi = (d)$ è un ideale primo (Teorema 10.4).

Noi conosciamo gli ideali primi di $\mathbb{Z}$: si tratta dell'ideale (0) e degli ideali (p) dove p è un numero primo. Dunque abbiamo due casi:

(1) $Ker\ \phi = (0)$; allora $\operatorname{Imm} \phi \cong \mathbb{Z}$. Dunque in F abbiamo un sottoanello isomorfo a $\mathbb{Z}$, che chiameremo ancora $\mathbb{Z}$ per non appesantire la notazione. Inoltre, visto che F è un campo, e deve dunque contenere gli inversi di tutti gli elementi diversi da 0, possiamo concludere che in F c'è un sottocampo isomorfo a $\mathbb{Q}$, che chiameremo ancora $\mathbb{Q}$. Si dice in questo caso che F è un *campo di caratteristica 0*.

(2) $Ker\ \phi = (p)$ con p numero primo; allora $\operatorname{Imm} \phi \cong \mathbb{Z}/(p) \cong \mathbb{Z}_p$, dunque F contiene un sottocampo isomorfo a $\mathbb{Z}_p$, che chiameremo ancora $\mathbb{Z}_p$. Si dice in questo caso che F è un *campo di caratteristica p*.

Allora in F vale che $1 + \cdots + 1$ (p addendi) è uguale a 0. Infatti

$$1 + \cdots + 1 = \phi(1) + \cdots + \phi(1) = \phi(1 + \cdots + 1) = \phi(p) = 0$$

Consideriamo adesso F come spazio vettoriale su $\mathbb{Z}_p$ e osserviamo che per ogni $v \in F$ la somma $v + \cdots + v$ (p addendi) è uguale a 0. Infatti, per le proprietà della moltiplicazione per scalare, $v + \cdots + v = (1 + \cdots + 1)v = 0v = 0$.

4. Esercizi

Esercizio 13.13. Trovare il polinomio minimo su $\mathbb{Q}$ di $1 + \imath$.

Esercizio 13.14. Dimostrare che $[\mathcal{A} : \mathbb{Q}] = \infty$, dove $\mathcal{A}$ è il campo dei numeri algebrici. [Suggerimento: usare ciò che avete dimostrato a esercitazioni sui polinomi irriducibili in $\mathbb{Q}[x]$.]

Esercizio 13.15. Sia $\theta : K \to L$ un omomorfismo fra due campi K e L. Dimostrare che θ è iniettivo. [Suggerimento: ricontrollare tutte le definizioni degli oggetti in gioco.]

Esercizio 13.16. Calcolare il grado di $\mathbb{Q}(\imath, \sqrt{2})$ su $\mathbb{Q}$ e scrivere una base. Trovare il polinomio minimo di $\sqrt{2} + \imath$ su $\mathbb{Q}$, su $\mathbb{Q}(\imath)$, su $\mathbb{Q}(\sqrt{2})$ e su $\mathbb{Q}(\imath\sqrt{2})$.

Esercizio 13.17. Calcolare il grado di $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ su $\mathbb{Q}$ e scrivere una base. Trovare il polinomio minimo di $\sqrt{3} - \sqrt{2}$ su $\mathbb{Q}$ e su $\mathbb{Q}(\sqrt{3})$.

Esercizio 13.18. Calcolare il grado su $\mathbb{Q}$ di $2 + \sqrt{2}$.

Esercizio 13.19. È vero o falso che i polinomi $x^3 - 2$ e $x^3 - 3$ sono irriducibili su $\mathbb{Q}(\imath)$?

Esercizio 13.20. Calcolare $[\mathbb{Q}(\sqrt{3 + 2\sqrt{2}}) : \mathbb{Q}]$.

Esercizio 13.21. Sia $K \subseteq L$ una estensione di campi. Sia $\alpha \in L$ un elemento algebrico su K di grado dispari. Dimostrare che $K(\alpha^2) = K(\alpha)$.

[3]Come già specificato in precedenza, in questo corso stiamo considerando esclusivamente anelli con unità, dunque utilizziamo la definizione di omomorfismo fra anelli con unità.

CAPITOLO 14

Lezioni del 11 e 17 dicembre

1. Campi di spezzamento

DEFINIZIONE 14.1. Sia F un campo e sia $f(x) \in F[x]$ un polinomio non nullo. Una estensione finita E di F si dice un campo di spezzamento su F per $f(x)$ se valgono entrambe le seguenti condizioni:

- in $E[x]$ $f(x)$ si fattorizza come prodotto di polinomi di grado 1;
- per ogni campo K tale che $F \subseteq K \subsetneq E$ il polinomio $f(x)$ non si fattorizza come prodotto di polinomi di grado 1 in $K[x]$.

OSSERVAZIONE 14.2. Dunque, con le notazioni della definizione, si può dire che in E si trovano tutte le radici di $f(x)$ e non esiste nessun sottocampo proprio K di E che contiene F e tutte le radici di $f(x)$.

OSSERVAZIONE 14.3. Sia L una estensione di F che contiene tutte le radici di $f(x)$ (in generale esistono molte estensioni con queste caratteristiche, che ne esista almeno una è garantito dal Teorema 12.9), e siano $\alpha_1, ..., \alpha_t$ tali radici. Allora $F(\alpha_1, ..., \alpha_t)$ è un sottocampo di L che è un campo di spezzamento di $f(x)$ su F. Possiamo da questo ricavare che, dato un campo F e un polinomio non nullo $f(x) \in F[x]$, esiste sempre un campo di spezzamento di $f(x)$ su F.

Inoltre, dato un campo di spezzamento E di $f(x)$ su F, se chiamiamo $\beta_1, ..., \beta_t$ le radici distinte di $f(x)$ in E allora risulta che $E = F(\beta_1, ..., \beta_t)$.

In generale, dato un campo F ed un polinomio non nullo $f(x) \in F[x]$, si possono costruire vari campi di spezzamento per $f(x)$ su F, ma nel prossimo paragrafo scopriremo che questi campi di spezzamento sono tutti isomorfi fra loro. L'osservazione precedente ci permette comunque fin da subito, dato un campo di spezzamento E, di stimare il grado $[E : F]$.

PROPOSIZIONE 14.4. *Sia F un campo e sia $f(x) \in F[x]$ un polinomio non nullo di grado n. Sia E un campo di spezzamento di $f(x)$ su F. Allora $[E : F] \leq n!$.*

DIMOSTRAZIONE. Siano $\beta_1, ..., \beta_t$ le radici distinte di $f(x)$ in E e dunque $E = F(\beta_1, ..., \beta_t)$. Osserviamo che $[F(\beta_1) : F] \leq n$, visto che il polinomio minimo di β_1 in $F[x]$ è uno dei fattori irriducibili di $f(x)$ e pertanto ha grado $\leq n$. Ora

$$[F(\beta_1, \beta_2) : F] = [F(\beta_1, \beta_2) : F(\beta_1)][F(\beta_1) : F]$$

per il Teorema 13.2. Visto che in $F(\beta_1)[x]$ possiamo scrivere la decomposizione $f(x) = (x-\beta_1)g(x)$, dove $g(x)$ ha grado $n-1$, vale $[F(\beta_1, \beta_2) : F(\beta_1)] \leq n-1$; infatti il polinomio minimo di β_2 su $F(\beta_1)$ è uno dei fattori irriducibili di $g(x)$ in $F(\beta_1)[x]$.

Procedendo in questo modo in n passi si ottiene $[E : F] \leq n!$.

□

Facciamo due esempi, studiando i sottocampi di $\mathbb{C}$ che sono campi di spezzamento dei polinomi $x^3 - 2$ e $x^4 - 2$ su $\mathbb{Q}$.

ESEMPIO 14.5. Il sottocampo di $\mathbb{C}$ che è campo di spezzamento di x^3-2 su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ dove $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\imath$ è una radice cubica di 1.

Si tratta del più piccolo sottocampo di $\mathbb{C}$ che contiene $\mathbb{Q}$, e le tre radici $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$. Allora tale campo contiene anche ω, e dunque contiene $\mathbb{Q}(\sqrt[3]{2}, \omega)$. Si verifica immediatamente anche l'inclusione opposta, dunque $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ è il campo di spezzamento cercato.

Il grado di $\mathbb{Q}(\sqrt[3]{2}, \omega)$ su $\mathbb{Q}$ è uguale a 6 (cioè 3!, dove 3 è il grado del polinomio x^3-2). Infatti per calcolare il grado si considera la catena di estensioni

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$$

L'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ha grado 3, come sappiamo visto che x^3-2 è irriducibile in $\mathbb{Q}[x]$ (e comunque avevamo già considerato questo esempio nel Paragrafo 2 del Capitolo 12). L'estensione $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$ ha grado 2, visto che il polinomio minimo di ω su $\mathbb{Q}(\sqrt[3]{2})[x]$ è x^2+x+1. Quest'ultima affermazione si motiva nel seguente modo: osserviamo innanzitutto che $x^3-1 = (x-1)(x^2+x+1)$, dunque ω è radice di x^2+x+1; questo polinomio è irriducibile in $\mathbb{Q}(\sqrt[3]{2})[x]$, perché se fosse riducibile avrebbe delle radici in $\mathbb{Q}(\sqrt[3]{2})$, mentre sappiamo che le sue radici sono ω e ω^2, ovvero dei numeri complessi non reali.

ESEMPIO 14.6. Il sottocampo di $\mathbb{C}$ che è campo di spezzamento di x^4-2 su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \imath\sqrt[4]{2}, -\imath\sqrt[4]{2})$, ossia il più piccolo sottocampo che contiene $\mathbb{Q}$ e le quattro radici del polinomio.

Si osserva subito che tale campo coincide con $\mathbb{Q}(\sqrt[4]{2}, \imath)$. Il grado di $\mathbb{Q}(\sqrt[4]{2}, \imath)$ su $\mathbb{Q}$ è uguale a 8 (è dunque strettamente minore di 4!, dove 4 è il grado del polinomio x^4-2). Infatti considerando la catena di estensioni

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, \imath)$$

si osserva che $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ ha grado 4, visto che x^4-2 è irriducibile in $\mathbb{Q}[x]$, e che $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, \imath)$ ha grado 2, dato che il polinomio minimo di $\imath$ su $\mathbb{Q}(\sqrt[4]{2})$ è x^2+1.

2. Un teorema di isomorfismo per campi di spezzamento

Cominciamo presentando una versione più in generale del Teorema 12.8. Siano F ed F' due campi, e sia $\phi : F \to F'$ un isomorfismo. Osserviamo innanzitutto che a questo isomorfismo si può associare in modo ovvio un isomorfismo di anelli $\widetilde{\phi} : F[x] \to F'[x]$ definito così: dato un polinomio $h(x) = a_n x^n + \cdots + a_1 x + a_0$ in $F[x]$ allora

$$\widetilde{\phi}(a_n x^n + \cdots + a_1 x + a_0) = \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0)$$

OSSERVAZIONE 14.7. Visto che $\widetilde{\phi}$ è un isomorfismo, in particolare se $p(x)$ è un polinomio irriducibile in $F[x]$ allora $\widetilde{\phi}(p(x))$ è un polinomio irriducibile in $F'[x]$.

TEOREMA 14.8. *Siano F ed F' due campi, e sia $\phi : F \to F'$ un isomorfismo. Siano $F \subseteq L$ e $F' \subseteq L'$ due estensioni di campi. Sia $a \in L$ algebrico su F, con polinomio minimo $p(x)$. Supponiamo che esista in L' una radice a' di $\widetilde{\phi}(p(x))$. Allora esiste un isomorfismo $\phi' : F(a) \to F'(a')$ tale che $\phi'(a) = a'$ e ϕ' ristretto a F coincide con ϕ.*

DIMOSTRAZIONE. Consideriamo l'omomorfismo $\theta : F[x] \to F'[x]/(\widetilde{\phi}(p(x)))$ ottenuto come composizione:

$$F[x] \xrightarrow{\widetilde{\phi}} F'[x] \xrightarrow{\pi} F'[x]/(\widetilde{\phi}(p(x)))$$

dove π è l'omomorfismo di proiezione. Si verifica facilmente che $Ker\ \theta = (p(x))$ e allora per il primo teorema di omomorfismo abbiamo un isomorfismo

$$\theta' : F[x]/(p(x)) \to F'[x]/(\widetilde{\phi}(p(x)))$$

con le seguenti caratteristiche: $\theta'(x + (p(x))) = x + (\widetilde{\phi}(p(x)))$ e θ' ristretto a F (che è un sottocampo di $F[x]/(p(x))$) coincide con ϕ. Ora il Teorema 12.8 (riguardate anche la discussione che lo precede) fornisce due isomorfismi, $\gamma : F(a) \to F[x]/(p(x))$ e $\delta : F'[x]/(\widetilde{\phi}(p(x))) \to F'(a')$ che coincidono con l'identità su F e tali che $\gamma(a) = x + (p(x))$ e $\delta(x + (\widetilde{\phi}(p(x)))) = a'$.

L'isomorfismo ϕ' che stiamo cercando ci viene dunque fornito dalla seguente composizione di isomorfismi:

$$F(a) \xrightarrow{\gamma} F[x]/(p(x)) \xrightarrow{\theta'} F'[x]/(\widetilde{\phi}(p(x))) \xrightarrow{\delta} F'(a')$$

□

Osservazione 14.9. Come avrete notato, nel caso in cui $F = F'$ e l'isomorfismo ϕ è l'identità, il teorema appena visto coincide con il Teorema 12.8.

Siamo pronti per enunciare e dimostrare il teorema sull'isomorfismo fra campi di spezzamento:

Teorema 14.10. *Siano F ed F' due campi, e sia $\phi : F \to F'$ un isomorfismo. Sia $\widetilde{\phi} : F[x] \to F'[x]$ l'isomorfismo di anelli associato.*

Dato un polinomio non nullo $f(x) \in F[x]$, sia E un campo di spezzamento di $f(x)$ su F e sia E' un campo di spezzamento di $\widetilde{\phi}(f(x))$ su F'. Allora esiste un isomorfismo $\phi' : E \to E'$ tale che ϕ' ristretto a F coincide con ϕ.

Dimostrazione. La dimostrazione è per induzione sul grado di $f(x)$. Per prima cosa osserviamo che se $deg\ f(x) \leq 1$ allora $E = F$ e $E' = F'$, dunque basta porre $\phi' = \phi$ e abbiamo l'isomorfismo cercato.

Supponiamo adesso che $deg\ f(x) > 1$ e sia $g(x) \in F[x]$ un fattore irriducibile di $f(x)$. Sia $a \in E$ una radice di $g(x)$ e sia $a' \in E'$ una radice di $\widetilde{\phi}(g(x))$ (che è anch'esso un polinomio irriducibile, come sappiamo).

Per il Teorema 14.8 esiste un isomorfismo $\theta : F(a) \to F'(a')$ tale che θ ristretto ad F coincide con ϕ e $\theta(a) = a'$.

Possiamo associare a θ il corrispondente isomorfismo di anelli $\widetilde{\theta} : F(a)[x] \to F'(a')[x]$. Notiamo che $\widetilde{\theta}$ manda $x - a$ in $x - a'$, dunque se chiamiamo $\overline{f}(x)$ il polinomio tale che $f(x) = (x - a)\overline{f}(x)$ in $F(a)[x]$, applicando a questa uguaglianza l'omomorfismo $\widetilde{\theta}$ otteniamo $\widetilde{\theta}(f(x)) = (x - a')\,\widetilde{\theta}(\overline{f}(x))$ in $F'(a')[x]$.

Siamo nella condizione di poter applicare l'ipotesi induttiva. Infatti abbiamo la seguente situazione:

- abbiamo l'isomorfismo θ fra i campi $F(a)$ ed $F'(a')$;
- abbiamo il polinomio $\overline{f}(x) \in F(a)[x]$ di grado $deg\ f(x) - 1$;
- il campo E è un campo di spezzamento per $\overline{f}(x)$ su $F(a)$;
- il campo E' è un campo di spezzamento per $\widetilde{\theta}(\overline{f}(x))$ su $F'(a')$.

Dunque per ipotesi induttiva esiste un isomorfismo $\phi' : E \to E'$ tale che ϕ' ristretto a $F(a)$ coincida con θ. Questo ϕ' è l'isomorfismo che cerchiamo: infatti ristretto a F coincide con θ che a sua volta coincide con ϕ.

Abbiamo dunque terminato la dimostrazione del passo induttivo.

□

Il seguente corollario è la riduzione dell'enunciato del teorema al caso semplificato in cui $F = F'$ e l'isomorfismo ϕ è l'identità.

COROLLARIO 14.11. *Sia F un campo e siano E ed E' due campi di spezzamento di un polinomio non nullo $f(x) \in F[x]$. Allora esiste un isomorfismo $\phi' : E \to E'$ tale che ϕ' ristretto a F è l'identità.*

OSSERVAZIONE 14.12. Dal teorema precedente segue che, dato un campo F, il grado su F di un campo di spezzamento di un polinomio non nullo $f(x) \in F[x]$ è unicamente determinato da F e $f(x)$, e non dipende dal particolare campo di spezzamento che stiamo considerando.

3. La classificazione dei campi finiti

3.1. L'omomorfismo di Frobenius. Cominciamo presentando un importante omomorfismo.

TEOREMA 14.13 (L'omomorfismo di Frobenius[1]). *Sia p un numero primo, e sia K un campo di caratteristica p. La funzione $\mathcal{F} : K \to K$, definita da $\mathcal{F}(a) = a^p$ per ogni $a \in K$, è un omomorfismo iniettivo.*

DIMOSTRAZIONE. Stabiliamo innanzitutto che $\mathcal{F}$ è un omomorfismo. La verifica che $\mathcal{F}(1) = 1$ e che per ogni $a, b \in K$ vale $\mathcal{F}(ab) = \mathcal{F}(a)\,\mathcal{F}(b)$ è immediata.

La verifica più interessante è quella relativa alla somma: bisogna dimostrare che per ogni $a, b \in K$ vale $\mathcal{F}(a + b) = \mathcal{F}(a) + \mathcal{F}(b)$, ossia $(a + b)^p = a^p + b^p$.

Ci rendiamo conto di aver in sostanza già affrontato questo problema, nella seconda dimostrazione del piccolo teorema di Fermat (Capitolo 5, Paragrafo 1). L'uguaglianza $(a+b)^p = a^p + b^p$ segue dal fatto che si può sviluppare il membro di sinistra utilizzando il teorema del binomio di Newton, e poi si utilizza il fatto che tutti i coefficienti $\binom{p}{i}$, con $1 \leq i \leq p - 1$, sono multipli di p e dunque sono uguali a 0 in un campo di caratteristica p.

Per quel che riguarda l'iniettività di $\mathcal{F}$, osserviamo che Ker $\mathcal{F}$ è un ideale proprio di K (non può essere Ker $\mathcal{F} = K$ perché $\mathcal{F}(1) = 1$). Visto che K è un campo, l'unico ideale proprio è (0).

□

OSSERVAZIONE 14.14. Anche le potenze $\mathcal{F}^j$ (con j intero positivo) dell'omomorfismo di Frobenius sono omomorfismi iniettivi.

Nel prossimo paragrafo (e nel prossimo corso di Algebra 1 !) tornerà molto utile la seguente osservazione.

TEOREMA 14.15. *Sia K un campo, e sia $\psi : K \to K$ un omomorfismo. Allora l'insieme*

$$Fix_\psi = \{k \in K \mid \psi(k) = k\}$$

degli elementi di K lasciati fissi da ψ è un sottocampo di K.

DIMOSTRAZIONE. Dimostriamo innanzitutto che Fix_ψ è un sottoanello di K. Per prima cosa osserviamo che $0 \in Fix_\psi$. Inoltre, se $r \in Fix_\psi$ allora

$$\psi(-r) = -\psi(r) = -r$$

[1]Ferdinand Georg Frobenius, matematico tedesco, 1849-1917.

dunque anche l'opposto di r appartiene a Fix_ψ.

Consideriamo ora $r, s \in Fix_\psi$. Vale che

$$\psi(r+s) = \psi(r) + \psi(s) = r + s$$

dunque $r + s \in Fix_\psi$. Abbiamo fin qui dimostrato che Fix_ψ è un sottogruppo rispetto alla somma.

Analogamente si dimostra che se $r, s \in Fix_\psi$ allora il prodotto rs appartiene a Fix_ψ. Inoltre $1 \in Fix_\psi$. Dunque Fix_ψ è un sottoanello di K. L'ultima cosa che resta da dimostrare è l'esistenza in Fix_ψ dell'inverso moltiplicativo di un elemento non zero. Sia $r \in Fix_\psi$ diverso da 0; allora

$$\psi(r^{-1}) = \psi(r)^{-1} = r^{-1}$$

e dunque $r^{-1} \in Fix_\psi$.

□

3.2. Il teorema di classificazione. Consideriamo un campo finito L (ossia un campo con un numero finito di elementi).

La prima osservazione che possiamo fare è che L non può avere caratteristica 0: in tal caso infatti conterrebbe un sottocampo isomorfo a $\mathbb{Q}$ e non sarebbe finito. Dunque la caratteristica di L è un numero primo p, e L contiene un sottocampo isomorfo a $\mathbb{Z}_p$ (vedi il Paragrafo 3 del Capitolo 13).

Inoltre il grado di L su $\mathbb{Z}_p$ deve essere finito, diciamo $n \in \mathbb{N} - \{0\}$, altrimenti L sarebbe uno spazio vettoriale di dimensione infinita e dunque avrebbe infiniti elementi.

Ora, la cardinalità di uno spazio vettoriale di dimensione n sul campo $\mathbb{Z}_p$ è p^n (considerate una base $v_1, ..., v_n$: un vettore dello spazio è una combinazione lineare $a_1v_1 + \cdots + a_nv_n$ dove i coefficienti a_i appartengono a $\mathbb{Z}_p$, dunque abbiamo p scelte per ogni coefficiente).

Abbiamo ottenuto una prima interessante osservazione, che riassumiamo nella seguente proposizione.

PROPOSIZIONE 14.16. *La cardinalità di un campo finito è un intero della forma p^n per un certo numero primo p ed un certo intero positivo n.*

Ora consideriamo il gruppo moltiplicativo $L^* = L - \{0\}$. Visto che ha cardinalità $p^n - 1$, per il Corollario 6.18 del Teorema di Lagrange vale che, per ogni $g \in L^*$,

$$g^{p^n-1} = 1$$

Considerando anche lo 0, possiamo scrivere che per ogni $g \in L$ vale

$$g^{p^n} = g$$

Dunque il polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ ha esattamente p^n soluzioni in L: più precisamente tutti gli elementi di L sono radici di $x^{p^n} - x$ e $x^{p^n} - x$ si fattorizza come prodotto di fattori di grado 1 in $L[x]$. Pertanto L è un campo di spezzamento di $x^{p^n} - x$ su $\mathbb{Z}_p$.

A questo punto facciamo entrare in gioco il Teorema 14.10 che ci garantisce che tutti i campi finiti con p^n elementi, essendo campi di spezzamento del polinomio $x^{p^n} - x$ su $\mathbb{Z}_p$, sono isomorfi fra loro.

Non abbiamo ancora dimostrato però che per ogni primo p e per ogni intero positivo n esiste una campo di ordine p^n. Rimediamo con il seguente teorema che caratterizza tutti i campi finiti.

TEOREMA 14.17 (Teorema di classificazione dei campi finiti). *Ogni campo finito ha cardinalità p^n, dove p è un numero primo e n un intero positivo. Inoltre, per ogni numero*

primo p e per ogni intero positivo n esiste un campo finito di cardinalità p^n, unico a meno di isomorfismo.

DIMOSTRAZIONE. L'unica cosa che resta da dimostrare è l'esistenza di un campo con p^n elementi. Consideriamo un campo di spezzamento R di $x^{p^n} - x$ su $\mathbb{Z}_p$. Il campo R è un campo di caratteristica p ed ha dimensione finita su $\mathbb{Z}_p$ (vedi Proposizione 14.4), dunque è un campo finito.

Sia $L = \{r \in R \mid \mathcal{F}^n r = r\}$ dove $\mathcal{F}$ è l'omomorfismo di Frobenius. Come sappiamo dal Teorema 14.15, l'insieme L, ovvero l'insieme dei punti fissi dell'omomorfismo $\mathcal{F}^n$, è un sottocampo di R; ricordando la definizione dell'omomorfismo di Frobenius, si osserva anche che gli elementi di L sono le radici di $x^{p^n} - x$. Tali radici sono p^n, perché sono tutte distinte fra loro (la derivata di $x^{p^n} - x$ è -1, dato che R ha caratteristica p, e non ha dunque radici in comune con $x^{p^n} - x$).

Allora L è un campo con p^n elementi (e alla fine di questo ragionamento possiamo fra l'altro anche concludere che coincide con R).

□

OSSERVAZIONE 14.18. Per indicare un campo finito con p^n elementi useremo la notazione molto diffusa $\mathbb{F}_{p^n}$.

4. Campi finiti e gruppi ciclici

Concludiamo il corso con la dimostrazione di un teorema molto importante, che afferma che il sottogruppo moltiplicativo di un campo finito è ciclico. Questo equivale a dire che, dato il campo $\mathbb{F}_{p^n}$, esiste un elemento $\alpha \in \mathbb{F}_{p^n}^*$ di ordine $p^n - 1$.

In particolare, se consideriamo i campi $\mathbb{Z}_p = \mathbb{F}_p$, questo si traduce nel fatto che esiste un elemento $\alpha \in \mathbb{Z}_p^*$ di ordine $p-1$. Sottolineiamo però che questo risultato non fornisce una strategia concreta per trovare α; il problema di trovare una formula semplice per individuare un generatore α è ancora aperto. Un risultato parziale noto, per esempio, è che se p è un primo della forma $4q+1$, con q a sua volta primo, allora 2 è un generatore ciclico di $\mathbb{Z}_p^*$.

TEOREMA 14.19. *Dato un campo finito $\mathbb{F}_{p^n}$ (dove p è primo e n è un intero positivo), il gruppo moltiplicativo $\mathbb{F}_{p^n}^*$ è ciclico.*

DIMOSTRAZIONE. Suddividiamo la dimostrazione in vari passi.

Passo 1: Sia d un divisore di $p^n - 1$. Allora ci sono esattamente d radici distinte del polinomio $x^d - 1$ in $\mathbb{F}_{p^n}$.

Infatti sia $p^n - 1 = dm$. Dalla uguaglianza

$$x^m - 1 = (x-1)(x^{m-1} + \cdots + x + 1)$$

si ricava, sostituendo x con x^d, l'uguaglianza

$$x^{p^n-1} - 1 = (x^d - 1)(x^{d(m-1)} + \cdots + x^d + 1)$$

Questo mostra che $x^d - 1$ divide $x^{p^n-1} - 1$. Poiché in $\mathbb{F}_{p^n}$ tutti gli elementi diversi da 0 sono radici di $x^{p^n-1} - 1$, il polinomio $x^{p^n-1} - 1$ si fattorizza in $\mathbb{F}_{p^n}[x]$ come prodotto di polinomi di grado 1, tutti distinti fra loro. Dunque anche $x^d - 1$ si fattorizza in $\mathbb{F}_{p^n}[x]$ come prodotto di polinomi di grado 1, tutti distinti fra loro, e pertanto possiede in $\mathbb{F}_{p^n}$ esattamente d radici distinte.

Passo 2: Sia r un numero primo tale che r^e sia un divisore di $p^n - 1$, con e intero positivo. Allora nel gruppo moltiplicativo $\mathbb{F}_{p^n}^*$ c'è un elemento di ordine r^e.

Per il Passo 1, il polinomio $x^{r^e} - 1$ ha r^e radici distinte in $\mathbb{F}_{p^n}$. Inoltre, sempre per il Passo 1, $x^{r^{e-1}} - 1$ ha r^{e-1} radici distinte in $\mathbb{F}_{p^n}$ (qui gioca un ruolo importante l'ipotesi $e \geq 1$).

Allora esiste un elemento $\beta \in \mathbb{F}_{p^n}$ che è radice di $x^{r^e} - 1$ ma non è radice di $x^{r^{e-1}} - 1$. Tale β appartiene a $\mathbb{F}_{p^n}^*$ e ha ordine moltiplicativo r^e (se avesse un ordine minore di r^e tale ordine dovrebbe essere un divisore di r^e e dunque sarebbe r^s con $s < e$, ma allora risulterebbe che $\beta^{r^{e-1}} = 1$, assurdo).

Passo 3 (lemma sui gruppi abeliani) : Consideriamo in un gruppo abeliano degli elementi $\beta_1, \beta_2, ..., \beta_m$ i cui ordini sono i numeri $a_1, a_2, ..., a_m$ a due a due primi fra loro; allora l'ordine del prodotto $\beta_1\beta_2 \cdots \beta_m$ è il prodotto degli ordini $a_1a_2 \cdots a_m$.

Certamente $(\beta_1\beta_2 \cdots \beta_m)^{a_1a_2 \cdots a_m} = 1$ (indichiamo con 1 l'identità del gruppo, per coerenza con la situazione in cui dovremo applicare il lemma fra poco). Dunque l'ordine ν di $\beta_1\beta_2 \cdots \beta_m$ è un divisore di $a_1a_2 \cdots a_m$. Supponiamo per assurdo che sia $\nu < a_1a_2 \cdots a_m$. Allora, visto che gli a_i sono primi fra loro, esiste un a_i, diciamo a_1, che non divide ν. Dunque $\beta_1^\nu \neq 1$ e dalla relazione

$$1 = (\beta_1\beta_2 \cdots \beta_m)^\nu = \beta_1^\nu(\beta_2 \cdots \beta_m)^\nu$$

ricaviamo

$$\beta_1^\nu = ((\beta_2 \cdots \beta_m)^{-1})^\nu$$

Ora l'ordine dell'elemento a sinistra è un divisore di a_1, visto che β_1 ha ordine a_1, mentre l'ordine dell'elemento di destra è un divisore di $a_2 \cdots a_m$, visto che certamente $(\beta_2 \cdots \beta_m)^{a_2 \cdots a_m} = 1$. Poiché a_1 e $a_2 \cdots a_m$ sono primi fra loro, questo significa che tale ordine è 1, ossia che $\beta_1^\nu = 1$, che contraddice $\beta_1^\nu \neq 1$.

Passo finale:
Sia $p^n - 1 = q_1^{e_1}q_2^{e_2} \cdots q_m^{e_m}$, con i q_i numeri primi, la fattorizzazione in primi di $p^n - 1$. Allora per il Passo 2 sappiamo che, per ogni $i = 1, ..., m$, esiste un elemento $\beta_i \in \mathbb{F}_{p^n}^*$ tale che $o(\beta_i) = q_i^{e_i}$.

Consideriamo l'elemento $\alpha = \beta_1\beta_2 \cdots \beta_m$. Per il Passo 3 sappiamo che α ha ordine $q_1^{e_1}q_2^{e_2} \cdots q_m^{e_m} = p^n - 1$, e dunque il gruppo ciclico moltiplicativo generato da α coincide con $\mathbb{F}_{p^n}^*$

□

COROLLARIO 14.20. *Dato un campo finito $\mathbb{F}_{p^n}$ (dove p è primo e n è un intero positivo), sia α un generatore del gruppo ciclico $\mathbb{F}_{p^n}^*$. Se chiamiamo $f(x)$ il polinomio minimo di α su $\mathbb{Z}_p[x]$ vale che*

$$\mathbb{F}_{p^n} \cong \mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[x]/(f(x))$$

DIMOSTRAZIONE. Si tratta di una immediata conseguenza del teorema precedente: il campo $\mathbb{Z}_p[\alpha]$ coincide con $\mathbb{F}_{p^n}$ perché $\mathbb{Z}_p[\alpha]$ è un sottoinsieme di $\mathbb{F}_{p^n}$ che contiene 0 e le potenze di α, ossia contiene tutti gli elementi di $\mathbb{F}_{p^n}$.

□

COROLLARIO 14.21. *Per ogni numero primo p e per ogni intero positivo n esiste in $\mathbb{Z}_p[x]$ un polinomio irriducibile di grado n.*

DIMOSTRAZIONE. Per trovare il polinomio richiesto basta prendere un generatore α di $\mathbb{F}_{p^n}^*$ e considerare il suo polinomio minimo $f(x)$. Per il corollario precedente sappiamo che

$$\mathbb{F}_{p^n} \cong \mathbb{Z}_p[x]/(f(x))$$

Contando le cardinalità dei campi a sinistra e a destra, si ricava che $deg\ f(x) = n$. □

5. Esercizi

ESERCIZIO 14.22. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^4 + 1$.

ESERCIZIO 14.23. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^5 - 1$.

ESERCIZIO 14.24. Dimostrare che il sottocampo di $\mathbb{C}$ che è campo di spezzamento su $\mathbb{Q}$ di $x^2 - 3$ è campo di spezzamento su $\mathbb{Q}$ anche di $x^2 - 2x - 2$.

ESERCIZIO 14.25. Dimostrare che il sottocampo K di $\mathbb{C}$ che è campo di spezzamento su $\mathbb{Q}$ di $(x^2 - 2x - 2)(x^2 + 1)$ è campo di spezzamento su $\mathbb{Q}$ anche di $x^5 - 3x^3 + x^2 - 3$. Trovare il grado $[K : \mathbb{Q}]$.

ESERCIZIO 14.26. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^4 + 2x^3 - 8x^2 - 6x - 1$.

ESERCIZIO 14.27. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^4 - x^2 - 2$.

ESERCIZIO 14.28. Dimostrare che $\mathbb{F}_8$ è un campo di spezzamento su $\mathbb{Z}_2$ di $x^3 + x + 1$. Elencare gli elementi di $\mathbb{F}_8$. Quanti di questi sono generatori del gruppo ciclico $\mathbb{F}_8^*$? Di quale altro polinomio di grado 3 in $\mathbb{Z}_2[x]$ si può dire che $\mathbb{F}_8$ è il campo di spezzamento?

ESERCIZIO 14.29. Trovare un polinomio $f(x) \in \mathbb{Z}_2[x]$ tale che $\mathbb{F}_{16}$ sia il campo di spezzamento su $\mathbb{Z}_2$ di $f(x)$.

[Traccia: trovate un polinomio irriducibile $f(x)$ di grado 4 in $\mathbb{Z}_2[x]$. Allora $\mathbb{Z}_2[x]/(f(x))$ è un campo di 16 elementi, dunque è isomorfo a $\mathbb{F}_{16}$. Questo significa che in $\mathbb{F}_{16}$ i polinomi $f(x)$ e $x^{2^4} - x$ hanno una radice in comune, allora non possono essere primi fra loro in $\mathbb{Z}_2[x]$. Visto che $f(x)$ è irriducibile, deve essere $f(x)|x^{2^4} - x$. Dunque in $\mathbb{F}_{16}$, che contiene tutte le radici di $x^{2^4} - x$, ci sono tutte le radici di $f(x)$.]

ESERCIZIO 14.30. Fattorizzare $x^{16} - x$ come prodotto di polinomi irriducibili in $\mathbb{Z}_2[x]$.

ESERCIZIO 14.31. Dato un numero primo p e un polinomio irriducibile $g(x) \in \mathbb{Z}_p[x]$ di grado n, dimostrare che in ogni campo $\mathbb{F}_{p^m}$ con m multiplo di n il polinomio $g(x)$ ha esattamente n radici distinte.

ESERCIZIO 14.32. Dato un numero primo p ed un intero positivo n, dimostrare che $x^{p^n} - x$ è il prodotto di tutti i polinomi monici irriducibili in $\mathbb{Z}_p[x]$ di grado d divisore di n.

ESERCIZIO 14.33. È vero o falso che per ogni primo p esiste un campo K di caratteristica p tale che l'omomorfismo di Frobenius $\mathcal{F} : K \to K$ non è un isomorfismo?

CAPITOLO 15

Qualche ulteriore esercizio o spunto di riflessione

1. Esercizi

ESERCIZIO 15.1. Descrivere il gruppo $Aut(\mathbb{Z})$ dove $\mathbb{Z}$ è considerato gruppo rispetto all'addizione.

ESERCIZIO 15.2. Dimostrare che $Aut(S_3) \cong S_3$.

ESERCIZIO 15.3 (I numeri primi di Mersenne[1]). I numeri primi di Mersenne sono i numeri primi che si trovano fra i numeri della forma $M_n = 2^n - 1$, dove n è un intero positivo. I più piccoli numeri primi di Mersenne sono $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{13} = 8191$, $M_{17} = 131071$, $M_{19} = 524287$.

Attualmente (novembre 2015) sono noti 48 numeri primi di Mersenne; fra questi c'è il più grande numero primo conosciuto $2^{57885161} - 1$.

a) Dimostrare che se n non è primo allora neppure $M_n = 2^n - 1$ è primo, dunque i numeri primi di Mersenne vanno cercati fra i numeri della forma M_p con p primo.
b) Dimostrare che se p è un primo dispari, allora per ogni numero primo q che divide M_p vale

$$q \equiv 1 \quad (2p)$$

ESERCIZIO 15.4. Dati due gruppi G_1, G_2 e un omomorfismo di gruppi $\phi : G_1 \to G_2$ dimostrare che se K è un sottogruppo di G_2 allora $\phi^{-1}(K) = \{x \in G_1 \mid \phi(x) \in K\}$ è un sottogruppo di G_1 che contiene $\operatorname{Ker}\phi$.

ESERCIZIO 15.5. Dimostrare che per ogni $\phi \in Aut(S_3)$ esiste $\tau \in S_3$ tale che $\phi = C_\tau$, ossia ogni automorfismo di S_3 coincide col coniugio rispetto ad un elemento.

ESERCIZIO 15.6. Dimostrare che $Aut(S_4) \cong S_4$.

ESERCIZIO 15.7. Dimostrare che per ogni $\phi \in Aut(S_4)$ esiste $\tau \in S_4$ tale che $\phi = C_\tau$, ossia ogni automorfismo di S_4 coincide col coniugio rispetto ad un elemento.

ESERCIZIO 15.8. Consideriamo un gruppo G e un suo sottogruppo normale H. Dimostrare che la proiezione $\pi_H : G \to G/H$ induce una corrispondenza bigettiva fra l'insieme dei sottogruppi di G/H e l'insieme dei sottogruppi di G che contengono H.

ESERCIZIO 15.9. Consideriamo un anello R e un suo ideale I. Dimostrare che la proiezione $\pi_I : R \to R/I$ induce una corrispondenza bigettiva fra l'insieme degli ideali di R/I e l'insieme degli ideali di R che contengono I.

ESERCIZIO 15.10. Sia G un gruppo con la seguente proprietà: esistono tre interi consecutivi $i-1, i, i+1$ tali che per ogni $a, b \in G$ vale $(ab)^{i-1} = a^{i-1}b^{i-1}$, $(ab)^i = a^i b^i$, $(ab)^{i+1} = a^{i+1}b^{i+1}$. Dimostrare che G è abeliano.

[1]Marin Mersenne, matematico francese (anche teologo e teorico della musica e del suono), 1588-1648.

Esercizio 15.11. Dato un numero primo p, si consideri lo spazio vettoriale $\mathbb{Z}_p^2$ e chiamiamo $GL(\mathbb{Z}_p^2)$ il gruppo delle applicazioni lineari invertibili da $\mathbb{Z}_p^2$ in sé. Consideriamo ora il gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$ con l'operazione $+$ e il suo gruppo degli automorfismi $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$. Dimostrare che $GL(\mathbb{Z}_p^2)$ è isomorfo a $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$.

Esercizio 15.12. Dato un numero primo p congruo a 1 modulo 4, si consideri l'insieme $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$. Dimostrare che la funzione $f : S \to S$ definita da

$$f((x, y, z)) = (x + 2z, z, y - x - z) \quad \text{se} \quad x < y - z$$
$$f((x, y, z)) = (2y - x, y, x - y + z) \quad \text{se} \quad y - z < x < 2y$$
$$f((x, y, z)) = (x - 2y, x - y + z, y) \quad \text{se} \quad x > 2y$$

è una involuzione, ossia $f \circ f$ è l'identità. Dimostrare inoltre che f ha un solo punto fisso. Dunque $|S|$ è dispari, e allora anche l'involuzione $g : S \to S$ data da $g((x, y, z)) = (x, z, y)$ deve avere un punto fisso. Questo dimostra che p si può scrivere come somma di due quadrati.

[Si tratta della 'one sentence proof' del Teorema 11.25 pubblicata da Zagier[2] in The American Mathematical Monthly, Vol. 97, No. 2 (Feb. 1990).]

Esercizio 15.13 (Solo due?). Trovare tutte le radici di $x^2 - 1$ nel corpo $\mathbb{H}$ dei quaternioni (definito nell'Esercizio 9.34).

Esercizio 15.14. Dato un numero primo p, quanti sono i polinomi irriducibili di grado 2 in $\mathbb{Z}_p[x]$?

Esercizio 15.15. Dato un numero primo p e due interi positivi m, n, dimostrare che $\mathbb{F}_{p^m}$ contiene un sottocampo isomorfo a $\mathbb{F}_{p^n}$ se e solo se $n|m$.

Esercizio 15.16. Dato un numero primo p e un intero positivo n, dimostrare che esistono $\frac{\phi(p^n-1)}{n}$ polinomi monici irriducibili in $\mathbb{Z}_p[x]$ di grado n tali che, se chiamiamo $\mathcal{R}$ l'insieme dato dall'unione delle loro radici, vale che $\mathcal{R}$ coincide con l'insieme dei generatori del gruppo moltiplicativo $\mathbb{F}_{p^n}^*$.

[La ϕ che compare è la funzione di Eulero, e i polinomi di cui si parla in questo esercizio sono spesso chiamati 'primitivi', ma noi non insistiamo troppo su questo nome perché abbiamo usato nel corso l'espressione 'polinomio primitivo' in un altro significato, altrettanto usato, ossia per esempio per indicare polinomi in $\mathbb{Z}[x]$ in cui il MCD dei coefficienti è uguale a 1.]

Esercizio 15.17. Dato un numero primo p, consideriamo il polinomio $f(x) \in \mathbb{Z}_p[x]$ che si fattorizza in $\mathbb{Z}_p[x]$ nel seguente modo:

$$f(x) = f_1(x)^{\alpha_1} f_2(x)^{\alpha_2} \cdots f_m(x)^{\alpha_m}$$

dove i polinomi $f_i(x)$ sono irriducibili e gli α_i sono interi positivi. Dimostrare che il campo di spezzamento di $f(x)$ su $\mathbb{Z}_p$ è $\mathbb{F}_{p^n}$ dove n è il minimo comune multiplo dei gradi dei polinomi $f_i(x)$.

Esercizio 15.18. Dato un numero primo p, un intero positivo n, e posto $q = p^n$, consideriamo il polinomio $f(x) \in \mathbb{F}_q[x]$ che si fattorizza in $\mathbb{F}_q[x]$ nel seguente modo:

$$f(x) = f_1(x)^{\alpha_1} f_2(x)^{\alpha_2} \cdots f_m(x)^{\alpha_m}$$

dove i polinomi $f_i(x)$ sono irriducibili e gli α_i sono interi positivi. Dimostrare che il campo di spezzamento di $f(x)$ su $\mathbb{F}_q$ è $\mathbb{F}_{q^n}$ dove n è il minimo comune multiplo dei gradi dei polinomi $f_i(x)$.

[2]Don Zagier, matematico americano, 1951-

2. Soluzione di due esercizi sui campi finiti

Le due soluzioni che presentiamo contengono informazioni utili per risolvere anche altri esercizi che sono stati proposti sui campi finiti.

2.1. Soluzione dell'Esercizio 14.32. Consideriamo un polinomio $q(x)$ irriducibile in $\mathbb{Z}_p[x]$ e di grado d con d divisore di n. Dobbiamo dimostrare che $q(x)$ divide $x^{p^n} - x$. Consideriamo il campo $L = \mathbb{Z}_p[x]/(q(x))$: si tratta di un campo con p^d elementi, dunque isomorfo a $\mathbb{F}_{p^d}$. Come sappiamo, ogni elemento y di L soddisfa $y^{p^d} = y$; inoltre in L c'è una radice α di $q(x)$. Allora per tale α vale

$$\alpha^{p^d} = \alpha$$

Visto che $d|n$ esiste un intero s tale che $ds = n$. Osserviamo allora che

$$\alpha^{p^n} = (\alpha^{p^d})^{p^{(s-1)d}} = \alpha^{p^{(s-1)d}}$$

In base a questo si dimostra facilmente per induzione su s che $\alpha^{p^n} = \alpha$. Allora α è una radice del polinomio $x^{p^n} - x$.

Dunque $q(x)$ e $x^{p^n} - x$ hanno una radice in comune in L. Se fossero primi fra loro in $\mathbb{Z}_p[x]$ potremo scrivere, per il Lemma di Bezout:

$$\lambda(x)q(x) + \mu(x)(x^{p^n} - x) = 1$$

per certi polinomi $\lambda(x), \mu(x) \in \mathbb{Z}_p[x]$. Tale uguaglianza dovrebbe valere anche in $L[x]$, ma allora, valutandola in α, avremmo

$$\lambda(\alpha)q(\alpha) + \mu(\alpha)(\alpha^{p^n} - \alpha) = 1$$

ovvero $0 = 1$, assurdo. Dunque $q(x)$ e $x^{p^n} - x$ non sono primi fra loro in $\mathbb{Z}_p[x]$. Dato che $q(x)$ è irriducibile, deve valere $MCD(q(x), x^{p^n} - x) = q(x)$, ossia $q(x)|x^{p^n} - x$, come volevamo dimostrare.

Dimostriamo adesso il viceversa, ossia che se $f(x)$ è un polinomio irriducibile che divide $x^{p^n} - x$ allora il grado d di $f(x)$ divide n. Consideriamo il campo $K = \mathbb{Z}_p[x]/(f(x))$, che ha p^d elementi ed è isomorfo a $\mathbb{F}_{p^d}$ e studiamo la sua relazione con il campo $\mathbb{F}_{p^n}$. Gli elementi di $\mathbb{F}_{p^n}$ sono tutte le radici del polinomio $x^{p^n} - x$. Dato che $f(x)$ divide $x^{p^n} - x$, fra gli elementi di $\mathbb{F}_{p^n}$ ci sono in particolare tutte le radici di $f(x)$. Sia β una tale radice. Il polinomio minimo di β su $\mathbb{Z}_p$ è proprio $f(x)$ visto che $f(x)$ è irriducibile. Allora il campo $K' = \mathbb{Z}_p(\beta)$ è isomorfo a $K = \mathbb{Z}_p[x]/(f(x))$, pertanto K' è un sottocampo di $\mathbb{F}_{p^n}$ isomorfo a $\mathbb{F}_{p^d}$.

Consideriamo ora un elemento γ che genera il gruppo ciclico $\mathbb{F}^*_{p^n}$ (qui si usa il Teorema 14.19), e consideriamo il sottocampo $K'(\gamma)$ di $\mathbb{F}_{p^n}$. Visto che l'insieme delle potenze di γ è $\mathbb{F}^*_{p^n}$, il campo $K'(\gamma)$ in realtà coincide con $\mathbb{F}_{p^n}$. Sia ora $g(x)$ il polinomio minimo di γ su K', e sia $s = deg\ g(x)$. Allora possiamo scrivere che

$$[K'(\gamma) : \mathbb{Z}_p] = [K'(\gamma) : K'][K' : \mathbb{Z}_p] = sd$$

D'altra parte, visto che $K'(\gamma) = \mathbb{F}_{p^n}$, sappiamo che

$$[K'(\gamma) : \mathbb{Z}_p] = [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n$$

Dunque $n = sd$ e $d|n$ come volevamo dimostrare.

In conclusione abbiamo dimostrato che nella fattorizzazione di $x^{p^n} - x$ compaiono tutti e soli i polinomi irriducibili in $\mathbb{Z}_p[x]$ di grado d con d che divide n. Inoltre ognuno di tali polinomi compare nella fattorizzazione con esponente 1, perché $x^{p^n} - x$ non ha radici multiple.

2.2. Soluzione dell'Esercizio 15.16. Come sappiamo, il gruppo moltiplicativo $\mathbb{F}_{p^n}^*$ è ciclico e ha $\phi(p^n-1)$ generatori. Per dimostrare quanto chiesto dall'esercizio, basta dimostrare che l'insieme dei polinomi minimi in $\mathbb{Z}_p[x]$ di questi generatori è costituito proprio da $\frac{\phi(p^n-1)}{n}$ polinomi di grado n, ognuno dei quali ha per radici esattamente n generatori distinti.

Sia dunque α un generatore di $\mathbb{F}_{p^n}^*$ e sia $s(x)$ il suo polinomio minimo in $\mathbb{Z}_p[x]$. Dal fatto che α è un generatore di $\mathbb{F}_{p^n}^*$ deduciamo che $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, che è una estensione di grado n di $\mathbb{Z}_p$. Visto che $\mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(s(x))$, concludiamo che $s(x)$ deve avere grado n. Per l'Esercizio 14.32 sappiamo che $s(x)$ divide $x^{p^n} - x$; visto che $\mathbb{F}_{p^n}$ è campo di spezzamento su $\mathbb{Z}_p$ per $x^{p^n} - x$ e le radici di $x^{p^n} - x$ sono tutte distinte, vale che $s(x)$ ha in $\mathbb{F}_{p^n}$ esattamente n radici distinte.

Resta solo da dimostrare che ognuna di tali radici è un generatore di $\mathbb{F}_{p^n}^*$. Sia β una radice di $s(x)$ diversa da α. Sappiamo, per il Teorema 12.8, che esiste un isomorfismo $\theta : \mathbb{Z}_p(\alpha) \to \mathbb{Z}_p(\beta)$ che lascia fisso $\mathbb{Z}_p$ e che manda α in β. Poiché $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, anche la sua immagine rispetto a θ ha p^n elementi e dunque vale $\mathbb{Z}_p(\beta) = \mathbb{F}_{p^n}$ (potevamo concludere che $\mathbb{Z}_p(\beta) = \mathbb{F}_{p^n}$ anche osservando direttamente che la cardinalità di $\mathbb{Z}_p(\beta)$ è p^n visto che $\mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[x]/(s(x))$).

Inoltre, poiché θ è un isomorfismo e β è l'immagine di α, vale che l'ordine moltiplicativo di β è uguale a quello di α, ossia β ha ordine moltiplicativo $p^n - 1$ ed è dunque un generatore di $\mathbb{F}_{p^n}^*$.

Riassumendo, abbiamo scoperto che le n radici del polinomio $s(x)$ sono distinte e sono generatori di $\mathbb{F}_{p^n}^*$. Se esiste un generatore γ di $\mathbb{F}_{p^n}^*$ che non è radice di $s(x)$ consideriamo il suo polinomio minimo $s_1(x)$ e ripetiamo il ragionamento. Continuando in questo modo, troviamo i $\frac{\phi(p^n-1)}{n}$ polinomi richiesti.

Osservazione 15.19. I polinomi che abbiamo appena trovato sono irriducibili, ma non è detto che siano tutti i polinomi irriducibili di grado n in $\mathbb{Z}_p[x]$. Per esempio, se $p = 2$ e $n = 6$, con il ragionamento precedente troviamo $\frac{\phi(2^6-1)}{6} = \frac{\phi(63)}{6} = 6$ polinomi, mentre i polinomi irriducibili di grado 6 su $\mathbb{Z}_2[x]$ sono nove. Per esempio il polinomio $x^6 + x^3 + 1$ è irriducibile ma non 'primitivo' nel senso di questo esercizio.

Osservazione 15.20. Possiamo notare che questo esercizio ci offre un regalo: ci permette di concludere che il numero $\frac{\phi(p^n-1)}{n}$ è intero, per ogni primo p e per ogni intero positivo n.

Bibliografia

[DM] P. Di Martino, *Algebra*, Pisa University Press 2013.