Benedetta Taccola e Romeo Mario

Appunti di Algebra 1

Dalle lezioni della professoressa Ilaria del Corso e
dall'esercitatore Filippo Gianluca Callegaro

2017/2018

Prefazione

Questi sono appunti del corso di Algebra 1 della facoltà di matematica a Pisa dell'anno 2017/2018 tenuto dal docente Ilaria del corso. É possibile che ci sia qualche errore. (Ultimo aggiornamento 12/05/21)

Indice

Gruppi

Capitolo 1

Azioni di Gruppo

1.1 Gruppo degli Automorfismi

1.1.1 Definizione : Sia G un gruppo, il $Gruppo\ degli\ Automorfismi\ di\ G$ è definito come $Aut(G) = \{f : G \longrightarrow G;\ \ f\ isomorfismo\}$

1.1.1 Proposizione : $(Aut(G), \circ)$ è un gruppo

Dimostrazione : Bisogna verificare le ipotesi di gruppo : (chiusura per $\circ$) $\forall \phi, \psi \in Aut(G) \Longrightarrow \phi \circ \psi \in Aut(G)$, infatti sappiamo che la composizione di due applicazioni bigettive è bigettiva inoltre la composizione di due omomorfismi è un omomorfismo $(\phi \circ \psi)(ab) = \phi(\psi(ab)) = \phi(\psi(a)\psi(b)) = \phi(\psi(a))\phi(\psi(b))$; (esistenza elemento neutro) $\forall \phi \in Aut(G)\ \ \phi \circ Id_G = Id_G \circ \phi = \phi$ dove Id_G è l'automorfismo identità; (inverso di ogni elemento) $\forall \phi \in Aut(G)\ \ \phi^{-1} \in Aut(G)$ basta verificare che è omomorfismo , in quanto ϕ e bigettiva ed esiste quindi un inversa come applicazione, infatti $\phi^{-1}(ab)$, siccome ϕ surgettiva, $\exists c, d \in G$ tale che $a = \phi(c)$ e $b = \phi(d)$ quindi $\phi^{-1}(ab) = \phi^{-1}(\phi(c)\phi(d)) = \phi^{-1}(\phi(cd)) = cd = \phi^{-1}(a)\phi^{-1}(b)$.

□

1.1.1 esempio : $Aut(\mathbb{Z}) = \{\pm Id_{\mathbb{Z}}\} \cong (\mathbb{Z}/_{2\mathbb{Z}}, +)$

$\mathbb{Z}$ (inteso come $(\mathbb{Z}, +)$) è ciclico perciò basta decidere l'immagine di un suo generatore, per esempio 1, quindi ogni endomorfismo di $\mathbb{Z}$ è descritto da $q_a : \mathbb{Z} \longrightarrow \mathbb{Z}$ con $q_a(1) = a$ e mi chiedo quali siano bigettivi. Abbiamo che $q_a(\mathbb{Z}) = a\mathbb{Z}$ quindi $a\mathbb{Z} = \mathbb{Z} \Longleftrightarrow a = \pm 1$ e $q_1 = Id_{\mathbb{Z}}\ \ e\ \ q_{-1} = -Id_{\mathbb{Z}}$ sono gli automorfismi di $\mathbb{Z}$.

1.1.2 esempio : $Aut(\mathbb{Z}/_{m\mathbb{Z}}) \cong \mathbb{Z}/^*_{m\mathbb{Z}}$

$\mathbb{Z}/_{m\mathbb{Z}}$ è ciclico quindi ogni edomorfismo è definito da $q_a : \mathbb{Z}/_{m\mathbb{Z}} \longrightarrow \mathbb{Z}/_{m\mathbb{Z}}$ dove $q_a(1) = a$

e $ord(a)|ord(1)$. Affinchè sia bigettivo a deve essere un generatore di $\mathbb{Z}/_{m\mathbb{Z}}$, quindi $(m,a)=1$ da cui si deduce che $|\{a \in \mathbb{Z}; (m,a)=1\}| = \phi(m)$ e $|Aut(\mathbb{Z}/_{m\mathbb{Z}})| = |\mathbb{Z}/^*_{m\mathbb{Z}}|$.
Sia $\tau : Aut(\mathbb{Z}/_{m\mathbb{Z}}) \longrightarrow \mathbb{Z}/^*_{m\mathbb{Z}}$ con $\tau(q_a) = a$; $\tau(q_a \circ q_b) = \tau(q_{ab}) = ab = \tau(q_a)\tau(q_b)$, è omomorfismo; $\tau(q_a) = \tau(q_b) \Longrightarrow a = b \Longrightarrow q_a = q_b$ quindi è iniettiva, perciò τ è isomorfismo.

1.1.1 esercizio : $Aut(\mathbb{Q})$, $Aut(\mathbb{R})$ (intesi come automorfismi di gruppo $(\mathbb{Q},+)$ e $(\mathbb{R},+)$).

soluzione :

1) Il campo $\mathbb{Q}$ ha struttura di gruppo $(\mathbb{Q},+)$ e anche struttura di spazio vettoriale $(\vec{\mathbb{Q}},+,\cdot,\mathbb{Q})$, osserviamo che ogni omomorfismo di $\mathbb{Q}$ è anche un'applicazione lineare infatti conserva la somma in quanto omomorfismo e conserva il prodotto per scalari: $\phi \in Aut(\mathbb{Q})$, $\frac{n}{m} \in \mathbb{Q}$ $(n,m \neq 0 \in \mathbb{Z})$, v un vettore; $\phi(v) = k$, $\phi(v) = \phi(\frac{mv}{m}) = m\phi(\frac{v}{m})$ quindi $\phi(\frac{v}{m}) = \frac{k}{m} \Longrightarrow \phi(\frac{nv}{m}) = n\phi(\frac{v}{m}) = \frac{nk}{m} = \frac{n\phi(v)}{m}$. Ogni endomorfismo di $\mathbb{Q}$ è definito da $\psi : \mathbb{Q} \longrightarrow \mathbb{Q}$ con $\psi(1) = a$ e $a \neq 0$, ovvero è un cambiamento di base. Verifichiamo quanto detto : è ben definito infatti $a = \psi(1) = \psi(\frac{m}{m}) = m\psi(\frac{1}{m})$ da cui $\forall \frac{n}{m} \in \mathbb{Q}$, $\psi(\frac{n}{m}) = n\psi(\frac{1}{m}) = \frac{an}{m} \in \mathbb{Q}$; il nucleo è $ker\psi = \{b \in \mathbb{Q} \mid \psi(b) = 0\} = \{b \in \mathbb{Q} \mid ab = 0\} = \{0\}$ quindi è iniettiva; $\forall \frac{n}{m} \in \mathbb{Q}$ con $n,m \in \mathbb{Z}$ allora $\psi(\frac{n}{am}) = \frac{n}{m}$ quindi è surgettiva perciò è una bigezione. $\psi(b+c) = a(b+c) = ab + ac = \psi(b) + \psi(c)$ quindi è un automorfismo. Sia allora $\phi : Aut(\mathbb{Q}) \longrightarrow \mathbb{Q}^*$ con $\phi(\psi_a) \longmapsto a$; è surgettiva per quanto detto prima, inoltre $ker(\phi) = \{\psi_a \in Aut\mathbb{Q} \mid \phi(\psi_a) = 1\} = \{\psi_a \in Aut\mathbb{Q} \mid a = 1\} = \{Id_{\mathbb{Q}}\}$ quindi è iniettiva e vale $|Aut(\mathbb{Q})| = |\mathbb{Q}^*|$; $\forall q \in \mathbb{Q}^*$ $\phi(\psi_q) = q$ quindi è surgettiva inoltre è omomorfismo infatti $\phi(\psi_a \circ \psi_b) = \phi(\psi_{ab}) = ab = \phi(\psi_a)\phi(\psi_b)$ perciò $Aut\mathbb{Q} \cong \mathbb{Q}^*$.

2) (da vedere) Consideriamo l'omomorfismo di valutazione $val_1 : Aut(\mathbb{R}) \longrightarrow \mathbb{R}^*$ con $val_1(\phi) = \phi(1)$ questo omomorfismo è surgettivo infatti consideriamo $\phi_\lambda : \mathbb{R} \longrightarrow \mathbb{R}$ tale che $\phi(x) \longmapsto \lambda x$ $\forall \lambda \in \mathbb{R}/\{0\}$ questo è un automorfismo di $\mathbb{R}$ (semplice verifica) in particolare $\phi_\lambda(1) = \lambda$. Il $ker(val_1) = \{\phi \in Aut(\mathbb{R}) \mid \phi(1) = 1\}$ il gruppo degli automorfismi di $\mathbb{R}$ che fissano $\mathbb{Q}$.

1.1.2 Definizione : Definiamo *Automorfismo interno* (o coniugio) $\forall g \in G$ l'omomorfismo $\phi_g : G \longrightarrow G$ con $\phi_g(x) = gxg^{-1}$.

Mostro che è un Automorfismo : ϕ_g è ben definito inoltre $\forall x,y \in G$ $\phi_g(x)\phi_g(y) = (gxg^{-1})(gyg^{-1}) = gx(g^{-1}g)yg^{-1} = gxyg^{-1} = \phi_g(xy)$ quindi è un omomorfismo; il $ker(\phi_g) = \{x|\phi_g(x) = gxg^{-1} = e\} = \{x|x = e\} = \{e\}$; sia $y \in G$ allora $\phi_g(g^{-1}yg) = y$ quindi è iniettiva e surgettiva perciò è un isomorfismo.

1.1.3 Definizione : $Int(G) = \{\phi_g$ automorfismo interno di $G\}$

1.1.2 Proposizione : $Int(G) \triangleleft Aut(G)$ e $Int(G) \cong G/_{Z(G)}$

Dimostrazione : $Int(G)$ è un sottogruppo infatti : $Id_G = \phi_e \in Int(G)$ (elemento neutro) inoltre $\forall \phi_g, \phi_h \in Int(G),\ \phi_g \circ \phi_h = \phi_{gh} \in Int(G)$ (chiuso per $\circ$), $\forall \phi_g \in G\ \ \phi_g^{-1} = \phi_{g^{-1}}$ (esiste l'inverso di ogni elemento) quindi è un sottogruppo. $\forall f \in Aut(G)\ \forall \phi_g \in Int(G)\ f \circ \phi_g \circ f^{-1}(x) = f(\phi_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) = f(g)xf(g^{-1}) = f(g)xf^{-1}(g) = \phi_{f(g)}(x)$ questo implica che $int(G)$ è normale in $Aut(G)$.

Sia $\psi : G \longrightarrow int(G)$ con $\psi(g) = \phi_g$questo è un omomorfismo surgettivo, il $ker(\psi) = \{g|\ \forall x \in G\ \ \psi(g)(x) = \phi_e(x)\} = \{g|\ \forall x \in G\ \ \phi_g(x) = \phi_e(x)\} = \{g|\ \forall x \in G\ \ gxg^{-1} = x\} = Z(G)$ quindi applicando il primo teorema di omomorfismo si ha la tesi.

□

1.1.1 osservazione : $H \triangleleft G \iff \phi_g(H) = H\ \ \forall \phi_g \in int(G)$ ovvero H è normale se e solo se è invariante per automorfismi interni.

1.1.4 Definizione : $H < G$ si dice *caratteristico* se è invariante per automorfismo, cioè se $\forall f \in Aut(G)\ \ f(H) = H$.

1.1.2 osservazione : Caratteristico $\Longrightarrow$ normale; non vale il viceversa, infatti in $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ il sottogruppo $< (1,0) >$ è normale ma non caratteristico dato che l'automorfismo ψ che scambia le coordinate è tale che $\psi(< (1,0) >) =< (0,1) > \neq < (1,0) >$.

1.2 Azione di Gruppo su un Insieme

1.2.1 Definizione : Sia G un gruppo e X un insieme, un'*azione* di G su X è un'omomorfismo $\gamma : G \longrightarrow S(X) = \{f : X \to X | f\ \text{è}\ bigettiva\}$ con $\gamma(g) = \psi_g$ e dove $\psi_g(x) = g \cdot x$.

1.2.1 esempio : Sia $C = \{z \in \mathbb{C}^* |\ |z| = 1\}$ la circonferenza unitaria e $X = \mathbb{R}^2$ allora $\gamma : C \longrightarrow S(\mathbb{R}^2)$ con $\gamma(z) = rot_{arg(z)}$, è una azione che ad ogni z associa una rotazione del piano. Verifico che è un omomorfismo: $\gamma(zw) = rot_{arg(zw)} = rot_{(\theta+\mu)} = rot_\theta rot_\mu = \gamma(z)\gamma(w)$ dove $arg(z) = \theta$ e $arg(w) = \mu$. Posso quindi scrivere l'azione come $\gamma(z) = z \cdot P$ dove il prodotto a destra ha il significato di "ruoto P di $arg(z)$" come spiegato.

1.2.1 osservazione : Un'azione γ definisce su X una relazione di equivalenza, $x \sim_\gamma y \iff \exists g \in G$ tale che $x = g \cdot y = \phi_g(y)$ (verificare che è una relazione di equivalenza)

1.2.2 Definizione : La classe di equivalenza di x è detta *orbita* di x, $orb(x) = \{g \cdot x | g \in G\}$

Allora abbiamo $X = \overset{\circ}{\bigcup_{x \in R}} orb(x)$ dove R è l'insieme dei rappresentanti delle orbite, se $|X| < \infty$

ho che $|X| = \sum_{x \in R} |orb(x)|$.

1.2.3 Definizione : $\forall x \in X$ si dice *stabilizzatore* di x $st(x) = \{g \in G | g \cdot x = x\}$

1.2.2 osservazione : $st(x) < G$ ma in generale non è sottogruppo normale.

Se due elementi dell'orbita sono uguali allora sono la stessa classe laterale in $G/st(x)$ infatti $g \cdot x = h \cdot x \iff \gamma_g(x) = \gamma_h(x) \iff \gamma_{h^{-1}} \circ \gamma_g(x) = x \iff \gamma_{h^{-1}g}(x) = x \iff h^{-1}g \cdot x = x \iff h^{-1}g \in st(x) \iff h^{-1}gst(x) = st(x) \iff gst(x) = hst(x)$.

1.2.1 Proposizione : Gli elementi dell'orbita di x sono in corrispondenza biunivoca con le classi laterali di $st(x)$.

Dimostrazione : considero $\gamma : orb(x) \longrightarrow G/st(x)$ con $\gamma(g \cdot x) = gst(x)$ verifico che è biettiva: $\gamma(g \cdot x) = \gamma(h \cdot x) \Longrightarrow gst(x) = hst(x)$ per l'osservazione 1.2.2 $\Longrightarrow g \cdot x = h \cdot x$ quindi è iniettiva; se $gst(x) \in G/st(x) \Longrightarrow \gamma(g \cdot x) = gst(x)$ quindi è surgettiva. □

1.2.2 esempio : sia C la circonferenza unitaria di $\mathbb{R}^2$; $orb(P)$ è la circonferenza intorno all'origine descritta da P. $st(P) = \{id\}$ per $P \neq 0$, $st(P) = C$ per $P = 0$.

1.2.3 esempio : sia $G = \mathbb{R}$ e $X = \mathbb{R}^2$ e consideriamo la mappa $\gamma : G \longrightarrow S(X)$ con $\gamma(g) = \psi_g$ e $\psi_g(P) = P + (g, 0)$ (traslo di g lungo l'asse x); allora γ è un'azione.

Verifico che è un omomorfismo : $\gamma(g + h) = \psi_{g+h}$ che $\forall P \in X$ è uguale a $P + (g + h, 0) = P + (g, 0) + (h, 0) = \psi_h(P + (g, 0)) = \psi_h(\psi_g(P)) = (\psi_g \circ \psi_h)(P)$ quindi è un omomorfismo.

1.2.3 osservazione : un'azione importante è l'*azione di coniugio* dove il gruppo è G e l'insieme X è il gruppo stesso $X = G$ ovvero $\gamma : G \longrightarrow int(G) < S(G)$ con $\gamma(g) = \psi_g$ e dove $\psi_g(x) = gxg^{-1}$. L'orbita di x è $orb(x) = \{g \cdot x | g \in G\} = \{gxg^{-1} | g \in G\}$ ed è detta *classe di coniugio* $orb(x) = cl(x) = C_x$. Lo stabilizzatore $st(x) = \{g \in G | g \cdot x = x\} = \{g \in G | gxg^{-1} = x\}$ è detto *centrazizzatore* $st(x) = Z_G(x)$.

1.2.1 esercizio : $\bigcap_{x \in G} Z_G(x) = Z(G)$.

soluzione : $g \in \bigcap_{x \in G} Z_G(x) \iff gxg^{-1} = x \ \forall x \iff g \in Z(G)$. Se G è finito allora $\forall x \ |G| = |cl_x||Z_G(x)|$.

1.2.4 Definizione : Si definisce *Centralizzatore di un sottogruppo di G* il gruppo $\bigcap_{x \in H} Z_G(x) = Z(H)$.

1.2.2 esempio : Sia G un gruppo e $X = \{H \mid H < G\}$, allora $\gamma : G \longrightarrow S(X)$ con $g \longmapsto \psi_g$ e dove $\psi_g(H) = gHg^{-1}$ è un'azione. Questa è ben definita infatti $e = geg^{-1} \in gHg^{-1}\,, ghg^{-1} \in gHg^{-1} \Longrightarrow (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1} \Longrightarrow gHg^{-1} < G$; $\gamma(gt)(H) = \psi_{gt}(H) = gtHt^{-1}g^{-1} = g\psi_t(H)g^{-1} = \psi_g(\psi_t(H)) = (\gamma(g) \circ \gamma(t))(H)$ quindi è un omomorfismo. Lo stabilizzatore $st(H) = \{g \in G | gHg^{-1} = H\} \stackrel{def}{=} N_G(H)$ ovvero lo stabilizzatore di H prende il nome di *normalizzatore* ed è il più grande sottogruppo di G dove H è normale ($H \triangleleft N_G(H)$); $orb(H) = \{gHg^{-1} | g \in G\} =$ (insieme dei coniugati di H) quindi $|G| = |N_G(H)||orb(H)|$ perciò $H \triangleleft G \Longleftrightarrow N_G(H) = G \Longleftrightarrow orb(H) = \{H\}$ allora # (coniugati di H) $= \#\{gHg^{-1} | g \in G\} = [G : N_G(H)]$.

1.3 Cardinalità

Ricordiamo che $\gamma : G \longrightarrow S(X)$ è un'azione e vale che $X = \overset{\circ}{\bigcup\limits_{x \in R}} orb(x)$ dove R è l'insieme dei rappresentanti delle orbite, se $|X| < \infty$ ho che $|X| = \sum\limits_{x \in R} |orb(x)| = \sum\limits_{x \in R} \frac{|G|}{|st(x)|} = \sum\limits_{x \in R'} 1 + \sum\limits_{x \in R/R'} \frac{|G|}{|st(x)|}$ dove R' è l'insieme dei rappresentanti delle orbite tali che $orb(x) = x$ ed R è l'insieme di tutti i rappresentanti delle orbite. Se $X = G$ l'azione e' detta di coniugio come nell'osservazione 1.2.3.

1.3.1 Proposizione (Formula delle Classi) : Sia $\gamma : G \longrightarrow S(G)$ l'azione di coniugio dell'osservazione 1.2.3 allora :

$$|G| = Z(G) + \sum_{x \in R/Z(G)} \frac{|G|}{|Z_G(x)|}$$

detta formula delle classi (di coniugio).

Dimostrazione : Per quanto detto le orbite sono le classi di equivalenza della relazione di equivalenza dell'osservazione 1.2.1 e queste per la proposizione 1.2.1 sono in corrispondenza biunivoca con le classi laterali di $G/Z_G(x)$ perciò vale $|G| = \sum\limits_{x \in R'} 1 + \sum\limits_{x \in R/R'} \frac{|G|}{|Z_G(x)|}$; per concludre osserviamo che $R' = \{x \in R \mid orb(x) = x\} = \{x \in R \mid gxg^{-1} = x\} = Z(G)$. □

1.4 Applicazione ai p-gruppi

1.4.1 Definizione : Sia p primo, un p-gruppo è un gruppo finito G, con $|G| = p^n$.

1.4.2 Proposizione : Il centro di un p-gruppo è non benele

Dimostrazione : Per la formula delle classi $p^n = Z(G) + \sum_{x \in R/Z(G)} \frac{|G|}{|Z_G(x)|}$; se $Z(G) = p^n$ abbiamo finito, se no $\exists x \in R/Z(G)$ in particolare $Z_G(x)$ è contenuto strettamente in G quindi $|G/Z_G(x)| = p^k$ con $k > 0$ allora $Z(G) = p^n - \sum_{x \in R/Z(G)} p^k \implies p|Z(G)$, inoltre $e \in Z(G)$ quindi $|Z(G)| \geq 1$ perciò abbiamo che $|Z(G)| = p^s$ con $s > 1$.

□

1.4.1 Lemma $G/Z(G)$ è ciclico $\iff$ G è abeliano

Dimostrazione : ($\implies$) siano $a, b \in G$ allora $ab = (x^i + z)(x^j + w)$ dove $z, w \in Z(G)$ e $x+Z(G)$ genera $G/Z(G)$ e opportuni $i, j \in \mathbb{Z}$, quindi $(x^i+z)(x^j+w) = x^{(i+j)}+x^iw+zx^j+zw = x^{(j+i)} + wx^i + x^jz + wz = (x^j + w)(x^i + z) = ba$.
($\impliedby$) G è abeliano quindi $Z(G) = G$ perciò $G/Z(G) = \{Z(G)\} \cong \{e\}$ che è un gruppo ciclico.

□

1.4.2 Preposizione : Un gruppo di ordine p^2 è abeliano

Dimostrazione : Per la proposizione precedente $|Z(G)| \in \{p, p^2\}$ se fosse p^2 abbiamo finito, se fosse p allora $|G/Z(G)| = p$ quindi $G/Z(G)$ è ciclico, ma per il lemma precedente questo è assurdo.

□

1.4.1 Teorema di cauchy : Sia p primo e G un gruppo finito. Se $p|ord(G) \implies \exists x \in G$ tale che $o(x) = p$

1.4.1 osservazione :(Teorema di Lagrange) $H < G \wedge x \in G \implies o(H)|o(G)$ e $o(x)|o(G)$; vale il viceversa? (ovvero se $d|o(G)$ $\exists x \in G \mid o(x) = d$? $\exists H < G \mid o(H)|o(G)$?)

No, infatti in $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ non esiste nessun elemento x di ordine 4 ma esiste un sottogruppo di ordine 4 che è il gruppo stesso; in S_5 non c'è un elemento di ordine 15 ne un sottogruppo di ordine 15.

Dimostrazione :(del teorema di Cauchy) Sia G un gruppo, $o(G) = pn$ dove p è un primo e $n \in \mathbb{N}$, facciamo una induzione forte su n.
Passo base : per $n = 1 \implies G$ è ciclico quindi $\exists x \in G \mid G =< x >$ perciò $o(x) = p$.

Passo induttivo : supponiamo che il teorema sia vero per gruppo di ordine pm con $m < n$, consideriamo allora un gruppo di cardinalità pn; se $\exists H < G \ : \ p||H| \Longrightarrow o(H) = pm$ con $m < n$ e per induzione $\exists x \in H \mid o(x) = p$. Supponiamo allora che $\forall H < G \ \ p \nmid |H|$, per la formula delle classi vale che $pn - \sum_{x \in R'} \frac{|G|}{|Z_G(x)|} = |Z(G)|$ siccome $Z_G(x) < G$ allora $p \nmid |Z_G(x)| \Longrightarrow p| \frac{|G|}{|Z_G(x)|}$ perciò $p| \, |Z(G)| \Longrightarrow Z(G) = G$ (se non fosse uguale a G sarabbe un sottogruppo proprio quindi p non lo dividerebbe, assurdo) quindi G è abeliano e per cauchy per gruppi abeliani $\exists x \in G$ con $o(x) = p$.

□

Aritmetica (Teorema di cauchy per gruppi abeliani)

Con le stesse ipotesi del teorema 2.1.1, ma con G abeliano, dimostriamo la tesi per induzione su n dove $|G| = pn$ con p primo. Passo base : ovvio. Passo induttivo : supponiamo vera per $m < n$ e consideriamo quindi G tale che $|G| = pn$; sia $y \neq e$ e $H =< y >$ allora sappiamo che $|G| = |H||G/H|$ quindi se $p| \, |G| \Longrightarrow p| \, |H| \vee p| \, |G/H|$. se $p| \, |H|$ allora o $H = G$ quindi G ciclico e quindi ha un elemento di ordine p, $(|G| = ab, \ \ G =< x > \Longrightarrow o(x^a) = b)$ se $|H| = pm < pn$ allora per induzione e vera la tesi; nel caso che $p| \, |G/H|$ allora $|G/H| = pm' < pm$ perché H contene almeno due elementi y e e. Per ipotesi induttiva esiste $zH \in G/H$ tale che $o(zH) = p$. Consideramo la proiezione π_H da G in G/H cha associa a x la sua classe laterale xH. Essendo un omomorfismo $o(zH)|o(z)$ quindi $o(z) = pk$ se $k = n$ allora G è ciclico e z^n ha ordine p se $k < n$ allora per induzione si ha la tesi.

□

Dimostrazione alternativa del Teorema di cauchy :

Questa dimostrazione è dovuta a *John Mckay*, matematico britannico. La sua dimostrazione, con le stesse ipotesi del teorema di cauchy, non dice solo che esiste un x di ordine p in G ma che le soluzioni di $x^p = e$ in G sono kp con $k \geq 1$.
Sia $X = \{(a_1, \ldots, a_p) \mid a_i \in G \wedge \prod_{i=1}^{p} a_i = e\}$, la cardinalità è $|X| = |G|^{p-1}$ in quanto scelgo $p-1$ elementi e il p-esimo lo scelgo in modo che il prodotto con tutti gli altri faccia e; considero :
$\varphi : \mathbb{Z}/_{p\mathbb{Z}} \longrightarrow S(X) \quad$ con $\overline{1}((a_1, \ldots, a_p)) = (a_p, a_1, \ldots, a_{p-1})$ sposta semplicemente gli elementi della stringa; Dimostro che è una azione : è ben definita infatti $\overline{n}((a_1, \ldots, a_p)) =$
$\overline{1} \longmapsto \overline{1}((a_1, \ldots, a_p))$
$= (a_{p-n}, \ldots, a_p, a_1, \ldots, a_{p-n-1})$, sapendo che $a_1 \cdots a_p = e \Longrightarrow a_{p-n} \cdots a_p = a_1^{-1} \cdots a_{p-n-1}^{-1}$ moltiplicando a sinistra e poi ri-moltiplicando a destra si ottiene $a_{p-n} \cdots a_p a_1 \cdots a_{p-n-1} = e$. Con una semplice verifica si dimostra che è un omomorfismo quindi è un'azione. $\forall \underline{a} \in X$, $|orb(\underline{a})| \in \{1, p\}$ in particolare vale 1 se $\underline{a} = (a, \ldots, a)$ per qualche $a \in G$ tale che $a^p = e$, sappiamo che se R è l'insieme dei rappresentanti delle orbite e R' e l'insieme dei rappresentanti con $|orb(\underline{a})| = 1$ allora vale $|X| = \sum_{\underline{a} \in R'} 1 + \sum_{\underline{a} \in R/R'} |orb(\underline{a})|$ ma per quanto detto prima $p||X|$ e

$p|\sum_{\underline{a}\in R/R'}|orb(\underline{a})|$ quindi $p|\sum_{\underline{a}\in R'}1=|R'|$ da cui la tesi.

□

1.4.1 esercizio : (Classificazione dei gruppi di ordine 6)

soluzione : Sia G un gruppo di ordine 6. Allora per cauchy esistono $x,y\in G$ tale che $o(x)=2$ e $o(y)=3$. Se G è abeliano allora $o(xy)=6$ infatti $xy\neq e,\ (xy)^2=xyxy=xxyy=y^2\neq e,\ (xy)^3=xyxyxy=xxxyyy=x^3y^3=x\neq e$, quindi $G=<xy>\cong \mathbb{Z}/_{6\mathbb{Z}}$. Se G non è abeliano consideriamo allora il sottogruppo $<x,y>$. Posso anche considerare l'insieme prodotto $<x><y>$ che in generale non è un sottogruppo ($H,K<G\Longrightarrow HK<G\Longleftrightarrow HK=KH$; inoltre $|HK|=|H||K|/_{|H\cap K|}$ infatti consideriamo l'applicazione $\gamma: H\times K\longrightarrow HK$ tale che $\gamma((h,k))=hk$; è ovviamente surgettiva, inotre se $s\in H\cap K\Longrightarrow (hs,s^{-1}k)\in H\times K\Longrightarrow \gamma((hs,s^{-1}k))=hk$ quindi $\forall hk\in HK$ ci sono $o(H\cap K)$ coppie in $H\times K$ che hannno immagine in hk quindi vale la tesi). Allora $|<x,y>|=(3\cdot 2)/1=6$ per cui $G=<x><y>\Longrightarrow <x>=\{e,x\},\ <y>=\{e,y,y^2\}\Longrightarrow <x><y>=\{e,x,y,xy,y^2,xy^2\}$ voglio dimostrare che è isomorfo a $S_3=\{e,\tau,\rho,\tau\rho,\tau^2,\rho\tau^2\}$ con $\tau=(1,2,3)$ e $\rho=(1,2)$. Sia $\phi: G\longrightarrow S_3$ tale che $\phi(x)=\rho,\ \phi(y)=\tau$; è ovviamente surgettiva per costruzione quindi è una bigezione per questioni di cardinalità, inoltre è un omomorfismo quindi vale la tesi.

1.4.2 Teorema di Cayley : Sia G un gruppo $\Longrightarrow G$ isomorfo a un sottogruppo di $S(G)$, in particolare se $|G|=n\Longrightarrow G$ è isomorfo a un sottogruppo di S_n.

Dimostrazione : Sia $\phi: G\longrightarrow S(G)$ con $\phi(g)=\gamma_g$ e $\gamma_g(x)=g\cdot x$ questa applicazione è un'azione: è ben definita, cioè $\gamma: G\longrightarrow G$ è bigettiva infatti $\gamma_g(x)=\gamma_g(y)\Longleftrightarrow g\cdot x=g\cdot y\Longleftrightarrow x=y$ (legge di cancellazione) quindi è iniettiva; inoltre è surgettiva in quanto $\forall y\in G\ \gamma_g(g^{-1}\cdot y)=y$ (non ho usato la cardinalità di G in modo da dimostrare che vale per G di cardinalità infinita); vedo allora che ϕ è un omomorfismo: $\forall x,g,h\in G\ \phi(gh)(x)=\gamma_{gh}(x)=(gh)\cdot x=g\cdot(h\cdot x)=\gamma_g(\gamma_h(x))=(\phi(g)\circ\phi(h))(x)$. ϕ è iniettiva infatti $ker\phi=\{g\mid \phi_g=\phi_e\}=\{g\mid g\cdot x=x\}=\{e\}$ quindi $S(G)$ contiene una copia isomorfa a G.

□

1.4.2 esercizi : $S_3\hookrightarrow S_6,\ \ \mathbb{Z}/_{5\mathbb{Z}}\hookrightarrow S_5,\ \ \mathbb{Z}/_{10\mathbb{Z}}\hookrightarrow S_{10}$ provare a vedere come sono fatti.

1.4.2 Definizione : Sia G un gruppo e $S\subset G$ un sottoinsieme. $<S>$ è il gruppo generato da S ed è il più piccolo sottogruppo di G che contiene S.

Devo dimostrare che un tale sottogruppo esiste: $<S>=\bigcap_{\substack{H<G\\ S\subset G}}H$ questo è un sottogruppo e contiene S ed è il più piccolo che lo contiene, se così non fosse ne esisterebbe uno più piccolo ma farebbe parte dell'intersezione quindi esiste.

1.4.3 Proposizione : $< S >= \{s_1 s_2 \cdots s_k \mid k \in \mathbb{N},\ s_i \in S \cup S^{-1}\} = X$ con $S^{-1} = \{s^{-1} \mid s \in S\}$

Dimostrazione :So che $< S >= \bigcap_{\substack{H<G \\ S\subset G}} H$ quindi $S \subset H$ ma H è un sottogruppo $\Longrightarrow S^{-1} \subset H \Longrightarrow S, S^{-1} \subset H \Longrightarrow X \subset H \Longrightarrow X \subset \bigcap_{\substack{H<G \\ S\subset G}} H =< S >$ inoltre X è un sottogruppo (banale verifica) e contiene S per costruzione perciò $X \supset \bigcap_{\substack{H<G \\ S\subset G}} H =< S >$ quindi vale la tesi.

□

1.4.2 osservazione : Se $|G| < +\infty \implies < S >= \{s_1 s_2 \cdots s_k \mid k \in \mathbb{N},\ s_i \in S\}$

1.4.3 Definizione : Sia G un gruppo. definisco *commutatore* di $gh \in G$ l'elemento $[g, h] = ghg^{-1}h^{-1}$

1.4.4 Definizione : $G' =< [g, h] \mid g, h \in G >= [G : G]$ è il *Gruppo dei commutatori* o *derivato* di G

Proprietà di $< S >$:

$< S >$ è abeliano $\Longrightarrow \forall s_1, s_2 \in S\ ,\ s_1 s_2 = s_2 s_1$.
$< S >$ è normale $\Longrightarrow \forall g \in G,\ \forall s \in S\ \ gsg^{-1} \in < S >$.
$< S >$ è caratteristico $\Longrightarrow \forall f \in Aut(G),\ \forall s \in S\ \ f(s) \in S$.

Proprietà di G' :

$G' = e \Longleftrightarrow G$ è abeliano .
$G' \triangleleft G$ $(\forall x \in G,\ \forall g, h \in G\ x[g, h]x^{-1} = xghg^{-1}h^{-1}x^{-1} = xgx^{-1}xhx^{-1}xg^{-1}x^{-1}xh^{-1}x^{-1} = [xgx^{-1}, xhx^{-1}])$.
G' è caratteristico in G $(\forall f \in Aut(G),\ \forall g, h \in G\ \ f([g, h]) = f(ghg^{-1}h^{-1}) = f(g)f(h)f(h)^{-1}f(h)^{-1} = [f(g), f(h)])$.
sia $H \triangleleft G$. Allora G/H è abeliano $\Longrightarrow G' \subset H$; in particolare G/G' è abeliano ed è detto *abelianizzato* di G, ed è il più grande quoziente abeliano di G (G/H abeliano $\Longrightarrow \forall x, y \in G\ xHyH = yHxH \Longrightarrow xyH = yxH \Longrightarrow x^{-1}y^{-1}xy \in H \Longrightarrow [x, y] \in H \Longrightarrow H \supset G'$) .

1.5 Gruppi Diedrali

1.5.1 Definizione : Sia $n \in \mathbb{N}$ fissato e consideriamo un n-agono regolare, l'insieme di tutte le isometrie che mandano l'n-agono regolare in se stesso formano il gruppo D_n detto *Gruppo Diedrale* .

1.5.1 Proposizione : $|D_n| = 2n$

Dimostrazione : Un'isometria dell'n-agono regolare è univocamente determinata dall'immagine di un vertice e di un lato adiacente al vertice quindi un vertice ha n vertici possibili dove poter andare ed il lato adiaente ha 2 possibili lati adiacenti al vertice dove poter andare quindi ci sono $2n$ isometrie distinte.

□

1.5.2 Proposizione : Sia ρ una rotazione che sottende un lato e σ una simmetria dell'n-agono regolare. Allora $\rho^n = e$, $\sigma^2 = e$, $\sigma\rho\sigma = \rho^{-1}$.

Dimostrazione : Le prime due relazioni sono ovvie; la terza è data dal fatto che una riflessione composta una rotazione è ancora una riflessione quindi usando la seconda proprietà abbiamo che $e = (\sigma\rho)^2 = \sigma\rho\sigma\rho$ da cui vale la tesi.

□

1.5.2 Definizione : Posso definire, grazie alla proposizione 1.5.3, $\rho^{[i]} = \rho^i$ dove $[i] \in \mathbb{Z}/n\mathbb{Z}$; i è ben definito in quanto $\rho^n = e$.

1.5.1 osservazione : Mettendo l'n-agono regolare nel piano reale posso rappresentare le isometrie di D_n con delle matrici che appartengono a $GL_2(\mathbb{R})$. Allora :

$$\rho \longmapsto \begin{pmatrix} cos(\frac{2\pi}{n}) & sen(\frac{2\pi}{n}) \\ -sen(\frac{2\pi}{n}) & cos(\frac{2\pi}{n}) \end{pmatrix} = M_\rho \qquad\qquad \sigma \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = M_\sigma$$

Se chiamo $\mathbb{D}_n$ il sottogruppo generato da queste due matrici allora $\gamma :< \rho, \sigma > \longrightarrow \mathbb{D}_n$ come definito sopra è un omomorfismo di gruppi, infatti composizioni di isometrie che fissano un insieme $\mathbb{P}$ è ancora una isometria che fissa $\mathbb{P}$ (in particolare l'n-agono) quindi è ben definito $\rho^i\sigma^j \longmapsto M_\rho^i M_\sigma^j$; si verifica facilmente che $M_\rho^n = I$, $M_\sigma^2 = I$, $M_\sigma M_\rho M_\sigma = M_\rho^{-1}$ quindi è un omomorfismo. Con questo omomorfismo vediamo che ρ e σ definiti sopra non sono legati da qualche relazione, perché se lo fossero lo sarebbero anche le matrici associate dall'omomorfismo che è assurdo.

1.5.3 Proposizione : Tutti gli elementi di D_n sono scrivibili come $\sigma\rho^i$ oppure ρ^i per $i \in \{0, \ldots, n-1\}$.

Dimostrazione : Sia $g = \rho^{a_1}\sigma^{b_1}\cdots\rho^{a_k}\sigma^{b_k}$ una composizione qualsiasi di ρ e σ. Usando la proposizione 1.5.2 g lo possiamo scrivere come $\rho^{c_1}\sigma\cdots\rho^{c_k}\sigma$ se $c_1 \neq 0$ allora è uguale a $\sigma\sigma\rho^{c_1}\sigma\cdots\sigma\rho^{c_k}\sigma = \sigma\rho^{-c_1}\cdots\rho^{-c_k} = \sigma\rho^{d_1}$ con $d_1 \equiv \sum_{i=1}^{k} - c_i \,(mod\, n)$, se $c_1 = 0$ allora è uguale a $\rho^{-c_2}\cdots\rho^{-c_k} = \rho^{d_2}$ con $d_2 \equiv \sum_{i=2}^{k} - c_i \,(mod\, n)$ con $d_1, d_2 \in \{0, \ldots, n-1\}$ essendo moduli n . Quindi $\rho, \sigma \in D_n \Longrightarrow < \rho, \sigma > < D_n$ ma per quanto detto prima e nell'osservazione 1.5.1 $| < \rho, \sigma > | = 2n$ e per questioni di cardinalità $D_n =< \rho, \sigma >$. □

1.5.2 osservazione : ρ e σ con le relazioni della proposizione 1.5.2 generano tutto D_n inoltre $\mathbb{D}_n \cong D_n \cong$ {parole con ρ e σ}/{relazioni tra parole}. {parole con ρ e σ} si esprime come $< \rho > * < \sigma > \cong \mathbb{Z} * \mathbb{Z}$ dove $*$ e detto prodotto libero (intuitivamente costruisce un gruppo formato da tutti i modi di comporre una frase di qualsiasi lunghezza con le "lettere" ρ e σ), quozientando per {relazioni tra parole}$\cong [(\rho^n, \sigma^2, \sigma\rho\sigma\rho)]$, che non è altro il sottogruppo generato da $(\rho^n, \sigma^2, \sigma\rho\sigma\rho)$ e da tutti i loro coniugati, si ottiene un isomorfismo con D_n.

Studio di D_n : ($D_n =< \rho, \sigma \mid \sigma^2 = \rho^n = e, \sigma\rho\sigma = \rho^{-1} >$ è un gruppo di $2n$ elementi, non abeliano se $n > 2$)

Quanti sono gli elementi di ordine k in D_n?

Sia ρ la rotazione di D_n e consideriamo $< \rho > \cong C_n < D_n$, in C_n, essendo ciclico, ci sono $\phi(k)$ elementi di ordine k se $k|n$. ρ^i sono le n rotazioni e $\sigma\rho^i$ sono le n simmetrie, osserviamo che $\sigma\rho^i\sigma\rho^i = \rho^{-i}\rho^i = e$ quindi in conclusione se n è pari ho $n+1$ elementi di ordine 2 (le n riflessioni più $\rho^{\frac{n}{2}}$), se n è dispari ho n elementi di ordine 2, se $k|n,\ k \neq 2$ ho $\phi(k)$ elementi di ordine k.

Quali sono i sottogruppi di D_n?

Intanto conosco il gruppo ciclico C_n e i suoi sottogruppi sono noti: uno per ogni divisore dell'ordine del gruppo; quindi dato $H < D_n$, se $H < C_n$ allora H è l'unico sottogruppo di ordine $|H|$. Se $H \not< C_n$ ma $H < D_n$ allora H contiene almeno una riflessione τ; considero allora $H \cap C_n$, voglio affermare che $(H \cap C_n) \overset{\circ}{\bigcup} (\tau H \cap C_n)$ ed esiste una bigezione tra $(H \cap C_n)$ e $(\tau H \cap C_n)$. Per dimostrare questa affermazione considero :

$$D_n \xrightarrow{\gamma} GL_2(\mathbb{R}) \xrightarrow{det} \{\pm 1\} \cong \mathbb{Z}/_{2\mathbb{Z}}$$
$$D_n \xrightarrow[omo.surg.]{} \{\pm 1\} \cong \mathbb{Z}/_{2\mathbb{Z}}$$

dove γ è l'omomorfismo definito nell'osservazione 1.5.1 e *det* è il determinante. $\varphi = \gamma \circ det$ è surgettivo infatti se prendiamo le matrici dell'osservazione 1.5.1 abbiamo che $det(M_\rho) = 1$ e $det(M_\sigma) = -1$; il $ker(\varphi) = C_n$ infatti $det(M_\rho^i M_\sigma^j)$ per Binet $det(M_\rho)^i det(M_\sigma)^j = 1^i(-1)^j = 1 \iff j = 0$. Quindi se $\varphi : D_n \longrightarrow \mathbb{Z}/_{2\mathbb{Z}}$ consideriamo $\varphi|_H$, siccome $H \not< C_n$ ma $H < D_n$ $\varphi|_H$ sarà surgettiva, il suo *ker* è $H \cap C_n$ e per il primo teorema di omomorfismo $H/_{H\cap C_n} \cong \mathbb{Z}/_{2\mathbb{Z}}$ per il teorema di lagrange(*aritmetica*) $|H|/_{|H\cap C_n|} = |\mathbb{Z}/_{2\mathbb{Z}}|$ da cui $|H| = 2|H \cap C_n|$. Osserviamo che $\tau H \cap C_n \not< H \cap C_n$ infatti se $h \in H$ allora $det(M_\tau M_h) = det(M_\tau)det(M_h) = -1$ quindi i due insiemi sono disgiunti inoltre $\tau h_1 = \tau h_2 \implies h_1 = h_2$ quindi $|\tau H \cap C_n| = |H \cap C_n|$ perciò se consideriamo $\psi : H \cap C_n \longrightarrow \tau H \cap C_n$ tale che $\psi(h) \longmapsto \tau h$ questa è una bigezione(banale verifica). A questo punto $H \cap C_n =< \rho^m >= \{e, \rho^m, \rho^{2m}, \dots, \rho^{n-m}\}$ con $m|n$, $\tau = \sigma\rho^i \implies \tau H \cap C_n = \{\sigma\rho^i, \sigma\rho^{i+m}, \dots, \sigma\rho^{i+n-m}\}$ l'unione di questi due insiemi da tutto H. Quindi H è composto da m rotazioni e m simmetrie in particolare $H =< \rho^m, \tau > \cong D_m$. In conclusione se $m|n$ ho che i sottogruppi di D_n sono della forma $\mathbb{Z}/_{m\mathbb{Z}}$ e D_m.

1.5.4 Proposizione : Siano $H \lhd G$ e $K < H$ con K caratteristico in H.

Dimostrazione : Sia $g \in G$, $\phi_g : G \longrightarrow G$ con $\phi_g = gxg^{-1}$, abbiamo che $\phi_g(H) = H \implies \phi_g|_H$ è un automorfismo perciò si ha che $\phi_g|_H(K) = K \ \forall g \in G \implies gKg^{-1} = H$ quindi $K \lhd G$. □

Quali sono i sottogruppi normali di D_n?

C_n ha indice 2 in D_n quindi $C_n \lhd D_n$ (*aritmetica* : $G/H = \{H, \tau H\} \implies g \in G$ allora $g = h_1 \vee g = \tau h_2$ con $h_1, h_2 \in H$ quindi sia $hg \in Hg$ con $g \notin H \implies g = \tau h_3 \wedge hg = \tau h_4 = \tau h_3 h_3^{-1} h_4 = gh_5 \implies Hg \subset gH$ inoltre $|Hg| = |gH| \implies H \lhd G$) osserviamo che, sia G un gruppo ciclico di ordine n allora $\forall m|n \ \exists! H$ tale che $|H| = m$ quindi ogni sottogruppo di un gruppo ciclico è caratteristico in particolare in D_n ogni sottogruppo di $< \rho > \cong C_n$ è caratteristico. Quindi per la proposizione precedente ogni sottogruppo di C_n è normale; se n è pari $< \rho^2 > < C_n$ ed ha $\frac{n}{2}$ elementi quindi se $H \not< C_n$, $H < D_n$, $H \cap C_n =< \rho^2 > \implies H =< \rho^2 > \overset{\circ}{\bigcup} \tau < \rho^2 > \implies [D_n : H] = 2 \implies H \lhd D_n$ e ce ne sono 2 di questa forma : $< \rho^2, \sigma >$ e $< \rho^2, \sigma\rho >$. Non sappiamo se sono tutti i sottogruppi normali, cerchiamo di caratterizzarli meglio; sapendo che $H \lhd G \iff gHg^{-1} = H \ \forall g \in G$ questo ci dice che in un sottogruppo normale se ci sta un elemento ci stanno anche tutti i suoi coniugati, cerchiamo quindi di capire come sono fatti i coniugati di un elemento di D_n in particolare di ρ^i e $\sigma\rho^i$ per la proposizione 1.5.3 : $\rho^i\rho^i\rho^{-i} = \rho^i$, $\sigma\rho^i\rho^i\rho^{-i}\sigma = \sigma\rho^i\sigma = \rho^{-i}$, quindi l'insieme dei coniugati di ρ^i è $\{\rho^i, \rho^{-i}\}$ in particolare se $i \in \{0, \frac{n}{2}\}$ si riduce rispettivamente a $\{e\}$ e $\{\rho^{\frac{n}{2}}\}$; $\rho^i\sigma\rho^j\rho^{-i} = \sigma\rho^{-i}\rho^j\rho^{-i} = \sigma\rho^{j-2i}$, $\sigma\rho^i\sigma\rho^j\rho^{-i}\sigma = \rho^{-i}\rho^j\rho^{-i}\sigma = \sigma\rho^{2i-j} \implies$ se n è pari $\sigma\rho^s \sim \sigma\rho^t \iff s \equiv t(2)$ quindi le riflessioni si spezzano in due classi di coniugio, se n è dispari tutte le riflessioni sono coniugate. In conclusione se n è dispari, se un sottogruppo contiene una riflessione, le contiene tutte e tutte le riflessioni generano D_n infatti σ è dato e $\rho = \sigma\sigma\rho$ per ciò $H \lhd D_n \implies H = D_n$, se non contiene

una riflessione allora è un sottogruppo di C_n; se n è pari oltre ai sottogruppi di C_n, se $H \triangleleft D_n$, $\sigma\rho^i \in H \Longrightarrow \sigma\rho^{i+2} \Longrightarrow \rho^2 \in H$. Allora se $H \neq D_n$ deve essere $< \rho^2, \sigma >$ e $< \rho^2, \sigma\rho >$ come quelli citati prima.

Quali sono i sottogruppi caratteristici di D_n?

Usando l'osservazione 1.1.2 e lo studio precedente si osserva che gli altri possibili sottogruppi caratteristici sono i sottogruppi di C_n e $< \rho^2, \sigma >, < \rho^2, \sigma\rho >$, sappiamo già che i sottogruppi di C_n sono caratteristici; notiamo che $\tau : D_n \longrightarrow D_n$ tale che $\tau(\rho) = \rho$ e $\tau(\sigma) = \sigma\rho$ è un automorfismo e scambia $< \rho^2, \sigma >$ con $< \rho^2, \sigma\rho >$ quindi non sono caratteristici.

Quale è *il centro di* D_n?

cerco τ tale che per ogni ρ, $\rho\tau\rho^{-1} = \tau$ dal lo studio precedente sui coniugi è evidente che gli unici τ sono $\{e\}$ se n è dispari $Z(D_n) = \{e\}$ e $\{e\}, \{\rho^{\frac{n}{2}}\}$ se n è pari $Z(D_n) \cong \mathbb{Z}/_{2\mathbb{Z}}$.

Quozienti di D_n

Per il Teorema di corrispondenza (*Aritmetica*) i quozienti sono in corrispondenza biunivoca con i sottogruppi normali, perciò esiste un quoziente per ogni $H \triangleleft G$ e a meno di automorfismo i quozienti si ottengono in questo modo. Dallo studio precedente sappiamo che i sottogruppi normali sono i sottogruppi di C_n e in particolare se n è pari abbiamo anche $< \rho^2, \sigma >$ e $< \rho^2, \sigma\rho >$; sia $< \rho^m > < C_n$ con $m|n$ vediamo che $|D_n/_{<\rho^m>}| = \frac{2n}{m}$ voglio dire che $D_n/_{<\rho^m>} \cong D_{\frac{n}{m}}$. Consideriamo l'omomorfimo $\gamma : D_n \longrightarrow D_{\frac{n}{m}}$ tale che $\gamma(\sigma) = \tau$ e $\gamma(\rho) = \epsilon$ dove $D_n =< \sigma, \rho \mid \rho^n = \sigma^2 = e, \sigma\rho\sigma = \rho^{-1} >$ e $D_{\frac{n}{m}} =< \tau, \epsilon \mid \epsilon^{\frac{n}{m}} = \tau^2 = e, \tau\epsilon\tau = \epsilon^{-1} >$, osserviamo che è surgettivo ed il *ker* è proprio $< \rho^m >$ quindi per il primo teorema di omomorfismo vale la tesi. Nel caso n pari ci sono gli altri due sottogruppi sopra citati ma entrambi hanno indice 2 quindi i quozienti sono isomorfi a $\mathbb{Z}/_{2\mathbb{Z}}$.

Chi è $Aut(D_n)$?

Intanto cerco di capire quale è la cardinalità ovvero $|Aut(D_n)|$; per definire un automorfismo di D_n è sufficiente definirlo sui generatori che sappiamo essere ρ e σ, e questi dovranno avere immagine in altri generatori di D_n affinché sia tale, ρ ha ordine n quindi dovrà avere immagine in un elemento di ordine di ordine n che sono della forma ρ^i con $(i, n) = 1$ quindi ci sono $\phi(n)$ possibilità (ϕ di eulero), inoltre σ ha ordine 2 e deve avere immagine in un elemento di ordine 2 che insieme a ρ^i scelto prima generi D_n e ci sono n rilessioni della forma $\sigma\rho^j$ quindi ci sono n scelte possibili (notimao che se n è pari $\rho^{\frac{n}{2}}$ ha ordine 2 ma la coppia $\rho^i, \rho^{\frac{n}{2}}$ non genera D_n); non siamo certi che le applicazioni definite prima siano effettivamente degli automorfismi, dimostro quindi che lo sono: sia $\gamma : D_n \longrightarrow D_n$ tale che

$\gamma(\rho^h) = \rho^{ih}$ e $\gamma(\sigma\rho^k) = \sigma\rho^j\rho^{ik}$ con $(i,n) = 1$ e j qualsiasi, γ è ben definita, resta da verificare $\gamma((\rho^s)(\sigma\rho^t)) = \gamma(\sigma\rho^{t-s}) = \sigma\rho^j\rho^{i(t-s)} = \sigma\rho^{-is}\rho^j\rho^{it} = \rho^{is}\sigma\rho^j\rho^{it} = \gamma(\rho^s)\gamma(\sigma\rho^t)$ quindi è un omomorfismo, inoltre per costruzione è bigettiva quindi $|Aut(D_n)| = n\phi(n)$ ed in particolare come insiemi esiste una bigezione tra $Aut(D_n)$ e $\mathbb{Z}/_{n\mathbb{Z}} \times (\mathbb{Z}/_{n\mathbb{Z}})^*$.

1.5.1 esempio : Studiamo $D_4 = \{\rho, \sigma \mid \rho^4 = \sigma^2 = e, \sigma\rho\sigma = \rho^{-1}\}$, i sottogruppi sono $< \rho > \cong \mathbb{Z}/_{4\mathbb{Z}}$, $< \rho^2 >$, $< \sigma >$, $< \sigma\rho >$, $< \sigma\rho^2 >$, $< \sigma\rho^3 >$ isomorfi a $\mathbb{Z}/_{2\mathbb{Z}}$, $< \rho^2, \sigma >$, $< \rho^2, \sigma\rho >$ isomorfi a $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ e banalmante $\{e\}$, D_4; tra questi $\{e\}$, D_4, $< \rho >$, $< \rho^2 >$, $< \rho^2, \sigma >$, $< \rho^2, \sigma\rho >$ sono normali; $\{e\}$, D_4, $< \rho >$, $< \rho^2 >$ sono caratteristici; $Z(D_4) =< \rho^2 >$ ed infine $\{e\} \cong D_4/D_4$, $D_4 \cong D_4/\{e\}$, $\mathbb{Z}/_{2\mathbb{Z}} \cong D_4/_{<\rho>}$, $D_2 \cong D_4/ < \rho^2 >$, $\mathbb{Z}/_{2\mathbb{Z}} \cong D_4/_{<\rho^2,\sigma>}$, $\mathbb{Z}/_{2\mathbb{Z}} \cong D_4/_{<\rho^2,\sigma\rho>}$ sono i quozienti.

1.5.1 esercizio : Fare lo stesso con D_6

1.6 Permutazioni

Sia X un insieme allora $S(X) = \{f : X \longrightarrow X \mid f \text{ è } bigettiva\}$, se $X = \{1, \ldots, n\}$ allora $S(X) = S_n$ con $|S_n| = n!$.

1.6.1 Definizione : Un elemento di S_n si chiama *Permutazione*.

per esempio consideriamo S_{10}, posso rappresentare una permutazione tramite :

$$\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 2\ 3\ 1\ 7\ 6\ 8\ 4\ 5\ 9\ 10 \end{pmatrix}$$

dice che l'immagine di un elemento del rigo di sopra va in un elemento del rigo di sotto per esempio 1 va in 2, 2 va in 3 etc...; si può esprimere anche come prodotto di *cicli disgiunti* in modo *unico* ovvero (123)(47)(568)(9)(10), che si semplifica in (123)(47)(568) dando quindi per scontato che i numeri che non compaiono vengono mandati in loro stessi; un ciclo è (...), sono disgiunti in quanto la funzione è bigettiva, in modo unico in quanto una scrittura individua una funzione, una diversa scrittura individua una diversa funzione ovviamente a meno di scambiare i cicli.

1.6.1 osservazione : Cicli disgiunti commutano, infatti siano σ, τ cicli disgiunti, ovviamente se $\sigma(a) \neq a \Longrightarrow \tau(a) = a$ analogamente $\tau(b) \neq b \Longrightarrow \sigma(b) = b$, in particolare per iniettività se $\sigma(a) \neq a \Longrightarrow \sigma\sigma(a) \neq \sigma(a) \Longrightarrow \tau\sigma(a) = \sigma(a)$ quindi $\sigma\tau(a) = \sigma(a) = \tau\sigma(a)$ analogamente

per il caso di b quindi in generale $\sigma\tau = \tau\sigma$.

1.6.2 osservazione : Un k-ciclo (ciclio di lunghezza k) ha k scritture diverse, infatti per esempio $(123) = (231) = (312)$ dovuto alla scelta del primo elemento che scrivi all'inizio del ciclo che sono esattamente k scelte gli altri sono univocamente determinati (attenzione $(123) \neq (132)$).

1.6.3 osservzione : I cicli sono orbite, infatti prendiamo $\sigma \in S_n = S(\{1, \ldots, n\})$ consideriamo l'azione $< \sigma > \hookrightarrow S_n$, $orb(x) = \{\sigma^k(x)\} = \{x, \sigma(x), \ldots, \sigma^k(x)\}$ che è proprio $\sigma = (x, \sigma(x), \ldots, \sigma^k(x))$. Per esempio in S_3 $(123) = (1, (123)(1), (123)^2(1)) = (2, (123)(2), (123)^2(2)) = (3, (123)(3), (123)^2(3))$.

1.6.1 Corollario : S_n è generato dai cicli.

1.6.1 esercizio : Quanti sono i k cicli in S_n con $k \leq n$?

soluzione : Un k-ciclio è essenzialmente una stringa di k numeri quindi il problema si riduce a trovare quanti k numeri posso estrarre da un insieme di n numeri ed equivalentemente a vedere quanti sono i sottoinsiemi di cardinalità k in un insieme di cardinalità n ($k \leq n$), che sappiamo essere $\binom{n}{k}$; non sono tutte infatti questi k numeri possono essere scambiati tra loro in $k!$ modi diversi quindi ci sono $\binom{n}{k}k!$, ma per l'osservazione 1.6.2 ognuna di queste si può scrivere in k modi equivalenti che abbiamo gia contato precedentemente quindi in tutto sono $\binom{n}{k}\frac{k!}{k}$.

1.6.2 esercizio : Quanti sono i $\sigma \in S_{12}$ che si possono scrivere come composizione di 2 3-cicli e 3 2-cicli disgiunti?

soluzione : per l'esercizio precedente sappiamo che ci sono $\binom{12}{3}\frac{3!}{3}$ 3-cicli, fissato quindi il primo 3-ciclo restano $12 - 3$ elementi liberi per gli altri cicli(li tolgo i primi tre affinché quelli che costruisco dopo siano disgiunti dal primo) quindi reiterando il ragionamento per il secondo 3-ciclo ho $\binom{9}{3}\frac{3!}{3}$ 3-cicli a disposizione; continuando così per ogni ciclo si ottiene complessivamente $\binom{12}{3}\frac{3!}{3}\binom{9}{3}\frac{3!}{3}\binom{6}{2}\frac{2!}{2}\binom{4}{2}\frac{2!}{2}\binom{2}{2}\frac{2!}{2}$ permutazioni; ne ho contati troppi infatti considerando i 3-cicli essendo disgiunti possono commutare senza cambiare la natura della permutazione ma col conto precedente li ho considerati distinti, quindi ci sono tante ripetizioni tanti quanti sono i modi di commutare i 3-cicli ovvero 2! ed analogamente 3! modi per i 2-cicli quindi complessivamente ci sono esattamente $\binom{12}{3}\frac{3!}{3}\binom{9}{3}\frac{3!}{3}\binom{6}{2}\frac{2!}{2}\binom{4}{2}\frac{2!}{2}\binom{2}{2}\frac{2!}{2}\frac{1}{2!3!}$ permutazioni (potevo contare i cicli anche con un ordine diverso in quanto tra loro commutano e per ciò la relazione rimane la stessa).

1.6.3 esercizio : Qual'è l'ordine di una permutazione di S_n?

soluzione : Intanto osserviamo che un k-ciclo ha ordine k infatti sia $\sigma = (a_1 \cdots a_k) \Longrightarrow \sigma^s(a_i) = a_{i+s}$ se $i \leq k$, $\sigma^s(a_i) = a_i$ se $i > k$ quindi, per $i \leq k$, $\sigma^s(a_i) = a_{i+s} = a_i \iff s = k$. Se la permutazione τ è formata da più cicli disgiunti allora l'ordine è $mcm(o(\tau_1), \ldots, o(\tau_l))$ dove $\tau = \tau_1, \ldots, \tau_l$ è la decomposizione in cicli disgiunti, infatti osserviamo che se m è tale che $(\tau)^m = e$ allora $e = \tau^m = (\tau_1 \cdots \tau_l)^m = (\tau_1)^m \cdots (\tau_l)^m \Longrightarrow (\tau_i)^m = e \ \forall i : 1, \ldots, l$ (se l'ultima uguaglianza non valesse allora significa che esiste j tale che $(\tau_j)^m \neq e \Longrightarrow \exists a_j$ tale che $\tau_j^m(a_j) \neq a_j$ per l'osservazione 1.6.1 abbiamo che $a_j = e(a_j) = (\tau_1)^m \cdots (\tau_j)^m \cdots (\tau_l)^m(a_j) = \tau_j^m(a_j) \neq a_j$) assurdo, quindi $o(\tau_i)|m$, ma se t è l'ordine di τ allora $\tau^t = e \Longrightarrow o(\tau_i)|t$ ed in imparticolare $t|m$ quindi vale la tesi.

1.6.1 esempio : sia $(123)(45)(1356)(26)$, la voglio scrivere in cicli disgiunti, vedo come agisce su $\{1, \ldots, n\}$, quindi $(123)(45)(1356)(26)(1) = (123)(45)(1356)(1) = (123)(45)(3) = (123)(3) = (1)$, proseguendo con gli altri numeri ottengo $(1)(2)(3456) = (3456)$; ha ordine 4 è l'inversa è $(3456)^3 = (3654)$.

1.6.2 Definizione : Sia $\tau \in S_n$ della forma (a_i, a_j), un 2-ciclo, allora τ si chiama *trasposizione*.

1.6.1 Proposizione : tutte le permutazioni di S_n sono prodotto di trasposizioni, quindi le trasposizioni generano tutto S_n.

Dimostrazione : Basta vedere che vale per un k-ciclio, in effetti $(1, \ldots, k) = (1, k)(1, k-1) \cdots (1, 2)$.

□

1.6.4 osservazione : La scrittura come prodotto di trasposizioni non è unica, per esempio $(12) = (12)(34)(34) = (12)(34)(35)(67)(34)(35)(67)$.

1.6.2 Proposizione : L'applicazione $sgn : S_n \longrightarrow \{\pm 1\} = \mathbb{Z}^* \quad \text{con } sgn(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$ è un omomorfismo di gruppi. Inoltre se σ è una trasposizione $sgn(\sigma) = -1$.

Dimostrazine : Sia al numeratore che al denominatore della produttoria compaiono tutte le differenze di tutte le coppie: al denominatore abbiamo $i - j$ dove $\{i, j\}$ è qualsiasi in $\{1, \ldots, n\}$ e $i < j$, al numeratore abbiamo $\sigma(i) - \sigma(j)$ dove $\{\sigma(i), \sigma(j)\}$ è qualsiasi in $\{1, \ldots, n\}$, quindi è ben definito.

$sgn(\sigma \circ \tau) = \prod_{1 \leq i < j \leq n} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \prod_{1 \leq i < j \leq n} \frac{\tau(i) - \tau(j)}{i - j} = sgn(\sigma)sgn(\tau)$ (al massimo ho moltiplicato per -1 numeratore e denominatore di qualche fattore) quindi è un omomorfismo. Sia (a, b) una

trasposizione allora $sgn((a,b)) = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j}$, se $\{i,j\}\cap\{a,b\} = \emptyset \Longrightarrow \frac{\sigma(i)-\sigma(j)}{i-j} = \frac{i-j}{i-j} = 1$ se $\{i,j\}\cap\{a,b\} = \{i,a\} \Longrightarrow \frac{\sigma(i)-\sigma(a)}{i-a} = \frac{i-b}{i-a}$ con $i<a$ oppure $\frac{\sigma(a)-\sigma(i))}{a-i} = \frac{b-i}{a-i} = \frac{i-b}{i-a}$ con

$a<i$ analogamente per intersezione $\{i,b\} \Longrightarrow \frac{\sigma(1)-\sigma(b)}{i-b} = \frac{\sigma(b)-\sigma(i)}{b-i} = \frac{i-a}{i-b}$ ed all'interno della produttoria questo con quello precedente del caso $\{i,a\}$ si semplificano a 1, rimane il caso con intersezione $\{a,b\}$ (senza perdita di generalità supponiamo $a<b$) $\Longrightarrow \frac{\sigma(a)-\sigma(b)}{a-b} = \frac{b-a}{a-b} = -1$ quindi ho un solo fattore negativo per cui $sgn((a,b)) = -1$.

□

1.6.2 Corollario : $sgn(\sigma)$ mi da la parità del numero di trasposizioni che compaiono in una qualsiasi scrittura di σ come prodotto di trasposizioni.

1.6.5 osservazione : $ker(sgn) = A_n = \{\sigma \in S_n \mid sgn(\sigma) = 1\}$ detto *gruppo alterno* il gruppo delle permutazioni pari. $A_n \triangleleft S_n,\ |A_n| = \frac{n!}{2},\ S_n/A_n = \{\pm 1\}$.

Tabella di S_5 :

Elemento	*Ordine*	*Numero*
(ab)	2	$\binom{5}{2}1! = 10$
(abc)	3	$\binom{5}{3}2! = 20$
$(abcd)$	4	$\binom{5}{4}3! = 30$
$(ab)(cd)$	2	$\binom{5}{2}\binom{3}{2}\frac{1}{2} = 15$
$(abcde)$	5	$4! = 24$
$(abc)(de)$	6	$\binom{5}{3}2!\binom{2}{2}1! = 20$
		$tot = 120 = 5!$

Classi di coniugio in S_n :

1.6.1 Teorema : Due permutazioni di S_n sono coniugate se e solo se hanno lo stesso dipo di decomposizione in cicli disgiunti.

Dimostrazione : ($\Longrightarrow$) Siano σ e $\tau\sigma\tau^{-1}$ con $\sigma = (a_1\cdots a_k)$ e $\tau(a_i) = b_i$ allora $\tau\sigma\tau^{-1}(b_i) = \tau\sigma(a_i) = \tau(a_{i+1}) = b_{i+1}$ se $x \neq b_i\ \forall i \Longrightarrow \tau^{-1}(x) \neq a_i \Longrightarrow \tau\sigma\tau^{-1}(x) = \tau\sigma(\tau^{-1}(x)) = \tau\tau^{-1}(x) = x$ quindi il coniugato di un k-ciclo è un k-ciclo. se la permutazione è composizione di cicli disgiunti: $\sigma = \sigma_1\cdots\sigma_k \Longrightarrow \tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1}\cdots\tau\sigma_k\tau^{-1}$ è si riconduce al caso precedente $\tau(a_1\cdots a_k)_i\tau^{-1} = (\tau(a_1)\cdots\tau(a_k))_i$ essendo σ_i disgiunti implica $\tau\sigma_i\tau^{-1}$ disgiunti.
($\Longleftarrow$) dato il ciclo $\sigma = (a_1\cdots a_k)$ ed il ciclo $\rho = (b_1\cdots b_k)$ allora prendo τ tale che $\tau(a_i) = b_i \Longrightarrow \tau\sigma\tau^{-1} = \rho$; se ho più cicli disgiunti faccio come prima ciclo con ciclo dello stesso tipo :

$$\sigma = (x_{11}\cdots x_{1k_1})\cdots(x_{r1}\cdots x_{rk_r})$$
$$\downarrow \qquad\qquad \downarrow$$
$$\rho = (y_{11}\cdots y_{1k_1})\cdots(y_{r1}\cdots y_{rk_r})$$

con $\tau(x_{ij}) = y_{ij}$ e vale che $\tau\sigma\tau^{-1} = \rho$.

□

1.6.2 esempio : Date $\sigma = (12345)(67)(89)$ e $\rho = (24167)(35)(89)$ la permutazione τ tale che $\tau\sigma\tau^{-1} = \rho$ è $\begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 2&4&1&6&7&3&5&8&9 \end{pmatrix} = (12463)(57)$. Prendendo $\nu \in Z(\sigma)$ ho che $\tau\nu$ va ancora bene, infatti $\tau\nu\sigma\nu^{-1}\tau^{-1} = \tau\sigma\tau^{-1}$. Quindi tutte le permutazioni di questo tipo sono la classe laterale $\tau Z(\sigma)$.

Centralizzatore di σ in S_n

Dal teorema delle classi sappiamo che $|Z_{S_n}(\sigma)||Cl(\sigma)| = n!$ per il teorema precedente sappiamo calcolare $|Cl(\sigma)|$ quindi in particolare ci sappiamo calcolare $|Z_{S_n}(\sigma)|$.

1.6.3 esempio : Sia $\sigma = (1234)(56)$ in S_{10}; sappiamo che $|Z_{S_n}(\sigma)| = \frac{10!}{|Cl(\sigma)|} = 8\,4!$. Osserviamo che $H = S(7,8,9,10) \subset Z(\sigma)$, $(1234) \subset Z(\sigma)$, $(56) \subset Z(\sigma)$, da questo si deduce che $K < (1234), (56) >=< (1234) >< (56) >$ e $|K| = 8$, quindi $K < Z(\sigma)$ e $H < Z(\sigma)$ con $|H| = 4!$ e vale che $HK = Z(\sigma)$ per un discorso di cardinalità e siccome le permutazioni sono disgiunte $H \triangleleft Z(\sigma)$ e $K \triangleleft Z(\sigma)$ quindi $Z(\sigma) \cong H \times K \cong S_4 \times (\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}})$ (vedremo in seguito come si formalizza meglio questa osservazione).

1.7 Prodotti diretti

1.7.1 Definizione : Sia G un gruppo finito, $|G| = p^m n$ con p primo e $(n,p) = 1$, se $H < G$ con $|H| = p^m$ allora H si dice $p - sylow$ di G.

1.7.1 esempio : $|D_7| = 14$, $| < \rho > | = 7$ è un 7-sylow ed è unico, $< \rho^i\sigma >$ sono 7 2-silow, quindi in generale i p-sylow non sono unici.

1.7.1 Lemma : Siano $H, K \triangleleft G$, $H \cap K = \{e\} \Longrightarrow hk = kh \ \forall h \in H,\ k \in K$

Dimostrazione : $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ soccome K è normale allora $hkh^{-1} \in K \Longrightarrow hkh^{-1}k^{-1} \in K$ ma $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$ siccome H normale $kh^{-1}k^{-1} \in H \Longrightarrow hkh^{-1}k^{-1} \in H \Longrightarrow hkh^{-1}k^{-1} \in H \cap K = \{e\} \Longrightarrow hkh^{-1}k^{-1} = e \Longrightarrow hk = kh$.

□

1.7.1 Teorema : Sia G un gruppo e siano H, K sottogruppi normali di G se : $HK = G$ e $H \cap K = \{e\} \Longrightarrow G \cong H \times K$

Dimostrazione : Sia $\phi : H \times K \longrightarrow G$ tale che $\phi((h,k)) = hk$; ϕ è un omomorfismo per il lemma 1.7.1 è surgettiva per la prima ipotesi ed è iniettiva per la seconda ipotesi del teorema. □

1.7.1 osservazione : In un prodotto diretto i fattori commutano fra di loro.

1.7.2 esempio : $G = H \times K \Longrightarrow Z(H \times K) \cong Z(H) \times Z(K)$ per il lemma 1.7.1 in quanto $Z(H) \times \{e_k\}$ e $\{e_h\} \times Z(K)$ sono sottogruppi normali di $Z(H \times K)$; $Int(H \times K) \cong H \times K/_{Z(H \times K)} \cong H \times K/_{Z(H) \times Z(K)} \cong H/_{Z(H)} \times K/_{Z(K)} \cong Int(H) \times Int(K)$ dove il penultimo isomorfismo è dato da $\gamma : H \times K \longrightarrow H/_{Z(H)} \times K/_{Z(K)}$ con $\gamma((h,k)) = (h' + Z(H), k' + Z(K))$ e Th. di omomorfismo.

1.7.1 Proposizione : sia $\phi : Aut(H) \times Aut(K) \longrightarrow Aut(H \times K)$ con $\phi((f,g)) = \gamma$ dove $\gamma((h,k)) = (f(h), g(k))$ allora ϕ è un omomorfismo iniettivo ed è surgettivo $\Longleftrightarrow H \times \{e_k\}$ e $\{e_h\} \times K$ sono caratteristici in $H \times K$.

Dimostrazione : ϕ e γ sono ben definite infatti $\forall\ f, g \in Aut(H) \times Aut(K)$, $f(h) \in H$ e $g(k) \in K \Longrightarrow \gamma(h,k) = (f(h), g(k)) \in H \times K$.
γ è un omomorfismo : $\gamma[(h,k)(h',k')] = \gamma(hh', kk') = (f(hh'), g(kk') = (f(h)g(k), f(h')g(k')) = \gamma(h,k)\gamma(h',k')$.
γ è iniettiva : $Ker(\gamma) = \{(h,k) : (f(h), g(k)) = (e_h, e_k)\} = \{\{e_h\} \times \{e_k\}\}$.
γ è surgettiva : $\forall (h,k) \in H \times K\ \exists\ h' \in H\ k' \in K : \gamma(h',k') = (f(h'), g(k')) = (h,k)$. Qunidi γ è un automorfismo di $H \times K$.
ϕ è omomorfismo : $\phi((f,g)(l,m)) = \phi((f \circ l, g \circ m)) = \phi(f,g) \circ \phi(l,m)$.
ϕ è iniettivo : $Ker(\phi) = \{(f,g) | \phi(f,g) = Id_{H \times K}\} = \{(Id_H, Id_K)\}$.
Supponiamo adesso che $H \times \{e_k\}$ e $\{e_h\} \times K$ sono caratteristici in $H \times K$ e dimostriamo la surgettività quindi l'isomorfismo di ϕ : $\forall \gamma \in Aut(H,K)$ pongo $f : H \longrightarrow H$ con $f(h) = \pi_H \gamma(h, e_k)$ e $g : K \longrightarrow K$ con $g(k) = \pi_K \gamma(e_h, k)$; dico che $f \in Aut(h)$, $g \in Aut(K)$ e che $\gamma = \phi(f,g)$; f e g sono composizioni di omomorfismo quindi sono omomorfismi, $Ker(f) = \{h | \pi_H \gamma(h, e_k) = e_h\} = \{h | \pi_H(h', e_k) = e_h\} = \{h | e_h = h' = \gamma(h)\} = \{e_h\}$, analogamente per $Ker(g)$ quindi sono iniettive; siccome γ è surgettiva $\forall h' \in H\ \exists h \in H | \gamma(h, e_k) = (h', e_k)$ quindi $f(h) = \pi_H \gamma(h, e_k) = \pi_H(h', e_k) = h'$, analogamente per g quindi sono surgettive perciò sono automorfismo; per concludere $\phi(f,g)(h,k) = (\pi_H \gamma(h, e_k), \phi_K \gamma(e_h, k)) = (h', k') = \gamma(h,k)$. □

1.7.2 Proposizione : (Criterio per sottogruppi caratteristici) Sia $G = H \times K$ con $(|H| = n, |K| = m) = 1$ allora H e K sono caratteristici in G.

Dimostrazione : $f \in Aut(H \times K)$ con $f(h, e_k) = (h', k')$; $ord(h, e_k) = ordh|n$ quindi $ord(h', k') = [ord(h'), ord(k')]|n$ in particolare $ord(k')|n$ ma per ipotesi $ord(k')|m$ siccome $(n, m) = 1 \Longrightarrow k' = e_k$ quindi $f(H \times \{e_k\}) \subset H \times \{e_k\}$ analogo per $f(e_h, k)$.

□

1.7.1 esercizio : Studiare $Aut(\mathbb{Z}/_{20\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}})$.

soluzione : so che $Aut(\mathbb{Z}/_{n\mathbb{Z}}) \cong \mathbb{Z} * /_{\mathbb{Z}}$ quindi $Aut(\mathbb{Z}/_{20\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \cong Aut(\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}) \cong Aut(\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \times Aut(\mathbb{Z}/_{5\mathbb{Z}}) \cong Aut(\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \times \mathbb{Z}/_{4\mathbb{Z}}$, devo studiare $Aut(\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}})$:

so che gli automorfismi conservano l'ordine degli elementi. $G = \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ ha generatori $(0, 1)$ e $(1, 0)$ il primo va in elemento di ordine 4 tra $\{(0, 1), (0, 3), (1, 1), (1, 3)\}$ il secondo in un elemento di ordine 2 tra $\{(1, 2), (1, 0)\}$, escludo $(0, 2)$ perché siccome $(0, 1)$ va in $\{(0, 1), (0, 3), (1, 1), (1, 3)\}$ allora $(0, 2)$ va in $2\{(0, 1), (0, 3), (1, 1), (1, 3)\} = \{(0, 2)\}$ quindi se $(1, 0)$ va in $(0, 2)$ non sarebbe iniettivo quindi un automorfismo; d'altro canto i sottogruppi caratteristici devono andare in loro stessi per esempio $G^2 = 2G = \{2(x, y)|(x, y) \in G\} = \{(2x, 2y)|(x, y) \in G\} = \{(0, 0), (0, 2)\}$ è caratteristico, per ciò $\gamma(0, 2) = (0, 2)$; ottengo cosi 8 possibili automorfismi. Mostro che $Aut(\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \cong D_4$, sia $\alpha \in Aut(G)|\ \alpha((1, 0)) = (1, 2)$ e $\alpha((0, 1)) = (0, 1)$ osserviamo che $\alpha((x, y)) = \alpha(x(1, 0) + y(0, 1)) = (x, 2x + y) \Longrightarrow ord(\alpha) = 2$, sia $\Gamma((1, 0)) = (1, 2)$ e $\Gamma((0, 1)) = (1, 1)$ osserviamo che $\Gamma((x, y)) = (x + y, 2x + y)$ quindi $ord(\Gamma) = 4$ in conclusione basta vedere che $\Gamma\alpha = \alpha\Gamma^{-1}$.

1.7.2 esercizio : (permutazioni) sia $\rho = (1, 2, 3, 4)(5, 6) \in S_{10}$ calcolare $Z_{S_{10}}(\rho)$ e $N_{S_{10}}(< \rho >) = \{\tau \in S_{10}|\tau\rho\tau^{-1} \in < \rho >\}$.

soluzione : $|Z_{S_{10}}(\rho)| = |S_{10}|/_{|C_{S_{10}}(\rho)|} = 8 \times 4!$ consideriamo $H =< (1, 2, 3, 4), (5, 6) > \cong \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ e $K = S_{\{7,8,9,10\}} \cong S_4$ è facile vedere che questi due gruppi verificano le ipotesi del teorema 1.7.1 quindi $Z_{S_{10}}(\rho) \cong \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times S_4$.
$< \rho >= \{Id, \rho, \rho^2, \rho^{-1}\}$ quindi $N_{S_{10}}(< \rho >) = \{\tau \in S_{10}|\tau\rho\tau^{-1} = \rho$ e $\tau\rho\tau^{-1} = \rho^{-1}\} = Z_{S_{10}}(\rho) \cup \{\tau|\tau\rho\tau^{-1} = \rho^{-1}\}$, osservo che $\tau_0 = (2, 4)$ e $\tau_1 = (1, 4)(2, 3)(5, 6)$ appartengono a $\{\tau|\tau\rho\tau^{-1} = \rho^{-1}\}$ come le trovo tutte ? : $\tau_0\rho(\tau_0)^{-1} = \rho^{-1}$, $\tau_1\rho(\tau_1)^{-1} = \rho^{-1} \Longrightarrow (\tau_1)^{-1}\tau_0\rho(\tau_0)^{-1}\tau_1 = \rho \Longrightarrow (\tau_1)^{-1}\tau_0 \in Z_{S_{10}}(\rho) \Longleftrightarrow \tau_0 \in \tau_1 Z_{S_{10}}(\rho)$ allora $\{\tau|\tau\rho\tau^{-1} = \rho^{-1}\} = \tau_0 Z_{S_{10}}(\rho)$ quindi $|N_{S_{10}}(< \rho >) = 2|Z_{S_{10}}(\rho)|$. In generale $N_{S_n}(< \rho >) = \{\tau \in S_n|\tau\rho\tau^{-1} = \rho^k, (ord(\rho), k) = 1\} \Longrightarrow |N_{S_n}(< \rho >)| = |Z_{S_n}(\rho)||\{k|(k, ord(\rho)) = 1\}|$, ovvero è il centralizzatore per il numero di equazioni della forma $\tau\rho\tau^{-1} = \rho^k$ quindi $|N_{S_n}(< \rho >)| = |Z_{S_n}(\rho)|\phi(ord(\rho))$.

1.7.2 osservazione : il coniugio non cambia la forma della permutazione, perciò l'equazioni $\tau\rho\tau^{-1} = \rho^k$ hanno soluzione se e solo se k coprimo con $ord(\rho)$.

1.7.3 esercizio : Sia G un gruppo abeliano in cui tutti gli elementi hanno ordine 2. Allora G ha indice 2^n ed è isomorfo a $(\mathbb{Z}/_{2\mathbb{Z}})^n$.

soluzione : Siano $g_1, \cdots, g_h$ tale che $< g_1, \cdots, g_h >= (\mathbb{Z}/_{2\mathbb{Z}})^h$, sia $g \in G \ < g_1, \cdots, g_h >$, $< g >= \mathbb{Z}\_2\mathbb{Z}$; voglio vedere che $< g_1, \cdots, g_h, g >= (\mathbb{Z}/_{2\mathbb{Z}})^{h+1}$, perchè in questo modo aggiungendo sempre più elementi arrivo ad avere G e la tesi. Basta osservare che i sottogruppi $< g_1, \cdots, g_h >$ e $< g >$ sono normali e disgiunti e concludo con il teorema 1.7.1.

1.7.4 esercizio : Sia G un gruppo, $H \triangleleft G$ ciclico, $G/_H$ ciclico di ordine coprimo con $|H|$, G abeliano finito $\Longrightarrow G$ ciclico.

soluzione : Per ipotesi $H =< x >$, $G/_H =< g < x >>$ e $(o(g < x >), o(x)) = 1$; $\forall a \in G \Longrightarrow n, m \in \mathbb{N} : a = g^n x^m \Longrightarrow G =< g, x >$ ma $(o(g), o(x)) = (o(g < x >), o(x)) = 1$ supponiamo che $o(g) = s$ e $o(x) = t \Longrightarrow$ le equazioni $sc \equiv 1(t)$ e $td \equiv 1(s)$ hanno soluzione in particolare $g = (gx)^{td}$ e $x = (gx)^{sc}$ quindi $G =< gx >$ ed è ciclico.

1.7.5 esercizio : (Classificazione dei gruppi di ordine 8)

soluzione : L'ordine di un elemento divide l'ordine del gruppo; se esiste un elemento di ordine 8 allora G è ciclico ed isomorfo a $\mathbb{Z}/_{8\mathbb{Z}}$, se tutti gli elementi hanno ordine 2 allora G è abeliano ed isomorfo a $\mathbb{Z}^3/_{2\mathbb{Z}}$ per l'esercizio 1.7.3. Supponiamo allora di avere un elemento g di ordine 4, $< g >= C_4 \triangleleft G$; ci chiediamo se G contiene altri elementi di ordine 4 al di fuori di C_4, se la risposta è no $\Longrightarrow \exists h \notin C_4$ tale che $o(h) = 2$; consideriamo $\gamma_h : C_4 \longrightarrow C_4$ con $\gamma_h(x) = hxh^{-1}$ se $\gamma_h = Id_{C_4} \Longrightarrow G \cong \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ in quanto C_4 è normale e $< h >$ deve essere caratteristico quindi normale e si conclude con il teorema 1.7.1 se $\gamma_h \neq Id_{C_4} \Longrightarrow hgh^{-1} = g$ con $o(h) = 4$ e $o(g) = 2$ quindi $G \cong D_4$. Se la risposta è si ovvero $\exists k \notin C_4$ tale che $o(k) = 4$ allora consideriamo $\gamma_k : C_4 \longrightarrow C_4$ con $\gamma_k(x) = kxk^{-1}$, se $\gamma_k = Id_{C_4}$ allora $G \cong \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ infatti $< g >= C_4$ e $< k >= C_4'$ quindi G si immerge in $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}$ che ha solo $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ come sottogruppo di ordine 8; se $\gamma_k \neq Id_{C_4}$ allora $o(k) = 4$, $o(g) = 4$, $kgk^{-1} = g^{-1}$ e $o(kg) = 4$ infatti $(kg)^2 = kgkg = kgg^{-1}k = k^2 \neq e$ abbiamo quindi $G = \{e, g, g^2, g^3, k, k^3, kg, (kg)^{-1}\}$ e dico che $G \cong Q_8$. in conclusione abbiamo 5 gruppi distinti a meno di isomorfismo.

1.5.4 Proposizione : (Criterio per stabilire se un sottogruppo è normale) Sia G un gruppo di ordine n e p il più piccolo primo che divide n, se $H < G$ tale che $[G : H] = p \Longrightarrow H \triangleleft G$.

Dimostrazione : Considero l'insieme delle classi laterali di H, $X = \{g_1H, \ldots, g_pH\} = G/H$, considero inoltre l'azione $\gamma : G \longrightarrow S(X)$ con $\gamma(g) = \pi_g$ e dove $\pi_g(g_1H) = gg_iH$, questa azione non fa altro che permutare le classi ovvero tanti quanti sono i modi di per permutare p elementi, quindi $S(X) \cong S_p$ (non confonderti con il teorema di cayley che in questo caso dice solo che G si immerge in S_n). Il nucleo di questo omomorfismo è $ker\gamma = \{g \in G \mid gg_iH = g_iH \ \forall i \in$

$\{1,\dots,p\}\} = \{g \mid g \in \bigcap_{x\in G} stab(xH)\}$, $g \in stab(xH) \Longrightarrow gxH = xH \Longrightarrow x^{-1}gxH = H \Longleftrightarrow x^{-1}gx \in H \Longleftrightarrow g \in xHx^{-1}$ quindi $g \in \bigcap_{x\in G} xHx^{-1} \stackrel{def}{=} H_G$, ($g \in xHx^{-1}$ ha senso in quanto xHx^{-1} è un gruppo, non ha senso la scrittura $g \in xH$ in quanto xH non è un gruppo). Per il primo teorema di omomorfismo sappiamo che $G/H_G \longrightarrow S_p$ è iniettiva quindi si immerge in S_p da cui $|G/H_G| \mid p!$ quindi ci sono due possibilità: $|G/H_G| \in \{1,p\}$, in quanto divide $p!$ che ha come più grande primo p ed n che ha come più piccolo primo p, sapendo che $H \in X$ abbiamo che in particolare $g \in ker \Longrightarrow gH = H \Longleftrightarrow g \in H \Longrightarrow H_G \subset H \Longrightarrow |G/H_G| \geq p$ quindi non può essere 1 ed è proprio p inoltre $H = H_G$ avendo lo stesso indice ed essendo $H_G \subset H$ per ciò H è il nucleo di un omomorfismo quindi $H \triangleleft G$ e vale la tesi.

□

1.7.3 osservazione Sia G un gruppo allora $\{g \in G | o(g) = \infty\}$ è un insieme caratteristico, se questo insieme è un sottogruppo allora è un sottogruppo caratteristico ed in generale lo è se G è abeliano.

1.7.6 esercizio : Determinare $|Aut(\mathbb{Z} \times \mathbb{Z}/_{4\mathbb{Z}})|$.

soluzione : Innanzi tutto osserviamo che $\{0\} \times \mathbb{Z}/_{n\mathbb{Z}}$ è caratteristico infatti se $(0,[1])$ ha immagine in (a,b) con $a \neq 0$ allora non sarebbe un omomorfismo in quanto $o(a,b) = \infty$ e $o(0,[1]) = n$. Sia $\gamma \in Aut(G)$ allora per quanto detto $\gamma(\{0\} \times \mathbb{Z}/_{n\mathbb{Z}}) = \{0\} \times \mathbb{Z}/_{n\mathbb{Z}}$ e considero $\gamma' : (\mathbb{Z} \times \mathbb{Z}/_{n\mathbb{Z}})/_{\{0\}\times\mathbb{Z}/_{n\mathbb{Z}}} \cong \mathbb{Z} \longrightarrow (\mathbb{Z} \times \mathbb{Z}/_{n\mathbb{Z}})/_{\{0\}\times\mathbb{Z}/_{n\mathbb{Z}}} \cong \mathbb{Z}$; scrivo una specie di matrice dove la prima colonna è l'mmagine di $(1,[0])$ e la seconda è l'immagine di $(0,[1])$:

$$\begin{pmatrix} c & 0 \\ [b] & [a] \end{pmatrix}$$

$c = \gamma'((0,[0])) = \{\pm 1\}$, $[b] = \gamma((1,[0])) \in \mathbb{Z}/_{n\mathbb{Z}}$, $[a] \in (\mathbb{Z}/_{n\mathbb{Z}})^*$ quindi $\gamma((x,y)) = (c,[b])x + (0,[a])y$, questa matrice descrive esattamente l'automorfismo, quindi contando i possibili $c,[a],[b]$ otteniamo che $|Aut(\mathbb{Z} \times \mathbb{Z}/_{n\mathbb{Z}})| = 2n\phi(n)$, i particolare in questo esercizio la cardinalità è 16.

1.7.7 esercizio : Sottogruppi caratteristici di $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$.

soluzione : sono $2\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \cong (\mathbb{Z}/_{2\mathbb{Z}})^2$ che sono tutti gli elementi di ordine minore o uguale a 2 e $2\mathbb{Z}/_{4\mathbb{Z}} \times \{0\}$ che è il gruppo dei quadrati.

1.7.4 osservazione : Se G abeliano, $n \in \mathbb{Z}$ allora $\Gamma_n : G \longrightarrow G$ con $\Gamma_n(g) = ng$ è un omomorfismo e $Ker(\Gamma)$ e $Imm(\Gamma)$ sono caratteristici infatti se $ng = 0 \Longrightarrow n\Gamma(g) = \Gamma(ng) = 0$ e se $h = ng \Longrightarrow \Gamma(h) = \Gamma(ng) = n\Gamma(g)$.

Capitolo 2

Prodotto Semidiretto

2.1 Il prodotto semidiretto

2.1.1 Definizione : Siano H, K dei gruppi, sia $\gamma : K \longrightarrow Aut(H)$ un omomorfismo tale che $\gamma(k) = \gamma_k \in Aut(H)$, $\gamma_k : H \longrightarrow H$ con $\gamma_k(h) = h' \in H$, si dice *prodotto semidiretto di H e K via γ* il prodotto cartesiano $H \times K$ con l'operazione definita da $(h, k) * (h', k') = (h\gamma_k(h'), kk')$ e si indica $(H \times K, *) = H \rtimes_\gamma K$.

2.1.1 osservazione : Il ruolo di H e K non è simmetrico ovvero $H \rtimes_\gamma K$ e $K \rtimes_{\gamma'} H$ sono due oggetti diversi.

2.1.1 Proposizione : $H \rtimes_\gamma K$ è un gruppo.

Dimostrazione : La chiusura rispetto all'operazione deriva dal fatto che H e K sono gruppi, l'operazione è associativa infatti $(a, b)((c, d)(e, f)) = (a, b)(c\gamma_d(e), df) = (a\gamma_b(c\gamma_d(e)), bdf) = (a\gamma_b(c)\gamma_b(\gamma_d(e)), bdf) = (a\gamma_b(c)\gamma_{bd}(e), bdf) = (a\gamma_b(c), bd)(e, f) = ((a, b)(c, d))(e, f)$; esiste l'elemento neutro che è (e_H, e_k) infatti $(h, k)(e_H, e_K) = (h\gamma_k(e_H), k) = (h, k)$ e $(e_H, e_K)(h, k) = (e_h\gamma_{e_K}(h), k) = (h, k)$, ed esiste l'inverso che è $(\gamma_{k^{-1}}(h^{-1}), k^{-1})$ infatti $(h, k)(\gamma_{k^{-1}}(h^{-1}), k^{-1}) = (h\gamma_k(\gamma_{k^{-1}}(h^{-1}), kk^{-1}) = (hh^{-1}, e_K) = (e_H, e_K)$, analogamente per la moltiplicazione a sinistra. □

2.1.2 osservazione : Il prodotto diretto è un caso particolare del prodotto semidiretto, ovvero quando l'omomorfismo γ è banale $\gamma(K) = Id_H \in Aut(H)$ infatti $(h, k) * (h', k') = (h\gamma_k(h'), kk') = (hId_k(h'), kk') = (hh', kk')$. Consideriamo per esempio $\mathbb{Z}/_{7\mathbb{Z}} \rtimes_\gamma \mathbb{Z}/_{7\mathbb{Z}}$ studiamo l'omomorfismo; $\gamma : \mathbb{Z}/_{7\mathbb{Z}} \longrightarrow (\mathbb{Z}/_{7\mathbb{Z}}) \cong \mathbb{Z}/_{6\mathbb{Z}}$, per una questione di ordine $\gamma([1]_7) = [0]_6$ quindi $\gamma(\mathbb{Z}/_{7\mathbb{Z}}) = \{[0]_6\}$ e con cio si deduce che esiste solo il prodotto diretto fra i due gruppi quindi è isomorfo a $\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}}$; ricorda che $[0]_6$ è un automorfismo.

2.1.3 osservazione : Dati $\bar{H} = H \times \{e_k\}$ e $\bar{K} = K \times \{e_H\}$ so che $\bar{H}, \bar{K} \triangleleft H \times K$. inoltre $\bar{H} \triangleleft H \rtimes_\gamma K$ infatti $\pi_K : H \rtimes_\gamma K \Longrightarrow K$ con $\pi_K((h,k)) = k$ è un omomorfismo e $H = Ker(\pi_K)$, invece $K \triangleleft H \rtimes_\gamma K \Longleftrightarrow$ il prodotto è diretto.

2.1.4 osservazione : Sia G un gruppo e H, K due suoi sottogruppi dove $H \triangleleft G$. allora HK è un sottogruppo di G. l'unica proprietà non banale è la chiusura per l'operazione; siano $hk, h'k' \in HK$ con $h, h' \in H$ e $k, k' \in K$, allora $hkh'k' = (hkh'k^{-1})kk' \in HK$ infatti per la normalità di H, $kh'k^{-1} \in H$ quindi $hkh'k^{-1} \in H$ e $kk' \in K$.

2.1.1 Teorema : (Scomposizione di un gruppo) Sia G un gruppo, siano $H \triangleleft G$ e $K < G$ sottogruppi, se $HK = G$ e $H \cap K = \{e_G\}$ allora $G \cong H \rtimes_\gamma K$ dove $\gamma : K \longrightarrow Aut(H)$ con $\gamma(k) = khk^{-1}$.

Dimostrazione : Intanto L'omomorfismo γ è ben definito in quanto H è normale, consideriamo adesso l'omomorfismo $F : H \rtimes_\gamma K \longrightarrow G$ con $\gamma((h,k)) = hk$; F è ben deinita, è un omomorfismo infatti $F((h,k) * (h',k')) = F(h\gamma_k(h'), kk') = h\gamma_k(h')kk' = hkh'k^{-1}kk' = hkh'k' = F(h,k)F(h',k')$; inoltre è surgettive perchè $HK = G$ ed iniettiva perchè se $F(h,k) = hk = e_G \Longrightarrow h = k^{-1} \Longrightarrow h, k \in H \cap K = \{e_G\}$.

□

2.1.1 esempio : $S_n \cong A_n \rtimes_\gamma < (1,2) >$ dove $\gamma_{(1,2)}(\sigma) = (1,2)\sigma(1,2)$; $D_n \cong < \rho > \rtimes_\gamma < \sigma >$ dove $\gamma_\sigma(\rho) = \sigma\rho\sigma^{-1} = \rho^{-1}$; $\mathbb{Z}/_{5\mathbb{Z}} \rtimes_\gamma \mathbb{Z}/_{3\mathbb{Z}}$, $\gamma : \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow (\mathbb{Z}/_{5\mathbb{Z}})^* \cong \mathbb{Z}/_{4\mathbb{Z}}$ ma $(3, \phi(5)) = 1 \Longrightarrow \mathbb{Z}/_{5\mathbb{Z}} \rtimes_\gamma \mathbb{Z}/_{3\mathbb{Z}} \cong \mathbb{Z}/_{5\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$ esiste un solo gruppo di ordine 15.

2.1.1 esercizio : (Classificazione gruppi di ordine pq con p, q primi)

soluzione : Se $p = q$ allora $|G| = p^2$ quindi G è abeliano e sappiamo che ci sono solo $\mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{9\mathbb{Z}}$ o $\mathbb{Z}/_{p^2\mathbb{Z}}$; supponiamo allora senza perdita di generalità $q > p$, per il teorema di Cauchy esistono due gruppi $H, K < G$ di ordine rispettivamente q, p, sappiamo che $H \triangleleft G$ perché ha indice il più picco primo che divide l'ordine del gruppo (Proposizione 1.5.4), oppure perché è l'unico sottogruppo di ordine q (questo ci dice che H è caratteristico) infatti supponiamo ci sia H' tale che $|H'| = q$ allora $|HH'| = |H||H'|/_{|H \cap H'|}$ ma $|H||H'| = q^2$ e $|H \cap H'|$ può essere 1 o q quindi $|HH'|$ può essere q^2 o q, q^2 è assurdo perché è maggiore della cardinalità del gruppo, q implica che $H = H'$ quindi è unico. Usando il Teorema 2.1.1 posso dire che $G \cong H \rtimes_\gamma K$ in quanto per una questione di ordine si ha che $H \cap K = \{e_g\}$ e che $|HK| = |H||K|/_{H \cap K} = |H||K| = pq$ siccome $HK \subset G$ allora sono uguali (ricordiamo che il fatto che H sia normale garantisce che HK sia un gruppo). Supponiamo che $H =< x >$ e $K =< y >$ allora avremo che $\gamma :< y > \longrightarrow Aut(< x >)$ con $\gamma(y) = \gamma_y$ dove $\gamma_y(x) = yxy^{-1} = x^l$; siccome γ è un omomorfismo deve valere che $ord(\gamma_y) | ord(y)$ quindi se $p \nmid q - 1 (|Aut < x > | = q - 1)$ allora $\gamma_y = Id_H$ e $G \cong \mathbb{Z}/_{pq\mathbb{Z}}$ se $p | q - 1$ allora oltre al gruppo precedente ho un'altro gruppo, biso-

gna solo determinare γ; $Aut < x > \cong \mathbb{Z}/_{q-1\mathbb{Z}}$ quindi gli elementi di ordine p sono $p-1$ che sono le scelte possibili dove posso mandare y posso quindi generare differenti gruppi diversi, ma vogliamo mostrare che questi $p-1$ gruppi sono tutti isomorfi tra loro; consideriamo due qualunque omomorfismi γ e γ' tale che $\gamma_y(x) = x^l$ e $\gamma'_y(x) = x^{l'}$ con l, l' coprimi con q, si ha che $(\gamma_y)^p = Id \Longrightarrow x^{l^p} = x \Longrightarrow l^p = 1$ quindi $ord(l) = ord(l') = p$ allora esiste $r \in (N)$ tale che $l' = l^r$ con $0 < r < p-1$ da questo segue che $\gamma'_y = \gamma_{y^r}$ infatti $\gamma_{y^r}(x) = (\gamma_y(x))^r = x^{l^r} = x^{l'}$; concludiamo esibendo $\psi : H \rtimes_\gamma K \longrightarrow H \rtimes_{\gamma'} K$ tale che $\psi((x,y)) = (x, y^r)$, questo è un isomorfismo (facile verifica) e possiamo dire che ogni prodotto semidiretto genera gruppi isomorfi quindi in questo caso ci sono solo due gruppi di ordine pq a meno di isomorfismo.

2.2 Ancora sulle permutazioni

(Classi di coniugio di A_n) Sappiamo che $|Z_{S_n}(\sigma)||Cl_{S_n}(\sigma)| = n!$ per il teorema delle classi, analogamente si ha che se $\sigma \in A_n$ allora vale $|Z_{A_n}(\sigma)||Cl_{A_n}(\sigma)| = n!/_2$ dove $Z_{A_n}(\sigma) = \{\rho \in A_n | \rho\sigma\rho^{-1} = \sigma\} = Z_{S_n}(\sigma) \cap A_n$.

2.2.1 Lemma : Sia $H < S_n$ allora $|H \cap A_n|$ è uguale a $|H|$ se $H \subset A_n$ oppure $|H|/_2$ se $H \not\subset A_n$.

Dimostrazione : Basta vedere che:

$$H \xrightarrow{\phi} S_n(\mathbb{R}) \xrightarrow{Surg.} S_n/_{A_n} = \{\pm 1\}$$
$$\gamma$$

$Ker(\gamma) = H \cap A_n$ e $H/_{A_n}$ si immerge in $\{\pm 1\}$ quindi $|Z_{A_n}(\sigma)|$ e uguale a $|Z_{S_n}(\sigma)|$ di conseguenza $|Cl_{A_n}(\sigma)| = |Cl_{S_n}(\sigma)|/_2$ viceversa $|Z_{A_n}(\sigma)|$ e uguale a $|Z_{S_n}(\sigma)|/_2$ di conseguenza $|Cl_{A_n}(\sigma)| = |Cl_{S_n}(\sigma)|$.

2.2.1 esercizio : I 3-cicli sono tutti coniugati in A_n per $n \geq 5$. (per $n = 3$ o $n = 4$ no)

soluzione : Sia $\sigma = (a,b,c)$ in S_n con $n \geq 5$, osserviamo che $(d,e) \in Z_{S_n}(\sigma)/Z_{A_n}(\sigma)$ con $d, e \notin \{a,b,c\}$, quindi per lemma precedente $|Cl_{A_n}(\sigma)| = |Cl_{S_n}(\sigma)|$; se $n = 3$, $A_3 =< (1,2,3) >$ allora $Cl_{S_3}((1,2,3)) = \{(1,2,3),(1,3,2)\}$ ma $|Cl_{S_3}((1,2,3))| = 2 \nmid 3 = |A_3|$ quindi $Cl_{S_3}((1,2,3)) = \{(1,2,3)\}$; se $n = 4$ si ha che $|A_4| = 12$ e $|Cl_{S_4}((a,b,c))| = \binom{4}{3}2! = 8 \nmid 12$ quindi $|Cl_{S_4}((a,b,c))| = 4$.

2.2.2 esercizio : I 5-cicli non sono tutti coniugati in A_5.

soluzione : le classi di coniugio di un 5-ciclo in S_5 sono 4!, se lo fossero anche in A_5 allora il centralizzatore in A_4 avrebbe cardinalità 5_2 assurdo quindi si deve spezzare.

2.2.1 esempio : A_4 non ha sottogruppi di ordine 6; se $\exists H < A_4$ tale che $|H| = 6$ allora $H \triangleleft A_4$ ed $\exists \sigma \in H$ dove $ord(\sigma) = 2$ e $\sigma = (a,b)(c,d)$. Osserviamo che $Cl_{S_4}(\sigma) = \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} = Cl_{A_4}(\sigma))$ inoltre $\mathbb{K} = \{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \triangleleft S_4$ ma se H normale e $\sigma \in H$ allora $Cl_{A_4}(\sigma) \subset H$ di conseguenza $\mathbb{K} \triangleleft H$ ma è assurdo infatti $|\mathbb{K}| = 4 \nmid 6 = |H|$.

2.2.1 Proposizione : A_n, $n \geq 5$ è semplice cioè non ha sottogruppi normali non banali.

Dimostrazione : Se $n = 5$ allora $|A_n| = 60$; consideriamo $H \triangleleft A_5$, se H contiene un 3-ciclo li contiene tutti ma siccome generano A_n allora $H = A_n$, se contiene un2 $\times$ 2-ciclo per coniugio contiene un 3-ciclo (es. ((1,2)(3,4))((1,5)(3,4))=(1,5,2)e si conclude come prima, se H contiene un 5-ciclo per coniugio contiene un 3-ciclo (es. (1,2,3,4,5)(1,5,3,4,2)=(3,4,5))e si conclude come prima, allora H è banale. Se $n \geq 6$ consideriamo $A_n \supset G_i = \{\sigma \in A_n | \sigma(i) = 1\} \cong A_{n-1}$ ogni G_i è coniugato tra loro. Facciamo una Induzione su n:

Passo Base: Gia verificato.

Passo Induttivo : Sia $N \triangleleft A_n \implies N \cap G_i \triangleleft G_i$ che per induzione si ha $N \cap G_i = G_i$ o $N \cap G_i = \{e\}$ $\forall i$; se $N \cap G_i = G_i$ per un cero i allora contiene almeno un 3-ciclo quindi $N = A_n$, se $N \cap G_i = \{e\} \forall i$ allora N è il sottogrupppo degli elementi che non fissano nessun elemento. Prendiamo $\sigma, \tau \in N$ se $\sigma(i) = \tau(i) \implies \sigma\tau^{-1}(i) = i \implies \sigma\tau^{-1} \implies \sigma = \tau$, fatta questa considerazione scrivo σ come prodotto di cicli disgiunti di lunghezza $r_1, \cdots, r_k$ decrescenti, ovvero $\sigma = C_1 \cdots C_k$. Supponiamo $r_i \geq 3$ per qualche i, quindi $C_i = (i_1, i_2, i_3, \cdots)$, prendo $\rho = (i_3, j, k)$ tale che $j, k \notin \{i_1, i_2, i_3\}$ allora $\rho\sigma\rho^{-1} = \tau$ e $\sigma(i_1) = \tau(i_1) = i_2$ ma $\sigma \neq \tau$ assurdo; quindi $\forall i$, $i = 2$ ovvero $\sigma = (i,j)(k,l)\cdots$ è prodotto di trasposizioni, prendo allora $\rho = (l,p,q)$ con $p, q \notin \{i,j,k\} \implies \tau = \rho\sigma\rho^{-1}$ e σ sono distinti ma $\sigma(i) = \tau(i) = j$, assurdo, quindi N è banale e A_n è perciò semplice.

□

sottogruppi normali di S_n : Per $n = 4$ si hanno oltre a quelli banali A_4 e $< (1,2)(3,4),(1,3)(2,4) >$. Per $n \geq 5$ S_n ha un solo sottogruppo normale che è A_n, infatti se $H \triangleleft S_n$ e $H \nmid A_n$ allora $H \cap A_n \triangleleft A_n$ ma siccome A_n è semplice $H \cap A_n = \{e\} \implies H$ è generato da una trasposizione quindi non è normale.

2.3 Il Teorema di Sylow

2.3.1 Teorema :(di Sylow) Sia G un gruppo finito, p primo tale che $|G| = p^n m$ con $(m, p) = 1$ allora :

esistenza : $\forall \alpha$, $0 \leq \alpha \leq n$ $\exists$ $H < G$ tale che $|H| = p^\alpha$.

inclusione :(versione debole) Ogni p-gruppo di G è contenuto in un p-sylow (se $H < G$ tale che $|H| = p^\alpha$ con $0 \leq \alpha \leq n$ allora H è contenuto in un sottogruppo di G di ordine $p^{\alpha+1}$).

coniugio : due qualsiasi p-sylow sono coniugati.

numero : $n_p = \#p$-sylow di G allora $n_p||G|$ e $n_p \equiv 1\ (p)$.

Dimostrazione :

Esistenza : Fisso $\alpha \in [0, n]$. Sia $\mathbb{M} = \{M \subset G||M| = p^\alpha\}$; allora $|\mathbb{M}| = \binom{p^n m}{p^\alpha} = \frac{(p^n m)!}{p^\alpha!(p^n m - p^\alpha)} = (p^n m \prod_{i=1}^{p^{\alpha-1}} (p^n m - i))/(p^\alpha \prod_{i=1}^{p^{\alpha-1}} (p^{\alpha-i})) = p^{n-\alpha} m \prod_{i=1}^{p^{\alpha-1}} (\frac{p^n m - i}{p^\alpha - i})$; osserviamo quindi che $p^{n-\alpha}||\mathbb{M}|$ e per $i = 1, \cdots, p^{\alpha-1}$ si ha che $v_p(p^n m - i) = v_p(p^\alpha - i) = v_p(i)$, dove v_p e l'omomorfismo di valutazione, quindi $v_p(\frac{p^n m - i}{p^\alpha - i}) = 0$ perciò $p^{n-\alpha}$ divide esattamente $|\mathbb{M}|$. Consideriamo ora l'azione di G su $\mathbb{M}$ data da $\phi : G \longrightarrow S(\mathbb{M})$ con $\phi(g) = \phi_g$ dove $\phi_g(M) = gM$; per il teorema delle classi $|\mathbb{M}| = \sum_{M_i \in R} |orb(M_i)| = \sum_{M_i \in R} \frac{|G|}{|stab(M_i)|}$ dove R è l'insieme dei rappresentanti delle orbite. Dico che esiste M_i tale che $|stab(M_i)| = p^\alpha$, intanto siccome $p^{n-\alpha}||\ |\mathbb{M}|$ allora non tutte le orbite hanno cardinalità multipla di $p^{n-\alpha+1}$ quindi esiste i tale che $p^{n-\alpha+1} \nmid |orb(m_i)| = \frac{p^n m}{stab(M_i)}$ quindi $p^\alpha | stab(M_i)$. In conclusione considero l'applicazione $\tau : stab(M_i) \longrightarrow M_i$ con $\tau(y) = yx$ dove $x \in M_i$, questa applicazione è iniettiva e siccome $|M_i| = p^\alpha$ allora $|stab(M_i)| \leq p^\alpha$ ma $p^\alpha | stab(M_i)$ perciò $p^\alpha = stab(M_i)$, dato che $stab(M_i) < G$ la tesi è verificata.

Inclusione : Sia $H < G$ con $|H| = p^\alpha$ e sia S un p-sylow di G. Consideriamo $X = G/_S$ l'insieme delle classi laterali e costruiamo l'applicazione $F : H \longrightarrow S(X)$ con $F(h) = \gamma_h$ dove $\gamma_h(gS) = hgS$; F è un'azione di H su X. Si ha che $m = |X| = [G : S] = \sum_{g_i \in R} |orb(g_i S)| = \sum_{g_i \in R} \frac{|H|}{stab(g_i S)} = \sum_{g_i \in R} \frac{p^\alpha}{stab(g_i S)}$ con R l'insieme dei rappresentanti delle orbite; ponendo $|stab(g_i S) = p^{n_i}$ si ha che $m = \sum_i p^{\alpha - n_i}$ ma $p \nmid m$ quindi esiste i_0 tale che $n_{i_0} = \alpha$ e $p^{\alpha - n_{i_0}} = 1$ quindi vale che $\forall h \in H\ h g_{i_0} = g_{i_0}$ allora $\forall h \in H\ g_{i_0}^{-1} h g_{i_0} \in S \iff h \in g_{i_0} S g_{i_0}^{-1} \iff H \subset g_{i_0} S g_{i_0}^{-1}$ siccome S è un p-sylow, è $g_{i_0} S g_{i_0}^{-1}$ è un gruppo con la stessa cardinalità allora $g_{i_0} S g_{i_0}^{-1}$ è un p-sylow e la tesi è confermata.

Coniugio : Siano H, S p-sylow, per la parte Inclusione applicata ad H so che esiste g tale che $H \subset g_{i_0} S g_{i_0}^{-1}$ per questioni di cardinalità vale $H = g_{i_0} S g_{i_0}^{-1}$ quindi la tesi.

Numero : Sia S un p-sylow, allora $n_p = \#p\text{-sylow} = \#\text{coniugati di } S \text{ in } G = [G : N_G(S)] \mid |G|$. Consideriamo ora l'azione di S su $Y = \{\text{coniugati di } S \text{ in } G\}$ ovvero $\phi : S \longrightarrow S(Y)$ con $\phi(g) = \gamma_g$ dove $\gamma_g(xSx^{-1}) = gxSx^{-1}g^{-1}$; dico che $orb(S)$ è l'unica orbita banale di questa azione, infatti sia $H \in Y$ tale che $orb(H) = \{H\}$, $S = stab(H) = \{s \in S | sHs^{-1} = H\} \iff S \subset N_G(H) \iff SH = HS \iff HS < G$ ora $|HS| = \frac{|H||S|}{|H \cap S|} = \frac{p^n p^n}{|H \cap S|}$ ma siccome $HS < G \implies |HS| \mid |G| = p^n m \implies |H \cap S| = p^n \implies H = S$. Uso ora che $|Y| = n_p = \sum_{H \in R} |orb(H)| = |orb(S)| + \sum_{H \in R/\{S\}} |orb(H)| = 1 + \sum_{H \in R/\{S\}} \frac{|S|}{|stab(H)|} \implies n_p = 1 + lp^k \implies n_p \equiv 1$ (p), dove R è l'insieme dei rappresentanti delle orbite, e la tesi è verificata.

□

2.3.1 esempio : Sia $G = S_4$, $|S_4| = 2^3 3$; sia P un 2-sylow di $S_4 \implies |P| = 8$ allora $P \cong D_4$ quindi D_4 si immerge in S_4.

2.3.1 esercizio : Chi è il 2-sylow di S_6.

2.3.2 esercizio : (Classificazione dei gruppi di ordine 12)

soluzione : Sia G tale che $|G| = 12 = 2^2 3$, vediamo il numero dei p-sylow; $n_3 \equiv 1\ (3)$ e $n_3 | 12$ allora $n_3 \in \{1, 4\}$, $n_2 \equiv 1\ (2)$ e $n_2 | 12$ allora $n_2 \in \{1, 3\}$ quindi uno tra il 2-sylow o 3-sylow è normale; il 2-sylow ha ordine 4 quindi è abeliano e può essere isomorfo a $\mathbb{Z}/_{4\mathbb{Z}}$ oppure $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$, il 3-sylow analogamente è isomorfo a $\mathbb{Z}/_{3\mathbb{Z}}$. Se il 3-sylow non è normale allora ha 4 coniugati, siccome l'intersezione tra questi è banale ci sono 8 elementi di ordine 3, restano solo 4 elementi liberi che comporranno il 2-sylow che sarà dunque unico perciò normale, usando il Teorema 2.1.1 otteniamo che $G \cong \mathbb{Z}/_{4\mathbb{Z}} \rtimes_\gamma \mathbb{Z}/_{3\mathbb{Z}}$ oppure $(\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z})/_{2\mathbb{Z}} \rtimes_\psi \mathbb{Z}/_{3\mathbb{Z}}$, studiamo quindi gli omomorfismi; $\gamma : \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{4\mathbb{Z}}) \cong \mathbb{Z}/_{2\mathbb{Z}}$, per questioni di ordine $\gamma([1]_3) = Id_{\mathbb{Z}/_{4\mathbb{Z}}}$ quindi c'è un prodotto diretto $G \cong \mathbb{Z}/_{12\mathbb{Z}}$. $\psi : \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \cong S_3$ quindi $\psi([1]_3) \in \{Id, \sigma, \sigma^2\}$ cioè due prodotti semidiretti e un gruppo abeliano $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{6\mathbb{Z}}$, dico che i due omomorfismo generano gruppi isomorfi; consideriamo l'azione di G su i 3-sylow data da $\phi : G \longrightarrow S(P_3) \cong S_4$ (P_3 è l'insieme dei 3-sylow), il $Ker(\phi) = \{g \in G | \forall P \in P_3 \phi_g(P) = P\} \iff \{g \in G | \forall P \in P_3 gPg^{-1} = P\} = \bigcap_{P \in P_3} N(P)$ ma $N(P) = P$ infatti $gPg^{-1} = P \iff g \in P$ quindi $\bigcap_{P \in P_3} N(P) = \bigcap_{P \in P_3} P = \{e\}$ perciò G si immerge in S_4, ma in S_4 c'è un unico sottogruppo di ordine 12 che è A_4 quindi $G \cong A_4$ e i due prodotti semidiretti generano lo stesso gruppo (è unico perchè se $H < S_4$ tale che $|H| = 12$ allora $|H \cap A_4| = 12$ oppure 6, ma per l'esempio 2.2.1 A_4 non ha sottogruppi di ordine 12 quindi $H = A_4$).
Se il 3-sylow è normale abbiamo, sempre per il teorema 2.1.1, $\mathbb{Z}/_{3\mathbb{Z}} \rtimes_\tau \mathbb{Z}/_{4\mathbb{Z}}$ oppure $\mathbb{Z}/_{3\mathbb{Z}} \rtimes_\sigma (\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}})$, studiamo quindi gli omomorfismi. $\tau : \mathbb{Z}/_{4\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{3\mathbb{Z}}) \cong \mathbb{Z}/_{2\mathbb{Z}}$, abbiamo

$\tau([1]_4) = Id_{\mathbb{Z}/_{3\mathbb{Z}}}$ che da un prodotto diretto già visto prima e $\tau([1]_4) = -Id_{\mathbb{Z}/_{3\mathbb{Z}}}$, inoltre abbiamo $\sigma : (\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \longrightarrow Aut(\mathbb{Z}/_{3\mathbb{Z}}) \cong \mathbb{Z}/_{2\mathbb{Z}}$ dove abbiamo sempre uno banale già visto prima e 3 non banali che danno D_6.

2.3.1 osservazione : $S_3 \times \mathbb{Z}/_{2\mathbb{Z}}$ ha ordine 12 ma non l'ho contato prima, perché? è facile vedere che $S_3 \times \mathbb{Z}/_{2\mathbb{Z}} \cong D_6$.

2.4 Il Teorema di Struttura per gruppi abeliani finiti

2.4.1 Teorema : Sia G un gruppo abeliano finito, allora G è prodotto diretto dei suoi p-sylow.

Dimostrazione : Sia $|G| = p_1^{e_1} \cdots p_r^{e_r}$, faccio una induzione su r :

Passo Base : per $r = 1$ G è un p-gruppo quindi è dimostrato.

Passo Induttivo : Sia $d|\,|G|$ consideriamo $G_d = \{x \in G | dx = 0\}$ e l'omomorfismo $\gamma_d : G \longrightarrow G$ con $\gamma_d(x) = dx$, G_d è il nucleo di questo omomorfismo, scrivo inoltre che $|G| = p^e m$ con m che ha $r-1$ fattori primi distinti. Dico che $G \cong G_{p^e} \times G_m$ infatti $G_{p^e} = \{g \in G | p^e g = 0\}$ è un p-gruppo, se un primo $q|\,|G_{p^e}|$ per cauchy esiste $y \in G_{p^e}$ tale che $ord(y) = q \Longrightarrow p = q$; inoltre G_{p^e} è un p-sylow infatti se S è un p-sylow allora $|S| = p^e$ e $S \subset G_{p^e} \Longrightarrow S = G_{p^e}$. Concludiamo col dire che $G_{p^e}, G_m \triangleleft G$ perché G è abeliano, $G_{p^e} \cap G_m = \{e\}$ per una questione di ordine e $G_{p^e} + G_m = G$ quindi $G \cong G_{p^e} \times G_m$ quindi per il passo induttivo $G \cong G_{p^e} \times G_{p_2^{e^2}} \times \cdots \times G_{p_r^{e^r}}$. □

2.4.1 Definizione : Sia G un gruppo abeliano finitamente generato. $T = \{x \in G | o(x) < \infty\}$ è l'insieme degli elementi di ordine finito ed è detto *insieme di torsione*.

2.4.1 osservazione : In un gruppo abeliano l'insieme di torsione T è un gruppo, inoltre G/T non ha elementi di torsione e vale che $G \cong T \times G/T$.

2.4.2 osservazione : non è detto che in generale l'insieme di torsione è un sottogruppo.

2.4.2 Teorema : Sia G un p-gruppo abeliano. Esisitono e sono unicamente determinati $r_1, \geq r_2 \geq \cdots \geq r_s$ tale che $G \cong \mathbb{Z}/_{p^{r_1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p^{r_s}\mathbb{Z}}$.

Dimostrazione :

Esistenza : $|G| = n$, facciamo una induzione su n :

Passo Base : $n = 1$ allora $G \cong \mathbb{Z}/_{p\mathbb{Z}}$.

Passo Induttivo : Sia $x_1 \in G$ tale che $ord(x_1) = p^{r_1}$ sia l'ordine massimo possibile in G, $< x >< G$. Per ipotesi induttiva $G/ < x_1 > \cong < x_2 > \times \cdots \times < x_s >$ dove $ord(x_i) = p^{r_i}$ con $r_2 \geq \cdots \geq r_s$. Consideriamo ora $\pi : G \longrightarrow G/ < x_1 >$, voglio vedere che esiste una copia isomorfa di $< x_2 > \times \cdots \times < x_s >$ in G; $\forall \bar{x} \in G/ < x_1 > \ \exists\, y \in \pi(\bar{x})^{-1}$ tale che $o(y) = o(\bar{x})$, infatti sia $p^r = o(\bar{x})$ e $\pi(y) = \bar{x}$ allora $\pi(p^r y) = p^r x = 0$ quindi $p^r y \in < x_1 > \implies \exists\, a \in \mathbb{Z}$ tale che $p^r y = a x_1$, di conseguenza $p^{r_1} y = 0$ perciò $0 = p^{r_1 - r}(p^r y) = p^{r_1 - r} a x_1$ ma $ord(x_1) = p^{r_1} \implies p^{r_1} | p^{r_1 - r} \implies p^r | a \implies a = p^r a_1$ da cui si ottiene che $p^r y = p^r a_1 x_1$, prendo ora $y - a_1 x_1$ si ha che $\pi(y - a_1 x_1) = \pi(y) = \bar{x}$ e $p^r(y - a_1 x_1) = p^r y - p^r a_1 x_1 = 0$ che è l'elemento cercato. Con questo risultato si sa che esistono $x_2, \cdots, x_s \in G$ tale che $ord(x_i) = ord(\bar{x_i}) = p^{r_i} \forall i = 2, \cdots, s$. Consideriamo quindi $H = < x_2, \cdots, x_s >$ si ha che $\pi|_H$ è bigettiva e che H è la copia isomorfa cercata, infatti la surgettività è ovvia, vadiamo che è anche iniettiva; $\pi(a_2 x_2 + \cdots + a_s x_s) = (a_2 \bar{x_2}, \cdots, a_s \bar{x_s}) = (\bar{0}, \cdots, \bar{0}) \iff p^{r_1} | a_i \forall i \implies p^{r_1} x_i = 0 \implies a_2 x_2 + \cdots + a_s x_s = 0$ quindi è iniettiva e perciò $H = < x_2, \cdots, x_s > \cong < \bar{x_2} > \times \cdots \times < \bar{x_s} >$. Adesso voglio dire che $G \cong < x_1> \times H$, basta verificare che $< x_1 > + H = G$ e $< x_1 > \cap H = \{e\}$; $< x_1 > + H = G \iff \forall g \in G, g = a x_1 + h, h \in H, a \in \mathbb{Z}$, so che $\bar{g} \in G/ < x_1 > = < x_2 > \times \cdots \times < x_s >$, detto $h = a_2 x_2 + \cdots + a_s x_s$ ho che $\pi(gh) = \bar{0} \implies g \in < x_1 >$ quindi $g = a x_1 + h$. Resta da dimostrare che $< x_1 > \cap H = \{e\}$; se $a_1 x_1 = a_2 x_2 + \cdots + a_s x_s$ allora $\pi(a_1 x_1) = \pi(a_2 x_2 + \cdots + a_s x_s) \implies \bar{0} = (a_2 \bar{x_2}, \cdots, a_s \bar{x_s}) \implies p^{r_1} | a_i \forall i \implies a_i x_i = 0 \forall i = 2, \cdots, s \implies a_1 x_1 = 0$. Possiamo concludere che $G \cong < x_1 > \times H \cong < x_1 > \times < x_2 > \times \cdots \times < x_s >$ e si verifica che gli ordini sono decrescenti.

Unicità : Per indizione su n, $|G| = p^n$:

Passo Base : Per $n = 1$ G è ciclico quindi $G \cong \mathbb{Z}/_{p\mathbb{Z}}$

Passo induttivo : $G \cong \mathbb{Z}/_{p^{r_1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_s^r\mathbb{Z}}$ con $r_1 \geq \cdots \geq r_s$ e $G \cong \mathbb{Z}/_{p^{k_1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_t^k\mathbb{Z}}$ con $k_1 \geq \cdots \geq k_t$; $G(p) = \{x \in G | o(x) = p\} \implies (\mathbb{Z}/_{p\mathbb{Z}})^s = (\mathbb{Z}/_{p\mathbb{Z}})^t \implies s = t$. Ora voglio vedere che anche gli esponenti sono uguali; Considero $pG \cong p\mathbb{Z}/_{p^{r_1}\mathbb{Z}} \times \cdots \times p\mathbb{Z}/_{p_s^r\mathbb{Z}} \cong \mathbb{Z}/_{p^{r_1 - 1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p^{r_s - 1}\mathbb{Z}}$ e $pG \cong p\mathbb{Z}/_{p^{k_1}\mathbb{Z}} \times \cdots \times p\mathbb{Z}/_{p_s^k\mathbb{Z}} \cong \mathbb{Z}/_{p^{k_1 - 1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p^{k_s - 1}\mathbb{Z}}$, per ipotesi induttivasu pG vale l'unicita quindi $r_i - 1 = k_i - 1 \implies r_i = k_1 \forall i$, quiesto conclude la dimostrazione.

□

2.4.3 Teorema : Sia G un gruppo abeliano finito. Allora G è prodotto diretto di gruppi ciclici: $G \cong \mathbb{Z}/_{n_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{n_s\mathbb{Z}}$, con $n_s | n_{s-1} | \cdots | n_1$ e tale scrittura è unica.

Dimostrazione :

Esistenza : $\forall p | \ |G|$ chiamiamo $G(p) = \{x \in G | p^k x = 0$ per qualche $k\}$ il p-sylow di G, per il Teo-

rema 2.4.1 $G \cong G(p_1) \times \cdots \times G(p_m)$ è questa decomposizione è unica a meno del'ordine dei fattori. Per il Teorema 2.4.2 esistono e sono unicamente determinati r_{ij} tale che $i = 1, \cdots, n$, $j = 1, \cdots, m$ e $r_{1j} \geq \cdots \geq r_{nj}$ $\forall j$, quindi $G \cong (\mathbb{Z}/_{p_1^{r_{11}}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_1^{r_{1n}}\mathbb{Z}}) \times \cdots \times (\mathbb{Z}/_{p_m^{r_{m1}}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_m^{r_{mn}}\mathbb{Z}})$ ora uso il teorema cinese del resto al contrario raggruppando i vari fattori in questo modo, dico che $n_s = p_1^{1s} \cdots p_m^{ms}$ ed in questo modo ottengo la tesi.

Unicità : se avessi due scritture diverse potrei ripercorrere gli isomorfismi al contrario e avrei due scritture diverse per almeno uno dei p-sylow.

□

2.4.1 osservazione : Le due scritture dei Teoremi 2.4.1 e 2.4.3 sono equivalenti.

2.4.1 esempio : $\mathbb{Z}/_{88\mathbb{Z}} \times \mathbb{Z}/_{44\mathbb{Z}} \cong (\mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{11\mathbb{Z}}) \times (\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{11\mathbb{Z}}) \cong (\mathbb{Z}/_{11\mathbb{Z}} \times \mathbb{Z}/_{11\mathbb{Z}}) \times (\mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}) \cong G(11) \times G(2)$.

2.4.2 esempio : $(\mathbb{Z}/_{9\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}) \times \mathbb{Z}/_{5\mathbb{Z}} \times (\mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \cong (\mathbb{Z}/_{9\mathbb{Z}} \times \mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}) \times (\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \cong \mathbb{Z}/_{360\mathbb{Z}} \times \mathbb{Z}/_{6\mathbb{Z}}$.

2.5 Esercizi

2.5.1 esercizio : (Classificazione dei gruppi di ordine 30)

soluzione : Studiamo i sylow; $n_5|6$, $n_5 \equiv 1(5) \Longrightarrow n_5 \in \{1, 6\}$ e $n_3|10$, $n_3 \equiv 1(3) \Longrightarrow n_3 \in \{1, 10\}$, se il P_5 non è normale allora ha 6 coniugati e siccome l'intersezione tra essi è banale ci sono $6\phi(6) = 24$ elementi di ordine 5, di conseguenza per una questione di dimensione il P_3 è normale ed quindi $P_5P_3 < G$ questo per la classificazione dei gruppi pq già fatta sappiamo che è isomorfo a $\mathbb{Z}/_{15\mathbb{Z}}$ perché $(5, \phi(2)) = 1$, inoltre questo gruppo è normale perché ha indice 2 quindi $G \cong \mathbb{Z}/_{15\mathbb{Z}} \rtimes_\tau \mathbb{Z}/_{2\mathbb{Z}}$. Se invece il P_5 è normale costruiamo comunque $P_5P_3 < G$ ed arriviamo alla stessa conclusione di prima quindi tutti i gruppi di ordine 30 sono distinti dai vari omomorfismi τ che definiscono il prodotto semidiretto e quindi studiamoli; $\tau : \mathbb{Z}/_{2\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{15\mathbb{Z}}) \cong \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$. Siano $x, y \in G$ tale che $o(x) = 15$ e $o(y) = 2$, $\tau(y) = \gamma_y$ dove $\gamma_y(x) = yxy^{-1} = x^a$ adesso se $\gamma_y^2 = Id$ in quanto l'immagine di un elemento di ordine 2 deve avere al più ordine 2, allora $x^{a^2} = x \Longrightarrow a^2 \equiv 1\,(15) \Longrightarrow a \equiv \pm 1, \pm 4\,(15)$ indicano i vari omomorfismi possibili. Voglio vedere a seconda della scelta di a che gruppo identificano; so che per $a = 1$ si ha $\mathbb{Z}/_{30\mathbb{Z}}$ e per $a = -1$ si ha D_{15}, le altre due a corrispondono agli elementi $(1, -1)$ e $(-1, 1)$ rispetto a $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$, le coppie indicano che gli omomorfismi agiscono banalmente su una componente del prodotto diretto quindi si hanno $D_4 \times \mathbb{Z}/_{3\mathbb{Z}}$ e $D_3 \times \mathbb{Z}/_{5\mathbb{Z}}$.

2.5.2 esercizio : Verificale le varie proposizioni :

1) $H \triangleleft K$ e $K \triangleleft G \Longrightarrow H \triangleleft G$.

2) $H < K < G$ H, K caratteristici $\Longrightarrow H < G$ caratteristico.

3) $H < K \triangleleft G$ H caratteristico $\Longrightarrow H \triangleleft G$.

4) $H \triangleleft K < G$ K caratteristico $\Longrightarrow H \triangleleft G$.

soluzione :

1) É falso. Sia $G = D_4$ e prendiamo $K =< \sigma, \sigma\rho^2 >$ e $H =< \sigma >$, $H \triangleleft K$ e $K \triangleleft G$ ma $H \not\triangleleft G$.

2) É vera. $H < G$ è caratteristico $\Longleftrightarrow \forall f \in Aut(G)\ f(H) = H$; so che K è caratteristico in G, quindi $f(K) = K$, cioè $f|_k \in Aut(K)$ ma H è inariante per $Aut(K) \Longrightarrow f|_k(H) = f(H) = H$.

3) É vera. Sia $\gamma_g \in Int(G)$, so che $\gamma_g(k) \in Aut(K)$, cioè $K \triangleleft G$, H è invariante per automorfismi di K quindi in particolare $\gamma_g|_K(H) = \gamma_g(H) = H$.

4) É falso. Prendo $G = A_4$ e come sottogruppo caratteristico prendo il sottogruppo di klein $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ e $H = \{e, (1,2)(3,4)\} \triangleleft V$ ma non in G.

2.5.3 esercizio : Sia G un gruppo con $|G| = 2d$ con d dispari. Allora esiste $H \triangleleft G$ con $|H| = d$, in particolare G non è semplice.

soluzione : Per il teorema di Cayley esiste $\phi : G \longrightarrow S(G) \cong S_2d$ omomorfismo con $\phi(g) = \gamma_g$ dove $\gamma_g(x) = gx$; $\forall x \in G$, $orb(x) = (x, gx, g^2x, \cdots, g^{m-1}x)$ con $ord(g) = m$. Allora, se pensiamo γ_g in S_2d, è prodotto di $\frac{2d}{m}$ cicli di lunghezza m. Adesso sia $H = (G \cong \phi(G)) \cap A_{2d} \Longrightarrow |H| \in \{d, 2d\}$. Per cauchy esiste $y \in G$ tale che $o(y) = 2$, γ_y è prodotto di d cicli di lunghezza 2, ma d dispari quindi $\gamma_y \notin A_{2d} \Longrightarrow |H| = d$.

2.5.4 esercizio : Sia G un gruppo semplice finito. Se esiste $H < G$, $[G : H] = n \Longrightarrow G \hookrightarrow A_n$.

soluzione : Sia $X = \{x_iH\}_{i=1}^{n}$ l'insieme delle classi laterali e sia $\psi : G \longrightarrow S(X) \cong S_n$, con $\phi(g) = \gamma_g$ dove $\gamma_g(xH) = gxH$, l'azione di G su X. $N = Ker(\phi) = \{g | gx_iH = x_iH\ \forall i\} = \{g \in G | gx_i \in x_iH\ \forall i\} = \{g \in G | g \in x_iHx_i^{-1}\ \forall i\} = \bigcap_{i=1}^{n} x_iHx_i^{-1}$. Considerando l'azione abbiamo che $[G : G \cap A_n] \in \{1, 2\}$ ma G è semplice e se fosse 2 l'indice avrebbe un sottogruppo normale quindi vale 1 e perciò G si immergie in A_n.

2.5.5 esercizio : Un gruppo di ordine 112 non è semplice.

soluzione : Studiamo il $P2$; $|P_2| = 16$, $n_2 \in \{1, 7\}$, se fosse 1 il P_2 sarebbe normale è la tesi e verificata, consideriamo quindi il caso che abbai 7 coniugati. Prendiamo il normalizzatore $N_G(P_2)$, questo ha indice 7 in quanto il $P_2 < N_G(P_2)$, quindi ha cardinalità 16 o 112, ma 112 non può essere se no il P_2 è normale cosa che abbiamo escluso. Per l'esercizio 2.5.4, G si immerge in A_7 ma $112 \nmid \frac{7!}{2}$, assurdo, quindi $n_2 = 1$ e G non è semplice.

2.5.6 esercizio : un gruppo di ordine 144 non è semplice.

soluzione : Studiamo il P_3; $|P_3| = 9$, $n_3 \in \{1, 4, 16\}$. Se $n_3 = 1$ allora il P_3 è normale e G non è semplice, se $n_3 = 4$ allora $N_G(P_3)$ ha indice 4 (usando il teorema delle classi sull'azione di coniugio di G sui 3-sylow) quindi G si immergie in A_4 ma $144 \nmid 4!$, assurdo per una questione d'ordine, resta il caso di $n_4 = 16$. Consideriamo quindi l'ultimo caso, se per ogni coppia P, P' di 3-sylow vale che $P \cap P' = \{e\}$ allora ci sono 128 elementi di ordine divisibile per 3, quindi il P_2 è normale e G non è semplice, allora supponiamo che esistono P, P' 3-sylow tale che $P \cap P' = H$, $|H| = 3$; siccome P, P' sono abeliani $PP' < N_G(H)$ e sono anche suoi 3-sylow (quindi anche in $N_G(H)$ vale che $n_3 \in \{1, 4, 16\}$), quindi $|N_G(H)| > 18 \Longrightarrow |N_G(H)| \in \{36, 72, 144\}$, consideriamo l'azione di G su le classi laterali di $N_G(H)$, nei casi in cui la cardinalità sia 36 o 72 $N_G(H)$ ha indice 4 o 2 quindi l'azione ha nucleo non banale ed è normale in G, se vale 144 allora H è normale in G, in ogni caso si trova un sottogruppo normale quindi G non è semplice.

2.5.7 esercizio : (Da vedere) p-sylow di $GL(n, \mathbb{F}_p)$.

soluzione : Intanto sappiamo che $|GL(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ perché abbiamo $(p^n - 1)$ scelte per la prima colonna della matrice, ovvero tutte meno quella nulla, poi $(p^n - p)$ per la seconda, ovvero tutte meno i multipli della prima, e così via. Esplicitando i fattori p si ha che $|GL(n, \mathbb{F}_p)| = pp^2 \cdots p^{n-1}a = p^{\frac{n(n-1)}{2}}a$ con $(a, p) = 1$, quindi abbiamo che il p-sylow P ha cardinalità $p^{\frac{n(n-1)}{2}}$. Sia $A \in P$, allora $A^{p^{\frac{n(n-1)}{2}}} = I$ quindi $\mu_A(x) | x^{p^{\frac{n(n-1)}{2}}} - 1 = (x-1)^{p^{\frac{n(n-1)}{2}}}$, dove l'ultima uguaglianza deriva dal fatto che siamo in $\mathbb{F}_p$, quindi $det(A) = 1$. $n_p \in \{\sum_{i=0}^{k} p^i\}_{k=0}^{n-1}$.

2.5.8 esercizio : Sia G un gruppo non abeliano tale che $|G| = p^3$. Allora $|Z(G)| = p$ e $G' = [G : G] = Z(G)$, e calcolare il numero di classi di coniugio.

soluzione : Intanto G è un p-gruppo quindi ha centro non banale e le possibilità per la sua cardinalità sono p, p^2, p^3, escludo p^3 perché G non è abeliano inoltre se fosse p^2 allora $|Int(G)| = \frac{|G|}{|Z(G)|} = p$ se $Int(G)$ è ciclico allora G abeliano e non va bene per le ipotesi quindi l'unica possibilità e che sia p. Adesso vediamo che $|G/Z(G)| = p^2$ quindi il quoziente è abeliano

e perciò $G' \subset Z(G) \Longrightarrow G' = \{e\}$ oppure $G' = Z(G)$ ma la prima si esclude perché implicherebbe che G sia abeliano quindi $G' = Z(G)$. In conclusione calcoliamo in numero di classi di coniugio, $p^3 = |G| = |Z(G) + \sum_{x \in R} \frac{|G|}{|Z(x)|}$, dove R è il numero di classi di coniugio non banali; osserviamo che se $x \notin Z(G)$ allora $|Z(x)| = p^2$ perchè $Z(G) \subset Z(x) \subset G$, da cui si ottiene che $p^3 = p + \sum_{x \in R} \frac{p^3}{p^3} = p + |R|p$ quindi il numero delle classi è $p + |R| = p^2 + p - 1$.

2.5.9 esercizio : A_n è generato da i 3-cicli.

soluzione : Ogni $\sigma \in S_n$ lo posso scrivere come composizione di trasposizioni, in particolare in A_n in un numero pari di trasposizioni. Osserviamo che composizione di due trasposizioni non disgiunte formano un 3-ciclo infatti $(a, b)(a, c) = (a, c, b)$ con $a \neq b \neq c$, invece composizione di due trasposizioni disgiunte la posso scrivere come composizioni di due 3-cicli, infatti $(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, c, b)(c, d, a)$, con $a \neq b \neq c \neq d$, quindi in conclusione prendo $\sigma \in A_n$ la scrivo come composizione di trasposizioni e a due a due le accoppio e come detto precedentemente o esce un 3-ciclo o un prodotto di due 3-cicli.

2.5.1 osservazione : Se $H \triangleleft S_n$ e $\tau \in H$, dove τ è un 3-ciclo, allora $A_n \subset H$.

2.5.10 esercizio : $(1, 2), (2, 3), (3, 4), \cdots, (n - 1, n)$ generano S_n

soluzione : Per induzione su n :

Passo base : $S_2 =< (1, 2) >$.

Passo induttivo : Per ipotesi induttiva $(1, 2), \cdots, (n - 2, n - 1)$ generano S_{n-1} che è sottogruppo di S_n e queste quindi generano tutte le trasposizioni (i, j) con $i < j < n$, ci mancano quelle della forma (i, n). Se $i = n - 1$ allora (i, n) sta nella lista, se $i < n - 1$ ho che $(i, n) = (n - 1, n)(1, n - 1)(n - 1, n)$ quindi posso generare tutte le trasposizioni e siccomme tutte le trasposizioni generano S_n la lista $(1, 2), \cdots, (n - 1, n)$ genera S_n.

2.5.2 osservazione : S_n è generato da un n-ciclo ed un particolare 2-ciclo, per esempio è generato da $\sigma = (1, 2, \cdots, n)$ e $\tau = (1, 2)$ infatti $\sigma^k \tau \sigma^{-k} = (k + 1, k + 2)$ che restituisce la lista dell'esercizio precedente e quindi genera tutto S_n, invece $\sigma = (1, 2, \cdots, n)$ e $\tau = (1, 3)$ non generano S_n. Per ogni p primo S_p è generato da un p-ciclo e da un qualsiasi 2-ciclo.

2.5.11 esercizio : Risolvere l'equazione $\sigma^4 = (1, 2, 3)(4, 5, 6) = \tau$ al variare di $\sigma \in S_10$.

soluzione : Osserviamo che $\sigma^{12} = e \Longrightarrow o(\sigma)|12$ e $3|o(\sigma)$ quindi $o(\sigma) = \{3, 6, 12\}$. Se $o(\sigma) = 3 \Longrightarrow \sigma = \tau$ ed è una soluzione. Se $o(\sigma) = 6$ allora σ può essere un 6-ciclo, $6 \times$ 3-ciclo, $6 \times$ 2-ciclo, $6 \times 2 \times$ 2-ciclo, $3 \times$ 2-ciclo, $3 \times 3 \times$ 2-ciclo, $3 \times 2 \times$ 2-ciclo, $3 \times 3 \times 2 \times$ 2-ciclo,

$3 \times 2 \times 2 \times 2$-ciclo, dobbiamo vedere se la quarta potenza di questi dia un 3×3-ciclo, rispettivamente la quarta potenza è un 3×3-ciclo, $3 \times 3 \times 3$-ciclo, 3×3-ciclo, 3×3-ciclo, 3-ciclo, 3×3-ciclo, 3-ciclo, 3×3-ciclo, 3-ciclo, quindi vanno bene un 6-ciclo, 6×2-ciclo, $6 \times 2 \times 2$-ciclo, $3 \times 3 \times 2$-ciclo, $3 \times 3 \times 2 \times 2$-ciclo, vediamo quante soluzioni ci sono di questa forma. I $3 \times 3 \times 2$-ciclo, $3 \times 3 \times 2 \times 2$-ciclo sono della forma $\tau \circ \gamma$ dove γ e un 2-ciclo o 2×2-ciclo di $S_{\{7,8,9,10\}}$ quindi ci sono $\binom{4}{2} + \frac{1}{2}\binom{4}{2}\binom{2}{2}$ permutazioni di questa forma; adesso vediamo il 6-ciclo, se abbiamo $\phi = (a, b, c, d, e, f)$ allora $\phi^4 = (a, e, c)(b, f, d) = (1, 2, 3)(4, 5, 6)$ possiamo supporre che $a = 1$ di conseguenza $e = 2$ e $c = 3$, adesso vedo che ci sono 3 modi di combinare (b, f, d) con $(4, 5, 6)$, (potevo anche vederlo dal 6-ciclo, ho 6 possibilità per a e si determinano anche e e c, poi ho 3 possibilità per b e si determinano anche f e d, poi nel 6-ciclo se traslo le sue componenti non cambia la permutazione quindi ci sono $\frac{6\times3}{6} = 3$ soluzioni), quindi ci sono 3 6-cicli che assolvono alla nostra richiesta, in tutto quindi ci sono $3(1 + \binom{4}{2} + \frac{1}{2}\binom{4}{2}\binom{2}{2})$ che sono date dal 6-ciclo composto l'identita, 2-ciclo e 2×2-ciclo di $S_{\{7,8,9,10\}}$. Se σ ha ordine 12 allora le possibilità sono 6×4-ciclo, 3×4-ciclo, $3 \times 4 \times 2$-ciclo, $3 \times 3 \times 4$-ciclo, la quarta potenza è rispettivamente un 3×3-ciclo, 3-ciclo, 3-ciclo, 3×3-ciclo, quindi vanno bene 6×4-ciclo e $3 \times 3 \times 4$-ciclo che sono in tutto $3(3!) + 3!$ ovvero i 6-cicli composti i 4-cicli di $S_{\{7,8,9,10\}}$ e τ composto i 4-cicli di $S_{\{7,8,9,10\}}$. Complessivamente di sono $4(\binom{4}{2} + \frac{1}{2}\binom{4}{2}\binom{2}{2} + 3! + 1) = 64$ soluzioni.

2.5.12 esercizio : Risolvere l'equazione $\sigma^4 = (1, 2, 3, 4)$ in S_{58}.

soluzione : per l'analisi fatta nell'esercizio precedente non si può ottenere un 4-ciclo da una 4 potenza di un qualsiasi ciclo, quindi non ha soluzione.

2.5.13 esercizio : Calcolare $|Aut(\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}})|$.

soluzione : Siano e_1, e_2, e_3 una base standard per $G = \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}$. Intanto G è abeliano e $G_p = \{g \in G | g$ ha ordine una potenza di $p\}$ è caratteristico. Definite le possibili immagini per i generatori abbiamo definito anche tutto l'automorfismo, adesso G ha 24 elementi di ordine 4 quindi e_2 ha 24 possibili immagini, e_3 deve andare in un elemento di ordine 4 diverso da quello individuato da e_2 e in modo che il gruppo $< e_2, e_3 >$ abbia ordine 16, ovvero imporre che $2\gamma(e_3) \neq 0$ (dice che non ha ordine 2) e $2\gamma(e_3) \neq 2\gamma(e_2)$ (affinché non generi un gruppo di ordine 8 con e_2). Se $\gamma(e_3) = x$ allora se $2x = 2\gamma(e_2) \iff x \in < \gamma(e_2), el.\ di\ ord.\ 2 >$ quindi $x = \gamma(e_2) + y$ con $o(y) = 2$ (infatti $2y = 2x - 2\gamma(e_2) = 0$), di conseguenza dire che $2x \neq 2\gamma(e_2)$ significa $x \neq \gamma(e_2) + y$ in questo modo escludo 8 casi ed e_3 ha così 16 possibili immagini. Infine e_1 può andare solo negli elementi di ordine 2 di G tranne negli elementi di ordine 2 di $< e_2, e_3 >$, perciò ha 4 possibili immagini. Quindi $|Aut(\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}})| = 24 \times 16 \times 4$.

2.5.14 esercizio : Calcolare $S'_n = [S_n : S_n]$, il derivato di S_n.

soluzione : S'_n non può essere $\{e\}$ perché S_n non è abeliano. S'_n è caratteristico quindi normale,

noto che per $n \geq 3$, $(1,2,3) = (1,2)(1,3)(1,2)(1,2) = [(1,2),(1,3)] \in S_n'$, quindi S_n' contiene un 3-ciclo e per normalità li contiene tutti quindi $A_n \subset S_n'$, osserviamo che $S_n/A_n \cong \mathbb{Z}/_{2\mathbb{Z}}$, quindi $S_n' \subset A_n$ per ciò $S_n' = A_n$; per $n = 1, 2$, S_n è abeliano quindi $S_n' = \{e\}$.

2.5.15 esercizio : Quale è il più piccolo n tale che $\mathbb{Z}/_{6\mathbb{Z}}$ si immerge in S_n.

soluzione : è sufficiente vedere quando sia possibile trovare un elemento di ordine 6. Per $n = 5$ si ha $(1,2)(3,4,5)$ che ha ordine 6.

2.5.16 esercizio : Quale è il più piccolo n tale che D_6 si immerge in S_n.

soluzione : É sufficiente trovare un elemento di ordine 6 ρ ed uno di ordine 2 σ tale che $\sigma\rho\sigma = \rho^{-1}$. portiamoci in S_5, sappiamo che ci troviamo un elemento di ordine 6 ed è il più piccolo dove lo si può trovare $\rho = (1,2)(3,4,5)$, quindi σ lo possiamo trovare in $N_{S_5}((1,2)(3,4,5)/Z((1,2)(3,4,5)$, (questo in generale no è sufficiente ma in questo caso lo è), prendiamo per esempio $\sigma = (5,4)$. In conclusione $< (1,2)(3,4,5),(5,5) >< S_5$ e $< (1,2)(3,4,5),(5,5) > \cong D_6$, quindi 5 è il più piccolo n dove si immerge.

2.5.17 esercizio : (Da vedere) Il più piccolo n tale che Q_8 si immerge in S_n e 8.

soluzione : Intanto per il teorema di Cayley si ha che Q_8 si immergie in S_8, bisogna solo far vedere che è il più piccolo dove si immerge. Q_8 ha ordine 8 quindi un S_n deve poterlo contenere perciò il minimo probabile è S_4, ma se lo fosse sarebbe un suo 2-sylow ma come sappiamo il 2-sylow di S_4 è D_4 come per S_5.

2.5.18 esercizio : (Da vedere) (Classificazione dei gruppi di ordine p^2q, con p, q primi)

soluzione : Se $p < q$ si ha che $n_q \in \{1, p^2\}$, quindi il q-sylow è normale o ha 16 coniugati. Nel primo caso si ha che $G \cong Q \rtimes_\gamma P$, dove Q è il q-sylow e P è il p-sylow, nel secondo caso, siccome i q-sylow hanno intersezione banale, ci sono $(q-1)p^2$ elementi di ordine q e quindi rimane un solo posto per il p-sylow perciò il p-sylow è normale e si ha $G \cong P \rtimes_\tau Q$. Se $p > q$ il p-sylow è normale perché ha indice il più piccolo primo che divide l'ordine del gruppo quindi si ha $G \cong P \rtimes_{\tau_1} Q$. Studiamo adesso i vari omomorfismi; $\gamma : P \longrightarrow Aut(Q)$, $P \cong \mathbb{Z}/_{p^2\mathbb{Z}}$ o $P \cong \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{p\mathbb{Z}}$ e $Q \cong \mathbb{Z}/_{q\mathbb{Z}}$. Quindi abbiamo $\gamma_1 : \mathbb{Z}/_{p^2\mathbb{Z}} \longrightarrow \mathbb{Z}/_{q-1\mathbb{Z}}$, se $(p, q-1) = 1$ allora $G \cong \mathbb{Z}/_{p^2q\mathbb{Z}}$, se $q - 1 = p^2$...

2.5.19 esercizi : $Aut(D_4)$

soluzione : Sappiamo che la cardinalità di questo gruppo è $4\phi(4) = 8$. Consideriamo $\rho \in Aut(D_4)$ dove $\rho(s) = sr$, $\rho(r) = r$ e $\sigma \in Aut(D_4)$ dove $\sigma(s) = s$, $\sigma(r) = r^3$. Si osserva

che $o(\rho) = 4$ quindi $< \rho >$ è normale, inoltre $o(\sigma) = 2$ e $\sigma \not\in < \rho >$, da ciò si dimostra che $< \rho >< \sigma >= Aut(D_4)$ e $< \rho > \cap < \sigma >$ quindi $Aut(D_4) \cong < \rho > \rtimes_\tau < \sigma > \cong \mathbb{Z}/_{4\mathbb{Z}} \rtimes_{\bar{\tau}} \mathbb{Z}/_{2\mathbb{Z}}$. Ora $\tau : \mathbb{Z}/_{2\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{4\mathbb{Z}}) \cong \mathbb{Z}/_{2\mathbb{Z}}$, ci sono due omomorfismi, uno banale ed uno non banale, vediamo quindi come agisce σ su ρ; si vede che $\sigma\rho\sigma = \rho^{-1}$ quindi $Aut(D_4) \cong D_4$.

2.5.20 esercizio : (Da vedere) Sia $G = D_{100}$. cercare i sottogruppi di ordine 4 e 50.

soluzione : Cerchiamo sottogruppi isomorfi a $\mathbb{Z}/_{4\mathbb{Z}}$: abbiamo solo $< r^{25} >$, dove r è la rotazione, che è normale e caratteristico. Il quoziente $D_{100}/_{<r^{25}>} \cong D_{25}$ che ha ordine 50. Cerchiamo sottogruppi isomorfi a $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$: li cerco nel centralizzatore perché $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ è abeliano. Sia s la riflessione, $|Z(sr^k)| = \frac{200}{Cl(sr^k)} = 4$ perché le classi di coniugio delle simmetrie si dividono in due, $Cl(s) = \{sr^k | k = 0, \cdots, 49\}$ e $Cl(sr) = \{sr^{k+1} | k = 0, \cdots, 49\}$. Nel centralizzatore di un elemento ci sono sempre l'elemento stesso, il centro e se l'elemento è potenza di un altro, allora ci sta pure quest'altro elemento. Quindi $Z(sr^k) =< sr^k, r^{50} >= \{Id, sr^k, r^{50}, sr^{k+50}\}$, in questa maniera ottengo 50 sottogruppi non normali di ordine 4 isomorfi a $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$. Cerco sottogruppi di indice 4 : $H < D_{100}$ con $[D_{100} : H]$. I sottogruppi di ordine 50 contengono i 5-sylow di D_{100}. Il 5-sylow di D_{100} è il gruppo $< r^4 > \subset H$ allora costruisco $\gamma : D_{100} \longrightarrow D_{100}/_{<r^4>} \cong D_4$ e per il teorema di corrispondenza basta trovare gli elementi di ordine 2 in D_4; sono $< r^2 >$ che è normale, $< s >$, $< sr >$, $< sr^2 >$, sr^3. Tornando indietro con γ^{-1} ottengo i sottogruppi cercati ($\gamma G \longrightarrow G/N \Longrightarrow \gamma^{-1}(H) = \{HN, H\}$, dove H è un sottogruppo...), $< r^2, r^4 >$, $< s, r^4 >$, $< sr, r^4 >$, $< sr^2, r^4 >$, sr^3, r^4.

2.5.21 esercizio : (Da vedere) (Classificazione dei gruppi di ordine 105)

soluzione : Consideriamo il 5-sylow, $n_5 \in \{1, 21\}$. Supponiamo che $n_5 = 21$ allora siccome l'intersezione tra i 5-sylow è banale ci sono 84 elementi di ordine 5. Il 7-sylow deve essere normale perché $n_7 \in \{1, 15\}$ e siccome l'intersezione è banale tra i 7-sylow se fossero 15 ci sarebbero 90 elementi di ordine 7 ma non c'è abbastanza posto perché sono rimasti liberi solo 21 elementi. Possiamo quindi costruire $P_5P_7 < G$, questo è un sottogruppo ed è isomorfo a $\mathbb{Z}/_{7\mathbb{Z}} \rtimes_\gamma \mathbb{Z}/_{5\mathbb{Z}}$, inoltre è normale perchè ha indice il più piccolo primo che divide l'ordine del gruppo quindi posso a sua volta costruire $P_3(P_5P_7) \cong (\mathbb{Z}/_{7\mathbb{Z}} \rtimes_\gamma \mathbb{Z}/_{5\mathbb{Z}}) \rtimes_\tau \mathbb{Z}/_{3\mathbb{Z}} \cong G$. Siccome $(\phi(7), 5) = 1$ allora $\gamma = Id$ perciò $G \cong (\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}) \rtimes_\tau \mathbb{Z}/_{3\mathbb{Z}}$. Adesso $\tau : \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}) \cong (\mathbb{Z}/_{6\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}})$ siccome $(3, 4) = 1$ allora il 3-sylow agisce solo sul 7-sylow quindi $G \cong (\mathbb{Z}/_{7\mathbb{Z}} \rtimes_{\tau_1} \mathbb{Z}/_{3\mathbb{Z}}) \times \mathbb{Z}/_{5\mathbb{Z}}$. Studiamo quindi $\tau_1 : \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{7\mathbb{Z}}) \cong \mathbb{Z}/_{6\mathbb{Z}} \cong (\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}})$ quindi ci possiamo ancora ridurre a studiare $\bar{\tau_1} : \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow \mathbb{Z}/_{3\mathbb{Z}}$. Ho un omomorfismo banale che da $\mathbb{Z}/_{105\mathbb{Z}}$ e due non banali appartenenti ad $Aut(\mathbb{Z}/_{3\mathbb{Z}})$. Dico che i due omomorfismi non banali generano gruppi isomorfi; infatti considero $\alpha \in Aut(\mathbb{Z}/_{3\mathbb{Z}})$ tale che $\alpha([1]_3) = [2]_3$ e considero $\psi : \mathbb{Z}/_{7\mathbb{Z}} \rtimes_{\tau_1^1} \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow \mathbb{Z}/_{7\mathbb{Z}} \rtimes_{\tau_1^2} \mathbb{Z}/_{3\mathbb{Z}}$ dove $\gamma_1^1([1]_3) = 2$, $\gamma_1^2([1]_3) = 4$ e osservando che $\alpha \circ \gamma_1^1(x) = \gamma_1^2(x) \circ \alpha$. Dico che $\psi((a, b)) = (\alpha(a), b)$ è questo definisce un isomorfismo infatti $\psi(a, b) = (\alpha(a), b) = (0, 0) \Longrightarrow (a, b) = (0, 0)$ inoltre $\forall (a, b) \in \mathbb{Z}/_{7\mathbb{Z}} \rtimes_{\tau_1^2} \mathbb{Z}/_{3\mathbb{Z}}$, $\psi((\alpha(a)^{-1}, b)) = (a, b)$. Quindi è bigettiva, abbiamo usato solo

che α è un automorfismo. Adesso $\psi((a,b)(c,d)) = \psi((a\gamma_1^1(b)(c), bd)) = (\alpha(a\gamma_1^1(b)(c)), bd) = (\alpha(a)\alpha(\gamma_1^1(b)(c)), bd) = (\alpha(a)\gamma_1^2(b)(\alpha(c)), bd) = (\alpha(a), b)(\alpha(c), d) = \psi((a,b))\psi((c,d))$. In conclusione abbiamo trovato un gruppo abeliano ed uno non abeliano. Se il 5-sylow è normale con alcune considerazioni di prima otteniamo che $G \cong (\mathbb{Z}/_{5\mathbb{Z}} \rtimes_\gamma \mathbb{Z}/_{7\mathbb{Z}}) \rtimes_\tau \mathbb{Z}/_{3\mathbb{Z}}$. con gli stessi ragionamenti di prima otteniamo che $G \cong \mathbb{Z}/_{5\mathbb{Z}} \times (\mathbb{Z}/_{7\mathbb{Z}} \rtimes_{\tau_1} \mathbb{Z}/_{3\mathbb{Z}})$ uguale al caso precedente. Quindi esistono solo due gruppi di ordine 105.

2.5.22 esercizio : Trovare un gruppo G tale che $|G| = 255$ e $H < G$ tale che $|H| = 85$ ciclico.

soluzione : Intanto dico che H è un gruppo ciclico. il P_{17} è normale perché ha indice il più piccolo primo che divide l'ordine del gruppo, quindi $G \cong P_{17}P_5$. Inoltre siccome $(5, \phi(17)) = 1$ si ha che $H \cong \mathbb{Z}/_{85\mathbb{Z}}$. Adesso osserviamo che $H \triangleleft G$ perché ha indice $[G : H] = 3$ il più piccolo primo che divide l'ordine del gruppo (un altro modo è supponendo che non sia normale. Prendiamo quindi un suo coniugato L, allora $|HL| = \frac{|H||L|}{|H\cap L|} = \frac{85^2}{|H\cap L|} \leq 255$. Quindi per forza $|H \cap L| = 85$ ed è quindi unico e perciò normale) quindi $G \cong \mathbb{Z}/_{85\mathbb{Z}} \rtimes_\tau \mathbb{Z}/_{3\mathbb{Z}}$. Ora $\tau : \mathbb{Z}/_{3\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{85\mathbb{Z}}) \cong (\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{16\mathbb{Z}})$ ma per questioni di ordine $\tau([1]_3) = Id_{\mathbb{Z}/_{85\mathbb{Z}}}$ per ciò $G \cong \mathbb{Z}/_{255\mathbb{Z}}$.

2.5.23 esercizio : Calcolare il centralizzatore e normalizzatore di $\sigma = (1,2,3)(4,5,6)$ in S_8

soluzione : Usando il teorema delle classi sappiamo che $|Z_{S_8}(\sigma)| = \frac{8!}{\frac{1}{2}\binom{8}{5}2\binom{5}{2}2} = 3!3! = 36$. Inoltre $H =< (1,2,3), (4,5,6), (7,8) >< Z_{S_8}(\sigma)$ che ha cardinalità 18 ed è abeliano e normale perché ha indice 2. Resta una permutazione che coniuga i due cicli di σ che $(1,4)(2,5)(3,6)$. In conclusione $Z_{S_8}(\sigma) =< (1,2,3), (4,5,6), (7,8) > \rtimes_\tau (1,4)(2,5)(3,6) \cong (\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \rtimes_\tau \mathbb{Z}/_{2\mathbb{Z}}$. Il prodotto diretto è non banale e $\tau([1]_2)((a,b,c)) = (b,a,c)$. Ci resta il normalizzatore. Consideriamo $\gamma : N_{S_8}(\sigma) \longrightarrow Aut(< \sigma >)$ tale che $\gamma(n) = \gamma_n$ e $\gamma_n(x) = nxn^{-1}$, quindi $Ker(\gamma) = Z_{S_8}(\sigma)$ ed è anche surgettiva. In conclusione $N_{S_8}(\sigma) \cong Z_{S_8}(\sigma) \rtimes_{\tau_1} Aut(< \sigma >)$.

2.5.24 esercizio : (Da vedere) Sia G un p-gruppo e $H < G$ sottogruppo proprio. Allora $H < N_G(H)$ (sottogruppo stretto, mai uguale).

soluzione : So che $Z(G)$ non è banale perchè G è un p-gruppo. Se $Z(G) \not< H$ allora $H < N_G(H)$ perchè $Z(G) \subset N_G(H)$. Se $Z(G) < H$, allora lo dimostro per induzione. Se $|G| = p$ e $|G| = p^2$ si ha che i gruppi abeliano ed ogni sottogruppo proprio è normale quindi il loro normalizzatore è tutto G che è maggiore del sottogruppo stesso. Ora sia $|G| = p^n$ ed un qualsiasi $H < G$, considero il diagramma :

$$\begin{array}{ccc} G & \xrightarrow{\quad\gamma\quad} & H \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ \bar{G} = G/_{Z(G)} & \xrightarrow{\bar{\gamma}} & H/_{Z(G)} = \bar{H} \end{array}$$

Per ipotesi induttiva $\bar{H} < N_{\bar{G}}(\bar{H})$. Quindi $H = \pi^{-1}(\bar{H}) < \pi^{-1}(N_{\bar{G}}(\bar{H})) = N_G(H)$ infatti sia $x \in \pi^{-1}(N_{\bar{G}}(\bar{H}))$ e $Z = Z(G)$, sappiamo che $\bar{x}\bar{H}\bar{x}^{-1} = \bar{H} \Longrightarrow xZHZx^{-1}Z = HZ \longrightarrow x(ZHZ)x^{-1} = xHx^{-1} = H$ quindi $x \in N_G(H)$ ma $x \notin H$.

2.5.25 esercizio : Quale è il minimo n tale che D_6 si immerge in A_n.

soluzione : Devo trovare una permutazione di ordine 6 pari ed una di ordine 2 pari che coniuga la rotazione nella sua invarsa. La più piccola la trovo in A_7, infatti prendo $\rho = (1,2)(3,4)(5,6,7)$ questa sarà la rotazione di ordine 6 pari. trovo la simmetria σ in $N_{S_7}(\rho) \cap A_7$, e prendo $\sigma = (1,2)(6,7)$. In conclusione noto che una permutazione di ordine 6 non la trovo in S_n con $n \leq 4$, in S_5 e S_6 le trovo ma sono della forma 2×3-ciclo o 6-ciclo ma queste sono dispari.

2.5.26 esercizio : Sia G un gruppo di ordine 60 e semplice. Allora $G \cong A_5$.

soluzione : Osserviamo che $n_5 \in \{1, 6\}$, siccome G è semplice abbiamo che $n_5 = 6$. Dall'azione di coniugio di G su l'insieme dei 5-sylow abbiamo che $[G : N(P_5)] = 6$ e per la semplicità di G si ha che $G \hookrightarrow A_6$, ed inoltre G ha indice 6 in A_6. Consideriamo quindi $\gamma : A_6 \longrightarrow S(X)$ l'azione di A_6 sull'insieme delle classi laterali di G. A_n si immerge in $S(X)$ perché semplice, quindi induce un'azione di G su X, $\gamma|_G : G \longrightarrow S(X)$. G agisce banalmente su X, per questo l'orbita di $G \in X$ è $\{G\}$, quindi G agisce anche su $X - \{G\}$, è posso costruire $G \hookrightarrow S(X - \{G\}) \cong S_5$. Quindi G è isomorfo ad un sottogruppo di S_5 di indice 2 che è A_5.

2.5.27 esercizio : Sia $G = Q_8 \times D_4$, trovare $Z(G)$.

soluzione : $Z(G) \cong Z(Q_8) \times Z(D_4) \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$.

2.6 Ancora Esercizi

2.6.1 esercizio : $Aut(Q_8 \times D_4)$

soluzione : Sia $\gamma \in Aut(Q_8 \times D_4)$ esprimo γ con una matrice $\left(\begin{smallmatrix} \alpha & \beta \\ \sigma & \delta \end{smallmatrix}\right)$ con $\gamma((g,h)) = (\alpha(g)\sigma(h), \beta(g)\delta(h))$ dove $\alpha : Q_8 \longrightarrow Q_8,\ \beta : Q_8 \longrightarrow D_4,\ \sigma : D_4 \longrightarrow Q_8,\ \delta : D_4 \longrightarrow D_4$, sono omomorfismi; vogliamo vedere per quali di questi omomorfismi la matrice così indicata identifichi un automorfismo

di $Q_8 \times D_4$.

Studiamo $\beta : Q_8 \longrightarrow D_4$: Osserviamo intanto che non esiste nessun omomorfismo surgettivo in quanto i due gruppi hanno la stessa cardinalità e se esistesse sarebbe un isomorfismo, assurdo; Q_8 ha 3 sottogruppi di indice 2, $< i >, < j >, < k >$, che sono il kernel di 3 omomorfismi surgettivi da Q_8 in $\mathbb{Z}/_{2\mathbb{Z}}$, troviamo anche un omomorfismo surgettivo da Q_8 in $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$e ovviamente uno banale (β non può avere immagine in $\mathbb{Z}/_{4\mathbb{Z}}$ perchè Q_8 ha un solo sottogruppo di indice 4 che ha come immagine $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$). Di questi omomorfismi sopra elencati non tutti vanno bene al fine di costruire la matrice iniziale, infatti prendiamo $i \in Q_8$ e consideriamo $Q_8 \overset{\phi}{\hookrightarrow} Q_8 \times D_4 \overset{\gamma}{\longrightarrow} Q_8 \times D_4$ con $\gamma \in Aut(Q_8 \times D_4)$ e tale che $\phi(i) = g = (i, e_{D_4})$ quindi $\gamma(g) = (\alpha(i), \beta(i))$; siccome γ è un automorfismo manda $Z(g) =< i > \times D_4$ in $Z(\gamma(g)) = Z(\alpha(i)) \times Z(\beta(i))$, ora $Z(\alpha(i))$ può essere Q_8 o $\mathbb{Z}/_{4\mathbb{Z}}$ e $Z(\beta(i))$ può essere D_4, $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ o $\mathbb{Z}/_{4\mathbb{Z}}$, quindi $Z(\alpha(i)) \times Z(\beta(i))$ può essere $Q_8 \times D_4$, $Q_8 \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$, $Q_8 \times \mathbb{Z}/_{4\mathbb{Z}}$, $\mathbb{Z}/_{4\mathbb{Z}} \times D_4$, $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ o $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}$; come li distinguo?, conto gli elementi di ordine 4 che rispettivamente sono 36,24,28,20,8,12, siccome $< i > \times D_4$ ha 20 elementi di ordine 4 allora abbiamo trovato che $Z(\alpha(i)) \times Z(\beta(i)) = \mathbb{Z}/_{4\mathbb{Z}} \times D_4$ quindi $Z(\beta(i)) = D_4$; poichè $\beta(i) \in D_4$ allora $\beta(i) \in Z(D_4) \cong \mathbb{Z}/_{2\mathbb{Z}}$, allora in conclusione $\beta : Q_8 \longrightarrow Z(D_4)$ e ci sono 4 omomorfismi di questo tipo, 3 surgettivi ed uno banale.

Studiamo $\sigma : D_4 \longrightarrow Q_8$: Le possibili immagini sono $\{e\}$ e $\mathbb{Z}/_{2\mathbb{Z}}$ perché i sottogruppi normali di D_4 sono : $< \rho^2 >, < \rho >, < \rho^2, \sigma >, < \rho^2, \rho\sigma >$ ($< \rho^2 >$ non lo contiamo perchè $D_4/_{<\rho^2>} \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ e non si immerge in Q_8), quindi abbiamo 4 omomorfismi, uno banale e 3 non banali che si posso spezzare come composizione di un quoziente e una immersione. In conclusione abbiamo $\sigma : D_4 \longrightarrow Z(Q_8) \cong \mathbb{Z}/_{2\mathbb{Z}}$ infatti sia $(g, h) \in Q_8 \times D_4$ se $\gamma((g, h)) = (\alpha(g)\sigma(h), \beta(g)\delta(h)) = (e_{Q_8}, e_{D_4})$ allora $\alpha(g), x \in Q_8$ e $x\alpha(g)\sigma(h) = xe_{Q_8} = e_{Q_8}x = \alpha(g)\sigma(h)x$, se $x = \alpha(g)^{-1}$ si ha che $\sigma(h) = \alpha(g)\sigma(h)\alpha(g)^{-1}$ quindi $\sigma(h) \in Z(Q_8)$; analogamente si ha lo stesso risultato già trovato prima per β.

Studiamo $\alpha : Q_8 \longrightarrow Q_8$: Se α non fosse surgettiva avrebbe $|Imm(\alpha)| \leq 2$ e $Imm(\alpha) \subset Z(Q_8)$ ma γ è un automorfismo quindi $\gamma|_{Q_8} = \begin{pmatrix} \alpha \\ \sigma \end{pmatrix} = Q_8$ però α, σ non sono surgettive per lo studio precedente quindi non può velere la seconda uguaglianza, perciò α è un automorfismo di Q_8.

Studiamo $\delta : D_4 \longrightarrow D_4$: Se δ non fosse surgettiva avrei che l'immagine sarebbe $\{e\}$ o $\mathbb{Z}/_{2\mathbb{Z}}$ o $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$, ma facendo la stessa considerazione di prima più lo studio di β otterrei che non ci sarebbero elementi di ordine 4 nella immagine di γ in particolare $\gamma|_{D_4}$ non sarebbe un automorfismo di D_4, quindi δ è un automorfismo di D_4.

Abbiamo quindi trovato che se $\alpha \in Aut(Q_8)$, $\beta : Q_8 \longrightarrow Z(D_4)$, $\sigma : D_4 \longrightarrow Z(Q_8)$, $\delta \in Aut(D_4)$ allora $\gamma = \begin{pmatrix} \alpha & \beta \\ \sigma & \delta \end{pmatrix} \in Aut(Q_8 \times D_4)$ e queste sono le condizioni necessarie, vorremmo che siamo sufficienti. Dico che γ è iniettiva : se $\gamma((g, h)) = (e_{Q_8}, e_{D_4})$ allora abbiamo

che $\alpha(g)\sigma(h) \in Z(Q_8) \Longrightarrow g \in Z(Q_8)$ e $\beta(g)\delta(h) \in Z(D_4) \Longrightarrow h \in Z(D_4)$ quindi osservando che $\alpha(-1)\sigma(\rho^2) = -1$, $\alpha(-1)\sigma(e_{D_4}) = -1$, $\beta(1)\delta(\rho^2) = \rho^2$, vale che $(g,h) = (e_{Q_8}, e_{D_4})$ quindi è iniettiva.

2.6.2 esercizio :(Da vedere) $Aut(Q_8)$

soluzione : Intanto osserviamo che $< -1 >$ è caratteristico dato che -1 è l'unico elemento di ordine 2 in Q_8. Consideriamo adesso l'omomorfismo $\psi : Aut(Q_8) \longrightarrow S_3$ tale che $s,t \in Aut(Q_8)$ (dove $s(i) = j$, $s(j) = i$, $s(k) = -k$ e $t(i) - i$, $t(j) = k$, $t(k) = j$) $\psi(s) = (1,2)$ e $\psi(t) = (2,3)$; si ha che il $Ker(\psi) = \{\gamma \in Aut(Q_8) | \gamma(i) = \pm 1,\ \gamma(j) = \pm j\} = Int(Q_8) \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$. Abbiamo cosi ottenuto la succesione $Int(Q_8) \longrightarrow Aut(Q_8) \longrightarrow S_3$, notiamo che $Int(Q_8) \cap \psi(S_3)^{-1} = \{e\} \Longrightarrow Aut(Q_8) \cong (\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \rtimes_\tau S_3$. Studiando l'omomorfismo $\tau : S_3 \longrightarrow Aut(\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}) \cong S_3$, si ottiene che $Aut(Q_8) \cong S_4$.

2.6.3 esercizio : $Aut(D_n)$

Sappiamo da uno studio precedente che $|Aut(D_n)| = n\phi(n)$ e che esiste una bigezione con $\mathbb{Z}/_{n\mathbb{Z}} \times (\mathbb{Z}/_{n\mathbb{Z}})^*$. Consideriamo adesso $\psi : Aut(D_n) \longrightarrow Aut(\mathbb{Z}/_{n\mathbb{Z}})$ con $\psi(\gamma) = \gamma|_{\mathbb{Z}/_{n\mathbb{Z}}}$; questa applicazione è ben definita in quanto $\mathbb{Z}/_{n\mathbb{Z}}$ è caratteristico in D_n, ed è surgettiva perché identifica gli automorfismi di D_n che fissano σ, il nucleo è l'insieme degli automorfismi di D_n che fissano la rotazione ρ, in conclusione si verifica che $D_n \cong \mathbb{Z}/_{n\mathbb{Z}} \rtimes_\tau (\mathbb{Z}/_{n\mathbb{Z}})^*$; i due gruppi hanno intersezione banale e insieme danno tutto D_n grazie all'omomorfismo ψ. Cerchiamo di capire come è fatto τ per studiare il prodotto semidiretto; i generatori di questo gruppo sono ϕ_j con $\phi_j(\rho) = \rho$, $\phi_j(\sigma) = \sigma\rho^j$ e ψ_i con $\psi_i(\rho) = \rho^i$, $\psi_i(\sigma) = \sigma$, quindi $Aut(D_n) = \{\phi_j \circ \psi_i | i \in (\mathbb{Z}/_{n\mathbb{Z}})^*,\ j \in \mathbb{Z}/_{n\mathbb{Z}}\}$, vediamo come agiscono su D_n, $\psi_i \circ \phi_j(\sigma\rho^a) = \sigma\rho^{ij+ia}$ e $\phi_j \circ \psi_i(\sigma\rho^a) = \sigma\rho^{j+ia}$, questo ci induce a studiare $\theta : Aut(D_n) \longrightarrow Aff(\mathbb{Z}/_{n\mathbb{Z}})$ con $\theta(\phi_j \circ \psi_i) = \beta$ dove $\beta(a) = j + ia$, con le osservazioni precedenti si deduce che questo omomorfismo è ben definito ed è un isomorfismo quindi $Aut(D_n) \cong Aff(\mathbb{Z}/_{n\mathbb{Z}})$. L'isomorfismo si può ottenere anche studiando $\mathbb{X} : Aff(\mathbb{Z}/_{n\mathbb{Z}}) \longrightarrow (\mathbb{Z}/_{n\mathbb{Z}})^*$ con $\mathbb{X}(\beta) = i$ dove $\beta(a) = j + ia$, il nucleo è proprio $\mathbb{Z}/_{n\mathbb{Z}}$ quindi si ottiene $Aff(\mathbb{Z}/_{n\mathbb{Z}}) \cong \mathbb{Z}/_{n\mathbb{Z}} \rtimes_{\tau_1} (\mathbb{Z}/_{n\mathbb{Z}})^*$, τ e τ_1 inducono lo stesso prodotto semidiretto.

2.6.4 esercizio : $Aut(\mathbb{Z}/_{n\mathbb{Z}})$

soluzione : Sappiamo che $Aut(\mathbb{Z}/_{n\mathbb{Z}}) \cong (\mathbb{Z}/_{n\mathbb{Z}})^*$, inoltre se $n = ab$ con $(a,b) = 1$ si ha che $(\mathbb{Z}/_{n\mathbb{Z}})^* \cong (\mathbb{Z}/_{a\mathbb{Z}})^* \times (\mathbb{Z}/_{b\mathbb{Z}})^*$, quindi ci riduciamo a studiare $\mathbb{Z}/_{p^n\mathbb{Z}}$ con p primo. Se $p = 2$ dico che $(\mathbb{Z}/_{2^n\mathbb{Z}}) \cong \mathbb{Z}/_{2^{n-2}\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$. So che la cardinalità è $\phi(2^n) = 2^{n-1}$, devo trovare un elemento x di ordine 2^{n-2} e uno y di ordine 2 tale che $x^{2^{n-3}} \neq y$, ed ho finito. Conto le soluzioni di $x^2 \equiv 1\ (2^n)$, $x^2 \equiv 1\ (2^n) \Longrightarrow (x-1)(x+1) \equiv 0\ (2^n) \Longrightarrow x \equiv 1\ (2^{n-1})$ oppure $x \equiv -1\ (2^{n-1})$. Adesso dimostriamo che 5 ha ordine 2^{n-2}, dico che $5^{2^{n-3}} \equiv 1 + 2^{n-1} \not\equiv 1\ (2^n)$. Per induzione su n; $n = 3 \Longrightarrow 5 \equiv 5\ (8)$. Adesso $5^{2^{n-3}} \equiv (5^{2^{n-4}})^2 \equiv (1 + 2^{n-2} + a2^{n-1})^2 \equiv 1 + 2^{n-1}\ (2^n)$.

quindi $5^{2^{n-2}} \equiv (1+2^{n-1})^2 \equiv 1\,(2^m)$ quindi 5 ha ordine 2^{n-2}. Ora basta prendere $-1+2^{n-1}$ che abbiamo dimostrato avere ordine 2 e non appartiene a $< 5 >$ per il conto precedente, quindi 5 e $-1+2^{n-1}$ sono gli elementi cercati che verificano la tesi. Se $p > 2$ dico che $(\mathbb{Z}/_{p^n\mathbb{Z}})^* \cong \mathbb{Z}/_{p^{n-1}\mathbb{Z}} \times (\mathbb{Z}/_{p\mathbb{Z}})^*$. Devo trovare x di ordine $p-1$ e y di ordine p^{m-1}. Considero $\pi : (\mathbb{Z}/_{p^n\mathbb{Z}})^* \longrightarrow (\mathbb{Z}/_{p\mathbb{Z}})^*$ con $\pi(a) = [a]_p$, se $[\epsilon]_p$ ha ordine p-1 allora esiste x tale che $o(x) = o(\epsilon)$. Adesso dico che $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \not\equiv 1\,(p^n)$, lo dimostro per induzione. $n = 2$ ok. Ora $(1+p)^{p^{n-2}} \equiv (1+p^{n-2}+ap^{n-1})^p \equiv (1+p^{k-2(1+ap)})^p \equiv \sum_{i=0}^{p} \binom{p}{i} (p^{n-2}(1+ap))^i \equiv 1+p^{n-1} \not\equiv 1\,(p^n)$. Quindi $(1+p)^{p^{m-1}} \equiv (1+p^{n-1})^p \equiv 1\,(p^n)$. In conclusione abbiamo x trovato prima di ordine p-1 e l'elemento p+1 di ordine p^{n-1} che verificano la tesi.

2.6.5 esercizio : $Aut(S_n)$

soluzione : Vogliamo dimostrare che $Aut(S_n) \cong S_n \ \forall n \geq 3,\ n \neq 6$. Sappiamo che $Int(S_n) \cong S_n/_{Z(S_n)} \cong S_n$. Un automorfismo di S_n è univocamente determinato da i 2-cicli. Consideriamo l'insieme $C_k = \{(a_1, a_2) \cdots (a_{2k-1}, a_{2k})\}$ dei k 2-cicli, ogni C_k può avere immagine in un altro C_j perché mando elementi di ordine in elementi di ordine 2 in elementi dello stesso ordine. Dico che $\gamma \in Aut(S_n)$, $\gamma(C_1) = C_1$ per ogni $n \neq 6$, ovvero un automorfismo di S_n manda C_1 in se stesso, tranne in S_6. Ora $|C_1| = \binom{n}{2}$ e $|C_k| = \binom{n}{2} \cdots \binom{n-2k+2}{2} \frac{1}{k!}$. Risolviamo l'equazione $|C_1| = |C_k|$; quindi si ha $\frac{n!}{(n-2)!2!} = \frac{1}{k!} \frac{n!}{2!(n-2)!} \frac{(n-2)!}{2!(n-4)!} \cdots \frac{(n-2k+2)}{2!(n-2k)!} \iff \frac{(n-2)!}{(n-2k)!} = 2^{k-1}k!$. Per $k = 2$ si ha $4 = (n-2)(n-3)$ impossibile, per $k = 3$ si ha $4 = (n-2)\binom{n-3}{2}$ e vale l'uguaglianza per $n = 6$, per $k > 3$ si ha $2^{k-1} = (n-2)\cdots(n-k+1)\binom{n-k}{k}$ è impossibile perché da un lato abbiamo prodotto di almeno due numeri consecutivi che non potranno mai avere un prodotto pari ad una potenza di due. Vale quindi la tesi meno che per $n = 6$ dove può accadere che $\gamma(C_1) = C_3$. Adesso dico che ogni automorfismo di S_n che fissa C_1 è un automorfismo interno. Vediamo come agisce all'interno di C_1, $\gamma((1,2)) = (a_1, a_2)$ e $\gamma((1,3)) = (a_1, a_3)$ con $a_2 \neq a_3$, di conseguenza $\gamma((2,3)) = \gamma((1,3)(1,2)(1,3)) = (a_1, a_3)(a_1, a_2)(a_1, a_3) = (a_2, a_3)$. Dimostro per induzione che $\gamma((1,i)) = (a_1, a_i)\ \forall i$ con $a_1 \neq a_2 \neq \cdots \neq a_i$. $(1,i)$ non commuta $(1,2)$, quindi $f((1,i))$ non commuta con (a_1, a_2); se fosse che $\gamma((1,i)) = (a_2, x)$ avrei che $(1,i)$ commuta con $(2,3)$ ma $\gamma((1,i)) = (a_2, x)$ non commuta con $\gamma((2,3)) = (a_2, a_3)$, assurdo, quindi $\gamma((1,i)) = (a_1, a_i)$. Perciò se consideriamo σ tale che $\sigma(i) = a_i$ allora $\gamma((1,i)) = \sigma(1,i)\sigma^{-1}$ ovvero coniuga i 2-cicli, siccome i 2-cicli generano tutto S_n allora γ è un coniugio. In conclusione per ogni n diversa da 6 si ha $Aut(S_n) \cong Int(S_n) \cong S_n$.

Anelli

Capitolo 3

Proprietà degli anelli

3.1 Prime definizioni

3.1.1 Definizione : La terna $(A, +, *)$ composta da un insieme A e due operazioni $+, *$ si chiama *anello* se la coppia $(A, +)$ è un gruppo abeliano, $*$ è associativa e vale la proprietà distributiva $a * (c + d)$ (che per brevità scriveremo $a(b + c)$) dove $a, b, c \in A$. Se un anello contiene l'elemento neutro 1 per $*$ allora si chiama *anello con unit*à.

3.1.1 esempio : Sia $\mathbb{K}$ un campo allora $\mathbb{Z}, \mathbb{K}[x], \mathbb{Z}[x], M_n(\mathbb{K})$ sono anelli, l'ultimo scritto è non commutativo.

3.1.2 Definizione Sia A un anello commutativo con unità. Sia $x \in A$, se esiste $y \in A$, $y \neq 0$ tale che $yx = xy = 0$ allora x si dice *divisore di* 0. Se esiste $n \in \mathbb{N}$ tale che $x^n = 0$ allora x si dice *nilpotente*. se esiste $y \in A$ tale che $xy = yx = 1$ allora x si dice *invertibile*.

3.1.3 Definizione : Sia A un anello commutativo. A si dice *dominio di integrit*à se $D = \{\text{divisori di 0 di } A\} = \{0\}$. A si dice *ridotto* se $N = \{x \in A | x \text{ è nilpotente}\} = \{0\}$. Con A^* si indica l'insieme degli elementi invertibili di A. Se in un anello ogni elemento è invertibile, allora si chiama *corpo*. Un corpo commutativo si chiama *campo*.

3.1.1 Proposizione :

1) A^* è un gruppo moltiplicativo.
2) $A^* \cap D = \emptyset$.
3) Se A è finito allora $A = A^* \cup D$.

Dimostrazione :

1) ovvio.
2) Se per assurdo esiste $x \in A^* \cap D$ allora esistono $y, z \neq 0$ tale che $xy = 1$ e $xz = 0$ ma allora $0 = 0y = (zx)y = z(xy) = z(1) = z$ assurdo.
3) Sia $x \in A$, $x \notin D$ allora consideriamo $\gamma_x : A \longrightarrow A$ con $\gamma_x(a) = xa$, siccome x non è un divisore di 0 allora $Ker(\gamma_x) = \{0\}$ e quindi per questioni di cardinalità è surgettiva, ovvero $1 \in Imm(\gamma_x) \Longrightarrow$ esiste y tale che $xy = 1 \Longrightarrow x \in A^*$.

□

3.1.1 Corollario : Se A è un dominio di integrità finito allora A è un campo.

3.1.1 osservazione : $N \subset D$ infatti sia $x \in N$ allora $x^n = 0$ per un opportuno n, ma $x^n = x(x^{n-1}) = 0$ quindi $x \in D$.

3.1.2 esempio : Sia A un anello :

A	A^*	D	N
$\mathbb{Z}$	$\{\pm 1\}$	$\{0\}$	$\{0\}$
$\mathbb{Z}/_{n\mathbb{Z}}$	$(\mathbb{Z}/_{n\mathbb{Z}})^*$	$\{a \mid (a,n) \neq 1\}$	$\{a \mid p_1 \cdots p_r \mid a \text{ per } n = p_1^{d_1} \cdots p_r^{d_r}\}$
$\mathbb{K}[x]$	$\mathbb{K}^*$	$\{0\}$	$\{0\}$

3.2 Ideali

3.2.1 Definizione : Sia $I \subset A$ è un *ideale* se $(I, +)$ è un sottogruppo e $\forall a \in A$, $aI \subset I$. Questa proprietà è detta di *assorbimento*.

3.2.1 esempio : $(f(x)) = \{p(x)f(x) | p(x) \in \mathbb{K}[x]\}$ è un ideale di polinomi in $\mathbb{K}[x]$.

Vedremo che gli ideali hanno proprietà simili ai sottogruppi normali. Inizialmente furono usati per rimediare alla mancanza di alcuni numeri notevoli come l'MCD.

3.2.2 esempio : In $\mathbb{Z}[x]$ 2 e x sono coprimi ma $(2, x) \neq 1$.

3.2.2 Definizione : Sia $S \subset A$ un sottoinsieme non vuoto di A allora si chiama *ideale generato da S in A* l'ideale $(S) = \{\sum_{i=1}^{n} s_i a_i | n \in \mathbb{N} \text{ con } s_i \in S \text{ e } a_i \in A\}$.

3.2.1 osservazione : In un anello non commutativo si definisce *ideale sinistro* un sottogruppo additivo tale che $aI \subset I$, *ideale destro* un sottogruppo additivo tale che $Ia \subset I$ e *ideale bilatero* un sottogruppo additivo tale che $aIb \subset I$.

3.2.2 osservazione : L'ideale generato da un sottoinsieme $(S) = SA$, definito prima, è un ideale destro.

Operazione tra ideali :

1) Siano $I, J \subset A$ ideali. In generale $I \cup J$ non è un ideale perché non è un sottogruppo e lo è solo quando uno è incluso in un altro.
2) $I \cap J$ è un ideale.
3) $I + J = \{i + j \mid i \in I, j \in J\}$ è un ideale ed è il minimo che contiene entrambi.
4) $IJ = \{ij \mid i \in I, j \in J\} = \{\sum_{\alpha=1}^{n} i_\alpha j_\alpha \mid n \in \mathbb{N}, i_\alpha \in I, j_\alpha \in J\}$ non è sempre un ideale.
5) $\sqrt{I} = r(I) = \{x \in A \mid x^n \in I \text{ per qualche } n\}$ si chiama *radicale di* I ed è un ideale.
6) $(I : J) = \{a \in A \mid aJ \in I\}$ è un ideale.

3.2.3 osservazione : $\sqrt{0} = N$ il radicale dell'ideale 0 è uguale all'insieme degli elementi nilpotenti, in particolare N è un ideale.

3.2.4 osservazione : Consideriamo l'anello $\mathbb{Z}$, chi sono i suoi ideali? cerchiamo i sottogruppi. I sottogruppi sono della forma $n\mathbb{Z}$ e tutti questi sono anche ideali.

3.2.1 esercizi : Dire se i seguenti insiemi : $m\mathbb{Z} \cap n\mathbb{Z}$, $m\mathbb{Z} + n\mathbb{Z}$, $m\mathbb{Z}n\mathbb{Z}$, $\sqrt{n\mathbb{Z}}$, $(n\mathbb{Z} : m\mathbb{Z})$ sono ideali e determinale per quali $a \in \mathbb{Z}$ sono uguali a $a\mathbb{Z}$.

soluzione : Sappiamo per l'osservazione 3.2.2 che sono tutti ideali meno che in alcuni casi l'insieme $m\mathbb{Z}n\mathbb{Z}$ quindi vediamo se in questo caso lo è. Sia $a \in \mathbb{Z}$ allora $am\mathbb{Z}n\mathbb{Z} = ma\mathbb{Z}n\mathbb{Z} = m\mathbb{Z}n\mathbb{Z}$, la prima uguaglianza deriva dal fatto che l'anello $\mathbb{Z}$ è commutativo. Osserviamo che $m\mathbb{Z} \cap n\mathbb{Z} = mcm(m,n)\mathbb{Z}$, $m\mathbb{Z} + n\mathbb{Z} = MCD(m,n)\mathbb{Z}$, $m\mathbb{Z}n\mathbb{Z} = mn\mathbb{Z}$, $\sqrt{n\mathbb{Z}} = p_1 \cdots p_r\mathbb{Z}$ dove $n = p_1^{a_1} \cdots p_r^{a_r}$ e $p_1, \cdots, p_r$ primi distinti, $(n\mathbb{Z} : m\mathbb{Z}) = n\mathbb{Z}$ se $(n,m) = 1$ oppure $(n\mathbb{Z} : m\mathbb{Z}) = \frac{n}{MCD(n,m)}\mathbb{Z}$ se $(n,m) \neq 1$.

3.2.3 Definizione : Sia $I \subset A$ un ideale, si dice che I è un *ideale proprio* se $I \neq A$.

3.2.1 Proposizione : I è un ideale proprio se e solo se $I \cap A^* = \emptyset$.

Dimostrazione : ($\Longrightarrow$) Sia I ideale proprio di A, allora esiste $a \in A/I$. se esiste $u \in I \cap A^*$ allora $1 = uu^{-1} \in I$ e di conseguenza per la proprietà di assorbimento $a1 \in I$ che è assurdo.
($\Longleftarrow$) Detto che $I \cap A^* = \emptyset$ allora I e contenuto strettamente in A in quanto non contene $1 \in A^*$.

□

3.2.1 Corollario : In un campo $\mathbb{K}$ gli unici ideali sono $\{0\}$ e $\mathbb{K}$.

3.2.3 esempio : Se p primo si ha che $(p^a) : (p^b) = (p^{a-b})$ se $a \geq b$ oppure $(p^a) : (p^b) = (1)$ se $a < b$, in altri termini $(p^a) : (p^b) = p^{max(a-b,0)}$; ad esempio $(3) : (9) = \mathbb{Z}$ e $(9) : (3) = (3)$. In generale se $m = p_1^{a_1} \cdots p_k^{a_k}$ e $n = p_1^{b_1} \cdots p_k^{b_k}$ allora $(m) : (n) = (p_1^{max(a_1-b_1,0)} \cdots p_k^{max(a_k-b_k,0)})$.

3.3 Omomorfismi di anelli

3.3.1 Definizione : Siano A, B anelli, l'applicazione $f : A \longrightarrow B$ è un *omomorfismo di anelli* se per ogni $a_1, a_2 \in A$ si ha che :
1) $f(a_1 + a_2) = f(a_1) + f(a_2)$.
2) $f(a_1 a_2) = f(a_1) f(a_2)$.
3) $f(1_A) = f(1_B)$.

3.3.1 osservazione : La terza condizione non è necessaria, si può costruire una teoria dove si considerano omomorfismi tutte le applicazioni che verificano solo le prime due condizioni. Aggiungendo però la terza condizione si semplificano molte cose ma se ne perdono altre per esempio l'applicazione inclusione, $f : A \longrightarrow A \times B$ dove $f(1_A) = (1_A, 0)$ non è un omomorfismo di anelli.

3.3.2 Definizione : Sia $I \subset A$ un ideale, allora $(a + I)(b + I) = ab + I$.

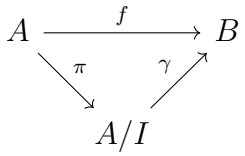
Il quoziente A/I è un anello, la verifica è semplice.

3.3.1 Proposizione : Gli ideali di A sono tutti e soli i nuclei di omomorfismi.

Dimostrazione : Sia I un ideale allora $I = Ker(\pi)$ dove $\pi : A \longrightarrow A/I$ è l'omomorfismo di proiezione. Sia $f : A \longrightarrow B$ un omomorfismo, allora il $ker(f)$ è un sottogruppo, verifico che è ideale. Sia $x \in Ker(f)$ allora $f(ax) = f(a)f(x) = 0$ quindi $ax \in Ker(f)$ e perciò $aKer(f) \subset Ker(f)$.

□

3.3.1 Teorema : (Di omomorfismo) Sia $f : A \longrightarrow B$ un omomorfismo e sia $I \subset ker(f)$ un ideale. Allora esiste uno ed un solo omomorfismo $\gamma : A/I \longrightarrow B$ tale che :



Dove γ è iniettivo e $\gamma(A/I) = f(A)$.

Dimostrazione : Per il teorema di omomorfismo di gruppi sappiamo che esiste ed è unica γ che verifica lo schema, bisogna solo verificare che questa γ è anche di anello ed abbiamo finito. Quindi $\gamma(\bar{a}\bar{b}) = f(ab) = f(a)f(b) = \gamma(\bar{a})\gamma(\bar{b})$ e $\gamma(1 + I) = f(1) = 1_B$, quindi vale la tesi.

□

3.3.1 Lemma : Sia $f : A \longrightarrow B$ un omomorfismo di anelli, $I \subset A$ ideale e $J \subset B$ ideale. allora $f(J)^{-1}$ è un ideale di A e se f è surgettiva $f(I)$ è un ideale di B.

Dimostrazione : Intanto sappiamo che $f(J)^{-1} < A$ è sottogruppo, verifichiamo la proprietà di assorbimento; consideriamo $ax \in af(J)^{-1}$ con $a \in A$ e $x \inf(J)^{-1}$, allora $f(ax) = f(a)f(x)$ ma $f(x) \in J$ che è ideale quindi anche $f(a)f(x)$ di conseguenza $af(J)^{-1} \in f(J)^{-1}$. Adesso supponiamo che f sia surgettiva e consideriamo l'insieme $bf(I)$ con $b \in B$, sappiamo che per la surgettività di f esiste $a \in A$ tale che $b = f(a)$ quindi $bf(I) = f(a)f(I) = f(aI) \subset f(I)$.

□

3.3.1 esempio : L'ipotesi di surgettivtà è necessaria infatti consideriamo $i : \mathbb{Z} \longrightarrow \mathbb{Q}$, l'ideale $n\mathbb{Z}$ ha immagine l'insieme $n\mathbb{Z}$ che non è ideale in $\mathbb{Q}$ dati che in quanto campo ha ideali solo 0 e tutto $\mathbb{Q}$.

3.3.2 Teorema : (Di corrispondenza) Sia $\pi : A \longrightarrow A/I$ un omomorfismo surgettivo, questo induce una corrispondenza biunivoca tra gli ideali di A/I e gli ideali di A che contengono I. Questa corrispondenza conserva l'ordinamento (analogo a quello per i gruppi già citato precedente).

Dimostrazione : Siano $I \subset J$ ideali dell'anello A, sappiamo per il lemma precedente che $\pi(J) = J/I$ è un ideale di A/J, e $\pi(K)^{-1}$ è un ideale di A, dove K è ideale di A/I.

□

3.3.2 osservazione : Siano I, J ideali, consideriamo l'insieme IJ definito nella sezione precedente, in generale vale che $IJ \subset I \cap J$ infatti se $x \in I$ e $y \in J$ allora $xy \in I \cap J$, prima uso l'assorbimento di I su y e poi l'assorbimento di J su x. In generale non sono uguali infatti

se $I = J = \mathbb{Z}/_{2\mathbb{Z}}$ allora $IJ = \mathbb{Z}/_{4\mathbb{Z}}$ e $I \cap J = \mathbb{Z}/_{2\mathbb{Z}}$.

3.3.2 Lemma : Se $I + J = (1) = A$, ovvero se I e J sono *comassimali* e si scrive (I, J), allora IJ è ideale e $IJ = I \cap J$.

Dimostrazione : Sappiamo già che $IJ \subset I \cap J$. Se I e J sono comassimali allora esiste $i \in I$ e $j \in J$ tale che $i+j = 1$, sia $x \in I \cap J$ allora $x = 1x = xi+xj \in IJ$ quindi $I \cap J \subset IJ$ e vale la tesi.
□

3.3.3 Teorema : (cinese) Siano I, J ideali dell'anello A e sia $f : A \longrightarrow A/I \times A/J$ dove $f(a) = (a + I, a + J)$. Allora :

1) f è omomorfismo e $Ker(f) = I \cap J$.
2) f è surgettiva se e solo se $I + J = A$, (il teorema in se dice solo che $I + J = A \Longrightarrow$ f surgettiva, ma siccome è vera anche l'altra implicazione noi la consideriamo nell'enunciato)
3) Nella ipotesi del 2) vale $A/_{IJ} \cong A/I \times A/J$.

Dimostrazione :

1) f è omomorfismo perché lo è sulle singole coordinate. $Ker(f) = \{a \in A \mid f(a) = (a + I, a + J) = (\bar{0}, \bar{0})\} = \{a \in A \mid a \in I \text{ e } a \in J\} = I \cap J$.
2) Supponiamo che $I + J = A$ allora esistono $i \in I$ e $j \in J$ tale che $1 = i + j$. Per ogni $(x + I, y + J) \in A/I \times A/J$ consideriamo $a = xj + yi$ allora $f(a) = f(a + I, a + J) = (xj+yi+I, xj+yi+J) = (x(1-i)+yi+I, xj+y(1-j)+J) = (x+(y-x)i+I, y+(x-y)j+J) = (x + I, y + J)$, quindi è surgettiva. Supponiamo infine che f sia surgettiva quindi esiste $a \in A$ tale che $f(a) = (1 + I, J)$ quindi $a - 1 \in I$ e $a \in J$ perciò $a - 1 = i \Longrightarrow 1 = a - i \in I + J$.
3) Applicando il teorema di omomorfismo si ed il lemma precedente si ha che $A/I \times A/J \cong A/_{Ker(f)} \cong A/_{I \cap J} \cong A/_{IJ}$.
□

3.3.1 esercizio : La sostituzione negli anelli di polinomi è sempre un omomorfismo.

soluzione : Sia A un anello e consideriamo l'anello $A[x_1, \cdots, x_n]$ e l'applicazione $\gamma : A[x_1, \cdots, x_n] \longrightarrow A[x_2, \cdots, x_n]$ dove $\gamma(f(x_1, \cdots, x_n)) = f(a, x_2, \cdots, x_n)$. siano $f = \alpha_1 x_1 + \cdots + \alpha_n x_n$ e $g = \beta_1 x_1 + \cdots + \beta_n x_n$ allora $\gamma(f + g) = a\alpha_1 + \cdots + \alpha_n x_n + a\beta_1 + \cdots + \beta_n x_n = \gamma(f) + \gamma(g)$.

3.3.3 Definizione : Consideriamo l'omomorfismo $f : A \longrightarrow B$, e sia I ideale di A e J ideale di B, sappiamo che $f^{-1}(J)$ è un ideale di A e prendo il nome di *contrazione di* J e si scrive J^C, invece $f(I)$ non è sempre un ideale di B quindi consideriamo l'ideale $(f(I))$ generato da $f(I)$ e prende il nome di *estensione di* I e si scrive I^E.

3.3.3 osservazione : Consideriamo il caso $f : A \hookrightarrow B$ allora $I^C = f^{-1}(I) = I \cap A$ e $I^E = IB$.

3.3.2 Proposizione : Se $J \subset B$ è primo allora J^C è primo in A.

Dimostrazione : Consideriamo :

$$A \xrightarrow{omo.inj.} B \longrightarrow B/J$$
$$\gamma$$

Il $Ker(\gamma) = J \cap A = J^C$ che è primo perché $A/_{J^C} \hookrightarrow B/J$ e B/J è un dominio quindi anche $A/_{J^C}$.

3.3.2 esercizio : Trovare ideale massimale che si contrae a ideale primo non massimale.

soluzione : (Da vedere)

3.4 Ideali notevoli

3.4.1 Definizione : Un ideale $I \subseteq A$ si dice *primo* se per ogni $x, y \in A$ si ha che se $xy \in I$ allora $x \in I$ oppure $y \in I$.

3.4.1 esempio : Gli ideali primi di $\mathbb{Z}$ sono della forma $p\mathbb{Z}$ dove p è primo e l'ideale 0.

3.4.2 Definizione : Un ideale $I \subseteq A$ si dice *massimale* se è massimale rispetto all'inclusione tra ideali propri, ovvero se $I \subset J \subsetneq A$ allora $I = J$.

3.4.3 Definizione : Un ideale $I \subseteq A$ si dice *principale* se esiste $x \in A$ tale che $I = (x)$.

3.4.4 Definizione : Sia Ω un insieme, $\leq$ un ordinamento parziale e $\Gamma \subset \Omega$ un sottoinsieme. $X \in \Omega$ si dice *massimo per* Ω se per ogni $A \in \Omega$, $A \leq X$. $M \in \Omega$ si dice *maggiorante per* Γ se per ogni $A \in \Gamma$, $A \leq M$. $A \in \Gamma$ è un *elemento massimale per* Γ se per ogni $B \in \Gamma$ tale che $B \geq A \implies B = A$. $C \subset \Gamma$ si dice *catena* se C è totalmente ordinato. $(\Gamma, \leq)$ si dice *induttivo* se ogni catena di Γ ammette un maggiorante per Γ.

3.4.1 Lemma : (Di Zorn) Sia $(\Gamma, \leq)$ parzialmente ordinato. Se $\Gamma \neq \emptyset$ e Γ è induttivo allora esiste M massimale.

3.4.1 osservazione : $\Gamma = \{I \subseteq A \mid I \text{ ideale proprio }\}$, $\subseteq$ è un ordinamento parziale su Γ. $C = \{I_\lambda\}_{\lambda \in \Lambda}$ è una catena; $I = \cup I_\lambda$ è un ideale di A e sta in Γ, Γ è induttivo quindi esiste elemento massimale. In un campo l'ideale 0 è massimale e gli ideali primi di $\mathbb{Z}$ diversi da 0 sono massimali.

3.4.1 Proposizione : Ogni ideale proprio di A è contenuto in un ideale massimale di A.

Dimostrazione : Sia $\Omega = \{J \subsetneq A \mid I \subseteq J\}$ dove $I \in \Omega \neq \emptyset$. Ω induttivo con $\subseteq$, allora per per il lemma di Zorn esiste $M \in \Omega$ massimale. Chiaramente $I \subset M$, osservo che M è in effetti un ideale massimale di A. Se $M \subseteq M' \subset A$ allora $I \subseteq M' \Longrightarrow M' \in \Omega$, ma M è massimale in Ω quindi $M = M'$.

□

3.4.1 Corollario : Per ogni $x \in A$, $x \notin A^*$ x è contenuto in un ideale massimale infatti considerando $I = (x)$ l'ideale generato da x, siccome x non è invertibile I è proprio in A quindi usando il lemma precedente si ha la tesi.

3.4.2 Proposizione : Sia $I \subsetneq A$ un ideale proprio di A, allora :

1) I è primo se e solo se A/I è un dominio.
2) I è massimale se e solo se A/I è un campo.

Dimostrazione :

1) consideriamo la proiezione $\pi : A \longrightarrow A/I$, allora I è primo $\Longleftrightarrow$ per ogni $xy \in I$ si ha che $x \in I$ oppure $y \in I \longrightarrow \pi(xy) = \pi(x)\pi(y)$ allora $\pi(x) = \bar{0}$ oppure $\pi(y) = \bar{0} \Longleftrightarrow A/I$ è dominio.
2) I massimale $\Longleftrightarrow$ in A/I ci sono solo ideali banali $\Longleftrightarrow$ A/I è un campo.

□

3.4.2 Corollario :

1) A dominio $\Longleftrightarrow$ $\{0\}$ è un ideale primo.
2) A campo $\Longleftrightarrow$ $\{0\}$ è massimale.
3) Massimale $\Longrightarrow$ primo, quindi un campo è anche un dominio.

3.4.2 osservazione : Il teorema di corrispondenza conserva l'indice, gli ideali massimali e

ideali primi, se $I \subset J$ allora $A/J \cong (A/I)/_{(J/I)}$.

3.5 Campo dei quozienti di un dominio

3.5.1 Definizione : Sia A un anello commutativo con unità e sia $\gamma : \mathbb{Z} \longrightarrow A$ un omomorfismo dove $\gamma(1) = 1_A$. Il $Ker(\gamma) = n\mathbb{Z}$ diciamo allora che A ha *caratteristica* n e si scrive $char(A) = n$.

3.5.2 Definizione : Sia A un dominio e $S \subset A$ un sottoinsieme. Se $1 \in S$, $0 \notin S$ e S moltiplicativamente chiuso ovvero se $s, t \in S \Longrightarrow st \in S$, allora si dice che S è *Parte Moltiplicativa di A*.

3.5.3 Definizione : Si definisce *anello delle frazioni* l'anello $S^{-1}A = \{(a, s) \mid a \in A, s \in S\}/_{\sim}$ con $(a, s) \sim (b, t) \Longleftrightarrow at = bs$, $[(a, s)] = \frac{a}{s}$.

3.5.1 osservazione : A è un dominio $\Longleftrightarrow S = A - \{0\}$ è una parte moltiplicativa, infatti se A è un dominio allora $1 \in A - \{0\}$ e $0 \notin A - \{0\}$ e se $s \neq 0, t \neq 0 \in A - \{0\} \Longrightarrow st \neq 0$ quindi $st \in A - \{0\}$, viceversa se $A - \{0\}$ è parte moltiplicativa allora se $s \neq 0, t \neq 0 \Longrightarrow st \neq 0$ quindi A è dominio.

3.5.1 esempio : Come già detto per ogni dominio A, $A - \{0\}$ è parte moltiplicativa, se $A = \mathbb{Z}$ allora $S = \{2^n\}_{n \geq 0}$ è una parte moltiplicativa. Se P è un ideale primo allora $S = A - P$ è parte moltiplicativa infatti $1 \notin P$ quindi appartiene ad S, $0 \in P$ quindi non appartiene ad S, inoltre per la primalità si P se $s, t \notin P$ allora $st \notin P$.

3.5.1 Proposizione : $(s^{-1}A, +, \cdot)$ è un anello.

Dimostrazione : $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ chiusura $+$, $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ chiusura $\cdot$. Resta da verificare che se $\frac{a}{s} = \frac{a'}{s'}$ e $\frac{b}{t} = \frac{b'}{t'}$ allora $\frac{at+bs}{st} = \frac{a't'+b's'}{s't'}$; sappiamo che $as' = a's$ e $bt' = b't$ allora considerando $(at + bs)s't' = as'tt' + bt's's = a'stt' + b'sts' = (a't' + b's')st$, sapendo che $st, s't' \in S$ allora si ha la tesi.

□

3.5.3 Definizione : Sia A un anello, se $S = A - \{0\}$ è una parte moltiplicativa allora l'anello delle frazioni $S^{-1}A$ è un campo ed è chiamato *campo dei quozienti diA* è si scrive $Q(A)$.

3.5.2 Proposizione : L'omomorfismo $\gamma : A \longrightarrow Q(A)$, dove $\gamma(a) = \frac{a}{1}$ è iniettivo.

Dimostrazione : Intanto verifichiamo che effettivamente $Q(A)$ sia un campo. Sia $\frac{0}{1} \neq \frac{a}{s} \in Q(A)$ allora se $a \neq 0 \Longrightarrow a \in S$ quindi $(\frac{a}{s})^{-1} = \frac{s}{a} \in Q(A)$. Detto ciò torniamo sull'omomorfismo; abbiamo che $\gamma(a_1) + \gamma(a_2) = \frac{a_1}{1} + \frac{a_2}{1} = \frac{a_1+a_2}{1} = \gamma(a_1 + a_2)$, $\gamma(a_1 a_2) = \frac{a_1 a_2}{1} = \frac{a_1}{1}\frac{a_2}{1} = \gamma(a_1)\gamma(a_2)$ e che $\gamma(1) = \frac{1}{1}$ quindi γ è un omomorfismo. Ora $Ker(\gamma) = \{a \mid \frac{a}{1} = \frac{0}{1}\} = \{0\}$ quindi è iniettiva.

□

3.5.1 Corollario :

1) Ogni dominio si immerge nel suo campo dei quozienti.

2) Se A è un dominio, $\mathbb{K}$ un campo ed A si immerge in $\mathbb{K}$ tramite ϕ, allora ϕ si può estendere ad una immersione di $Q(A)$ in $\mathbb{K}$.

Dimostrazione : Il punto 1) è conseguenza della preposizione precedente, quindi dimostriamo il punto 2). Sia $\gamma : A \longrightarrow \mathbb{K}$, e $\tilde{\gamma} : Q(A) \longrightarrow \mathbb{K}$ dove $\tilde{\gamma}|_A = \gamma$. Intanto $\tilde{\gamma}$ è ovviamente iniettiva perché $Q(A)$ è campo, è ben definita infatti $\tilde{\gamma}(\frac{a}{s}) = \gamma(a)\gamma(s)^{-1} \in \mathbb{K}$ dato che $\gamma(s) \neq 0 \Longleftrightarrow s \neq 0$, perché γ iniettiva, quindi in $\mathbb{K}$ esiste $\gamma(s)^{-1}$ e perciò vale che $\gamma(a)\gamma(s)^{-1} \in \mathbb{K}$. Inoltre $\tilde{\gamma}(\frac{a}{s})$ non dipende dal rappresentante infatti se si ha $\frac{a}{s} = \frac{a'}{s'}$ ovvero $as' = a's$ allora $\tilde{\gamma}(\frac{a}{s}) = \gamma(a)\gamma(s)^{-1} = \gamma(as^{-1}) = \gamma(a's'^{-1}) = \gamma(a')\gamma(s')^{-1} = \tilde{\gamma}(\frac{a'}{s'})$ quindi $\tilde{\gamma}$ è un omomorfismo.

□

3.5.2 esempio : Sia $\mathbb{K}[x]$ l'anello dei polinomi a coefficienti in $\mathbb{K}$ allora $\mathbb{K}(x) = \{\frac{f(x)}{g(x)} \mid g(x) \neq 0\}$ è il campo dei quozienti di $\mathbb{K}[x]$. Sia $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'anello degli interi di gauss, che è un dominio, allora $\mathbb{Q}(i) = \mathbb{Q}[i] \cong \mathbb{Q}[x]/_{(x^2-1)}$ è il suo campo dei quozienti. Si posso fare anelli di frazioni anche senza avere un dominio ma bisogna sistemare la relazione di equivalenza.

3.5.4 Definizione : Se A è un dominio allora si definisce $Frac(A) = \{\frac{a}{b} \mid a \in A,\ b \in A/\{0\}\}/_\sim$ con $\frac{a}{b} \sim \frac{a'}{b'} \Longleftrightarrow ab' = ba'$. Sia $S \subset A$ tale che $0 \notin S$, S moltiplicativamente chiuso, allora si definisce $S^{-1}A = \{\frac{a}{s} \mid a \in A,\ s \in S\}/_\sim$ con $\frac{a}{s} \sim \frac{a'}{s'} \Longleftrightarrow as' = sa'$.

3.5.1 esercizio : (Da vedere)

1) Sia $S \subset \mathbb{Z},\ S = \{2^n\}_{n\geq 1}$, allora si ha l'anello $S^{-1}A$. Chi sono gli ideali primi ?

2) $P \subset A$ ideale primo, $S = A/P$. Chi sono gli ideali primi di $S^{-1}A$?

3) Se A non è un dominio, $0 \notin S \subset A$ e S moltiplicativamente chiuso, esiste $r \in S^{-1}A$ tale che se $\frac{a}{b} \sim \frac{a'}{b'} \Longrightarrow (ab' - ba')r = 0$.

soluzione :

1)

2)

3) Sia $A = \{f : \mathbb{R} \longrightarrow \mathbb{R},\ \textit{continua}\}$ e sia $I = \{f \in A \mid f(0) = 0\}$, questo è un ideale primo, allora consideriamo $S = A/I$ e di conseguenza $S^{-1}A$ allora se $\frac{f}{g} \sim \frac{h}{g}$ e f, h coincidono in un intorno di 0 allora esiste g' tale che $(fg - hg)g' = 0$.

3.5.3 Proposizione : Siano A, B domini e sia $0 \notin S \subset A$ moltiplicativamente chiuso, consideriamo $f : A \longrightarrow B$ tale che $f(S) \subset B^*$. Allora esiste ed è unica $\tilde{f} : S^{-1}A \longrightarrow B$ tale che $\tilde{f}$ estende f e commuta lo schema :

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & \searrow^{ini.} \quad \nearrow_{\tilde{f}} & \\ & S^{-1}A & \end{array}$$

Dimostrazione : Osserviamo che se $a \in A,\ s \in S$ allora $f(a) = \tilde{f}(\frac{sa}{s}) = \tilde{f}(s)\tilde{f}(\frac{a}{s}) = f(s)\tilde{f}(\frac{a}{s}) \Longrightarrow \tilde{f}(\frac{a}{s}) = f(a)f^{-1}(s)$, esiste $f^{-1}(s)$ per ipotesi in quanto $f(s) \in B^*$. Ora se $\frac{a}{s} \sim \frac{b}{t}$ allora $\tilde{f}(\frac{a}{s}) = \tilde{f}(\frac{b}{t}) \Longrightarrow f(a)f^{-1}(s) = f(b)f^{-1}(t)$ ma per ipotesi $\frac{a}{s} \sim \frac{b}{t} \Longrightarrow at = bs \Longrightarrow f(at) = f(a)f(t) = f(b)f(s) \Longrightarrow f(a)f^{-1}(s) = f(b)f^{-1}(t)$ quindi $\tilde{f}$ è ben definita. É facile vedere che è anche un omomorfismo, inoltre $Ker(\tilde{f}) = \{\frac{a}{s} \mid \tilde{f}(\frac{a}{s}) = 0\} = \{\frac{a}{s} \mid f^{-1}(s)f(a) = 0\} = \{\frac{a}{s} \mid f(a) = 0\} = S^{-1}Ker(f)$.

□

3.5.3 esempio : Consideriamo l'anello $\mathbb{Z}$ e l'ideale primo $P = (3)$ e il sottoinsieme $S = \mathbb{Z}/P$ allora si ha $S^{-1}\mathbb{Z} = \mathbb{Z}_{(3)} = \{\frac{a}{b},\ 3 \not| b\}$. Sia I un ideale di $\mathbb{Z}$ allora :
$I = (2) \Longrightarrow S^{-1}I = \mathbb{Z}$
$I = (3) \Longrightarrow S^{-1}I = (3)$
$I = (6) \Longrightarrow S^{-1}I = (3)$
$I = (9) \Longrightarrow S^{-1}I = (9)$
Allora la mappa che corrisponde I ad $S^{-1}I$ non è iniettiva.

3.5.2 esercizio :

1) Non esiste $f : \mathbb{Z}[x] \longrightarrow \mathbb{Q}$ omomorfismo surgettivo.

2) Preso $S \subset \mathbb{Z},\ S = \{interi\ dispari\}$. Allora esiste $g : \mathbb{Z}[x] \longrightarrow \mathbb{Q}$ omomorfismo surgettivo.

3) Sia P ideale primo di A dominio. Allora $S = A/P$ è moltiplicativamente chiuso. Sia $A_P = S^{-1}A$, gli ideali di A_P corrispondono agli ideali di A contenenti P, inoltre A_P ha un unico ideale massimale che è $S^{-1}P$.

soluzione :

1) Consideriamo un omomorfismo $f : \mathbb{Z}[x] \longrightarrow \mathbb{Q}$, questo è tale che $f(1) = 1,\ f(0) = 0,\ f(x) = \frac{p}{q}$, ma l'immagine di f ha elementi razionali di denominatore una potenza di q che essendo solo prodotto di un numero finito di primi non può dare ogni denominatore di ogni razionale di $\mathbb{Q}$ quindi non può essere surgettiva per ogni scelta di $f(x)$.

2) Considero $f : S^{-1}\mathbb{Z}[x] \longrightarrow \mathbb{Q}$, tale che $f(x) = \frac{1}{2}$ ora per ogni $\frac{a}{b} \in \mathbb{Q}$ con $b = 2^m d$ con d dispari, si ha che $f(d^{-1}ax^m) = \frac{a}{b}$, quindi è surgettiva.

3) $S = A/P$ e moltiplicativamente chiuso infatti se $a, b \in S$ e $ab \notin S \Longrightarrow ab \in P$ ma P essendo primo implica $a \in P \vee b \in P$, assurdo, quindi $ab \in S$. $\tau : \{I\ ideale\ di \mathbb{Z}\} \longrightarrow \{J\ ideale\ di\ A_P\}$ è una corrispondenza non iniettiva tra gli ideali di $\mathbb{Z}$ contenenti P e gli ideali di A_P infatti se I è ideale di $\mathbb{Z}$ allora $S^{-1}I$ è ideale di A_P inoltre $S^{-1}I$ è proprio $\Longleftrightarrow I \cap S = \emptyset \Longleftrightarrow I \subset P$. $S^{-1}P$ è l'unico ideale massimale di A_P, infatti è massimale perché $A_P/_{S^{-1}P} \cong \bar{S}^{-1}(A/P) = Frac(A/P)$ che è un campo. Ora osserviamo che se $x \in A_p/S^{-1}P$ allora $x = \frac{a}{b}$ con $a, b \in S$ quindi x è invertibile e per questo $S^{-1}P$ è l'unico ideale massimale.

3.6 Divisibilità nei domini

3.6.1 Definizione : Sia A un dominio, $a, b \in A$ con $a \neq 0$ allora a *divide* b, $a|b$, se $b = ac$ con $c \in A$.

3.6.1 osservazione : $a|b \Longleftrightarrow (b) \subseteq (a)$ infatti $a|b \Longleftrightarrow b = ac \Longleftrightarrow b \in (a) \Longleftrightarrow (b) \subseteq (a)$.

3.6.2 Definizione : $a, a' \in A$ si dicono *associati*, e si scrive $a \sim a'$, se vale una delle seguenti condizioni :

1) $a|a'$ e $a'|a$.

2) $(a) = (a')$.

3) $a = a'u$ con $u \in A^*$.

3.6.1 Proposizione : Le tre condizioni della definizione precedente sono equivalenti.

Dimostrazione : 1) $\iff$ 2) : segue dall'osservazione 3.6.1. 1) $\implies$ 3) : se $a|a'$ $a'|a$ esistono u, v tale che $a = a'u$ e $a' = av$ quindi $a = auv \implies a(1 - uv) = 0$ ma A è un dominio quindi $uv = 1$ ovvero $u.v \in A^*$. 3) $\implies$ 2) : Se $a = a'u$ con $u \in A^* \implies a \in (a') \implies (a) \subseteq (a')$ ma $a' = au^{-1}$ quindi $(a') \subseteq (a)$ perciò $(a) = (a')$.

□

3.6.3 Definizione : Siano $a, b \in A$ non entrambi nulli. Allora $d \in A$ è un MCD *pera*$, b$, e si scrive $(a, b) = d$, se :

1) $d|a$ e $d|b$.

2) se $c \in A$ tale che $c|a$ e $c|b$ allora $c|d$.

3.6.2 Preposizione : se d e d' sono MCD per a, b allora $d \sim d'$.

Dimostrazione : in quanto MCD vale che $d|d'$ e $d'|d$, si conclude con la proposizione 3.6.1.

□

3.6.4 Definizione : Un elemento $x \in A$, $x \notin A^* \cup \{0\}$ si dice *primo* se per ogni $a, b \in A$ tale che $x|ab$ si ha che $x|a \vee x|b$. Si dice *irriducibile* se $x = ab$, $a, b \in A$ allora $a \in A^* \vee b \in A^*$.

3.6.3 Proposizione :

1) x è primo $\iff$ l'ideale (x) è primo diverso da 0.

2) x è irriducibile $\iff$ L'ideale (x) è massimale tra gli ideali principali.

Dimostrazione :

1) Ovvio dalla definizione.

2) ($\implies$) : $(x) \subseteq (y) \subsetneq A$ allora $x \in (y)$, $x = ay$ ma x irriducibile quindi $a \in A^*$ (se fosse $y \in A^*$ allora $(y) = A$ che va contro le ipotesi), quindi $(x) = (y)$.
($\impliedby$) : Supponiamo che x non si irriducibile quindi $x = ab$, $a, b \notin A^*$. Osserviamo allora che vale $(x) \subsetneq (a) \subsetneq A$ quindi $a = xc \implies x = xcb$ siccome siamo in un dominio si ha che $b, c \in A^*$

assurdo.

□

3.6.4 Proposizione : x primo $\Longrightarrow$ x irriducibile.

Dimostrazione : Sia x primo tale che $x = ab$ quindi $x|ab$ e perciò $x|a$ oppure $x|b$, supponiamo senza perdita di generalità che $x|a$ ovvero $a = xc$ di conseguenza $x = xcb$ essendo in un dominio si ha che $c, b \in A^*$ quindi x irriducibile.

□

3.6.5 Proposizione : Sia I un ideale dell'anello A. allora :

1) $\sqrt{I}$ è un ideale di A.

2) $I \subset \sqrt{I}$.

3) I, J ideali di A. Allora $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

4) $\sqrt{I} = A \Longleftrightarrow I = A$.

5) Se P primo allora $\sqrt{P} = P$ (gli ideali per cui vale $\sqrt{I} = I$ si dicono *ideali radicali*).

6) $\sqrt{I} = \bigcap\limits_{I \subset P} P$ dove P è un ideale primo, in particolare $N = \bigcap\limits_{P \subset A} P$

Dimostrazione :

1) Per ogni $ax \in a\sqrt{I}$ con $x \in \sqrt{I}$, $a \in A$ si ha che $x^n \in I$ per definizione di radicale, quindi $a^n x^n \in I$ in quando I è ideale perciò, siccome $a^n x^n = (ax)^n$, si ha che $ax \in \sqrt{I}$ di conseguenza $a\sqrt{I} \subset \sqrt{I}$ ovvero vale a proprietà di assorbimento. Ora siano $x, y \in \sqrt{I}$ quindi esistono $n, m \in \mathbb{N}$ tale che $x^n, y^m \in I$, consideriamo adesso l'elemento $x + y$ e osserviamo che $(x+y)^{n+m} = \sum\limits_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i}$ se $i < n$ allora $n + m - i > m$ quindi $y^{n+m-i} \in I$ e di conseguenza anche $x^i y^{n+m-i} \in I$, se $i \geq n$ allora $x^i \in I$ e di conseguenza anche $x^i y^{n+m-i} \in I$, in conclusione si ha che $(x+y)^{n+m} \in I$ quindi $x + y \in \sqrt{I}$ ovvero $\sqrt{I}$ è chiuso per $+$ e perciò è un gruppo, ottenendo così la tesi.

2) ovvio.

3) Osserviamo intanto che se $I \subset J \Longrightarrow \sqrt{I} \subset \sqrt{J}$, infatti se $x \in \sqrt{I}$ allora esiste $n \in \mathbb{N}$ tale che $x^n \in I \subset J$ quindi $x \in \sqrt{J}$. sappiamo già che $IJ \subseteq I \cap J$ quindi $\sqrt{IJ} \subseteq \sqrt{I \cap J}$. Osserviamo inoltre che $I \cap J \subset I$ e $I \cap J \subset J$ quindi $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. In conclusione se

$x \in \sqrt{I} \cap \sqrt{J}$ allora esistono $n, m \in \mathbb{N}$ tale che $x^n \in I$ è $x^m \in J$ quindi $x^{n+m} = x^n x^m \in IJ$ ovvero $x \in \sqrt{IJ}$. Abbiamo perciò dimostrato che $\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$ che implica la tesi.

4) ovvio.

5) Sappiamo che $P \subset \sqrt{P}$. Se $x \in \sqrt{P}$ allora $x^n \in P$ ma per la primalità di P $x \in P$ quindi $\sqrt{P} \subset P$ e si ha la tesi.

6) Dimostro prima che $N = \bigcap_{P \subset A} P$: se $x \in N$ allora esiste $n \in \mathbb{N}$ tale che $x^n = 0$ ma per P primo $0 \in P$ quindi $x^n \in P$ e quindi $x \in P$ per la primalità di P, e con ciò vale che $N \subset \bigcap_{P \subset A} P$. Adesso dimostriamo che $\bigcap_{P \subset A} P \subset N$. Supponiamo per assurdo che se $x \in P$ per ogni P primo allora x non è nilpotente. Considero $\Gamma = \{I \subset A \mid x^n \notin I \ \forall n\}$; intanto osserviamo che $0 \in \Gamma$ dato che x non è nilpotente, inoltre Γ è induttivo infatti se C è una catena allora $J = \bigcup_{I \in C} I \in \Gamma$ è un ideale ed è maggiorante di C; applico allora il lemma di Zorn, quindi esiste un ideale primo $P_0 \in \Gamma$ massimale in Γ. In generale questo P_0 non è massimale nell'anello A, ma è primo; sia $ab \in P_0$, se P_0 non fosse primo allora $a, b \notin P_0$ allora $P_0 \subsetneq (a) + P_0$ e $P_0 \subsetneq (b) + P_0$, per la massimalità di P_0 si ha che $P_0 \subsetneq (a) + P_0$, $P_0 \subsetneq (b) + P_0 \notin \Gamma$ quindi esistono $n, m \in \mathbb{N}$ tale che $x^n \in P_0 \subsetneq (a) + P_0$ e $x^m \in P_0 \subsetneq (b) + P_0$ ma $x^{m+n} = x^n x^m \in ((a) + P_0)((b) + P_0) \subseteq P + (ab) = P$ cioè $x^{n+m} \in P_0$ e quindi $P_0 \notin \Gamma$ assurdo, perciò P_0 primo. Abbiamo quindi trovato un ideale primo che non contiene x che è assurdo dato che x è nell'intersezione di tutti gli ideali primi, di conseguenza x deve essere nilpotente. Dimostro ora che $\sqrt{I} = \bigcap_{J \subset P} P$. Considero l'omomorfismo di proiezione $\pi : A \longrightarrow A/I$ sappiamo che in A/I, $N_{A/I} = \bigcap_{J/I \subset \bar{P}} \bar{P}$ ma per il teorema di corrispondenza si ha che $\sqrt{I} = \pi^{-1}(N_{A/I}) = \bigcap_{J/I \subset \bar{P}} \pi^{-1}(\bar{P}) = \bigcap_{I \subset P} P$.

□

Capitolo 4

Anelli speciali

4.1 Domini euclidei

4.1.1 Definizione : Il dominio A è un *dominio euclideo*, e si dice ED, se esiste una applicazione $d : A/\{0\} \longrightarrow \mathbb{N}$ tale che :

1) $d(x) \leq d(xy)$ per ogni $x, y \in A/\{0\}$.

2) per ogni $x \in A,\ y \in A/\{0\}$ esistono $q, r \in A$ tale che $x = qy+r$ con $r = 0$ oppure $d(r) < d(y)$.

4.1.1 esempio : Sono ED, $(\mathbb{Z}, d)$ con $d(x) = |x|$ è l'applicazione modulo, $(\mathbb{K}[x], d)$ con $d = deg$ è l'applicazione grado di un polinomio, $(\mathbb{Z}[i], d)$ dove $d = ||\cdot||$ è l'applicazione norma.

4.1.1 Preposizione : Sia A un ED, gli elementi di grado minimo di A sono gli elementi di A^*.

Dimostrazione : $\emptyset \neq d(A/\{0\}) \subset \mathbb{N}$ quindi esiste minimo. Sia m il minimo di $d(A/\{0\})$, voglio dire che $d(x) = m \iff x \in A^* \iff (x) = A$.
($\Longrightarrow$) Sia $a \in A$ allora $a = qx + r$ con $d(r) < d(x)$ ma x ha grado minimo quindi $r = 0$ quindi $a \in (x) \Longrightarrow A = (x)$.
($\Longleftarrow$) Sia $x \in A^* \Longrightarrow (x) = A$ quindi per ogni $a \in A$, $a = xy$ con $y \in A$, $d(x) < d(xy) = d(a)$ perciò $d(x) = mind(A/\{0\})$.

□

4.1.1 osservazione : Sia A un ED allora per ogni $a, b \in A$ esiste MCD e lo posso calcolare tramite l'algoritmo di Euclide :
$a = q_0 b + r_0$
$q_o = q_1 r_0 + r_1$

...
$q_n = q_{n+1}r_n + 0$
La successione di resti è decrescente quindi ha termine. A questo punto da $q_{n-1} = q_n r_{n-1} + r_n$ si ha che $MCD = r_n$ e ci ricaviamo che $r_n = q_{n-1} - q_n r_{n-1}$ e si torna indietro sostituendo i vari q_i arrivando a $r_n = as + bt$.

4.1.2 esempio : Consideriamo $\mathbb{Z}[i]$ e $\alpha, \beta \in \mathbb{Z}[i]$ con $\alpha = a + ib$ e $\beta = c + id$. Definisco la distanza $N : \mathbb{Z}[i]/\{0\} \longrightarrow \mathbb{N}$ con $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$ dove $\bar{\alpha} = a - ib$ il coniugato di α. Adesso definisco la divisione euclidea in $\mathbb{Z}[i]$; Voglio dividere α per β, per fare ciò considero il prodotto $q\beta$, al variare di $q \in \mathbb{Z}[i]$ il prodotto genera una griglia formata da quadrati di lato $N(\beta)$, allora α sarà dentro uno di questi quadrati, trovo quindi quel q_0 tale che $q_0\beta$ è uno dei vertici del quadrato che circoscrive α. Allora $\alpha = q_0\beta + r$, devo dimostrare che $N(r) < N(\beta)$, il caso peggiore è che r si trovi al centro del quadrato quindi $N(r) = \frac{N(\beta)\sqrt{2}}{2} < N(\beta)$.

4.2 Prodotto diretto di anelli

4.2.1 osservazione : Siano A, B anelli e $A \times B$ il loro prodotto diretto, allora se $(x, y) \in N_{A\times B}$ allora $x \in N_A$ e $y \in N_B$, inoltre $(A \times B)^* = A^* \times B^*$.

4.2.1 Proposizione : Gli ideali di $A \times B$ sono tutti i prodotti diretti di un ideale di A e un ideale di B.

Dimostrazione : Sia $I \in A$ e $J \in B$ allora $I \times J$ è ideale di $A \times B$ infatti per ogni $(a, b) \in A \times B$ si ha che $(a, b)I \times J = aI \times bJ \subset I \times J$. Sia $\Gamma \subset A \times B$ un ideale; considero $\pi_A : A \times B \longrightarrow A$ l'omomorfismo proiezione su A, siccome π_A è surgettiva $\pi_A(\Gamma)$ è un ideale di A, analogamente per π_B, la proiezione su B, si ha che $\pi_B(\Gamma)$ è un ideale di B. So che vale sempre $\Gamma \subset \pi_A(\Gamma) \times \pi_B(\Gamma)$, voglio l'inclusione opposta; per ogni $(a, b) \in \pi_A(\Gamma) \times \pi_B(\Gamma)$ esistono $x \in A$ e $y \in B$ tale che $(a, y), (x, b) \in \Gamma$ osserviamo adesso che $\Gamma \ni (1, 0)(a, y) + (0, 1)(x, b) = (a, 0) + (0, b) = (a, b)$ e si ha la tesi.

□

4.2.1 esempio : Troviamo gli ideali di $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$. I sottogruppi sono $\{0\}, \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}, \mathbb{Z}/_{2\mathbb{Z}} \times \{0\}, \{0\} \times \mathbb{Z}/_{2\mathbb{Z}}$ che sono ideali e $H = \{(1, 1), (0, 0)\}$ che non è un ideale dato che $(1, 0)(1, 1) = (1, 0) \notin H$.

4.2.1 esercizio : (Da vedere) Determinare gli ideali primi e ideali massimali di $\mathbb{Z} \times \mathbb{Z}$.

soluzione : Gli ideali di $\mathbb{Z} \times \mathbb{Z}$ sono della forma $n\mathbb{Z} \times m\mathbb{Z}$. Gli ideali $\mathbb{Z} \times \{0\}$ e $\{0\} \times \mathbb{Z}$

sono primi ma non massimali, gli ideali $\mathbb{Z} \times p\mathbb{Z}$ e $p\mathbb{Z} \times \mathbb{Z}$ sono massimali, in generale sono tutti primi dato che $\mathbb{Z} \times \mathbb{Z}/_{n\mathbb{Z} \times m\mathbb{Z}} \cong \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$ che è un dominio.

4.3 Domini a ideali principali

4.3.1 Definizione : Il dominio A è un *domino a ideali principali*, e si dice PID, se tutti gli ideali di A sono principali.

4.3.1 Proposizione : Sia A ED allora A è PID.

Dimostrazione : Sia $I \subset A$ un ideale, allora si ah che $I = (0)$ oppure $I \neq (0)$ allora scelgo x_0 elemento di grado minimo in I, osservo che $(x_0) \subset I$ ed inoltre per ogni $a \in I$ si ha che $a = qx_0 + r$ con $d(r) < d(x_0)$ che per la minimalità di x_0 vale che $r = 0$ e quindi $a = qx_0$ ovvero $I \subset (x_0)$ perciò $I = (x_0)$.

□

4.3.2 Preposizione : Esiste MCD dei PID.

Dimostrazione : Siano $a, b \in A$, consideriamo l'ideale (a, b) generato da a, b, siccome A è PID esiste $d \in A$ tale che $(a, b) = (d)$, dico che $d = MCD(a, b)$. Intanto osserviamo che $d|a$ e $d|b$ dato che $a, b \in (d)$, adesso sia c tale che $c|a$ e $c|b$ allora $(d) = (a, b) \subset (c) \Longrightarrow d|c$.

□

4.3.3 Preposizione : Sia A PID. Gli ideali primi di A sono $\{0\}$ e gli ideali massimali.

Dimostrazione : Sia (x) primo con $x \neq 0$ allora x è primo quindi irriducibile perciò (x) è massimale tra gli ideali principali, poichè A è PID allora (x) è massimale.

□

4.3.1 esempio : Consideriamo l'anello $\mathbb{K}[x, y]$ e l'ideale (x), (x) è primo, infatti consideriamo $\gamma : \mathbb{K}[x, y] \longrightarrow \mathbb{K}[y]$ dove $\gamma(f(x, y)) = f(0, y)$ il $Ker(\gamma) = \{f \mid f(o, y) = 0\} = (x)$ quindi per il teorema di omomorfismo $\mathbb{K}[x, y]/_{(x)} = \mathbb{K}[y]$ che un dominio ma non un campo.

4.3.1 Corollario : Sia A PID, se x è irriducibile allora è primo.

Dimostrazione : x irriducibile $\Longrightarrow$ (x) massimale $\Longrightarrow$ (x) primo $\Longrightarrow$ x primo.

□

4.4 Interi di Gauss

Abbiamo visto che l'anello $\mathbb{Z}[i]$ è un ED, detto anello degli interi di Gauss, l'applicazione d che caratterizza gli ED è la norma, $N(a+ib) = a^2 + b^2$.

4.4.1 osservazione : La norma è un'applicazione moltiplicativa, ovvero $N(zw) = N(z)N(w)$, infatti siano $z = a + ib$, $w = c + id$ due interi di Gauss, allora $N((a + ib)(c + id)) = N(ac - bd + i(ad + bc)) = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 - 2acbd + a^2d^2 + b^2c^2 + 2adbc = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2) = N(z)N(w)$.

4.4.2 osservazione : Se la norma di $z \in \mathbb{Z}[i]$ è un numero primo p allora z è primo in $\mathbb{Z}[i]$, infatti sia z tale che $N(z) = p$ allora se non fosse primo, siccome $\mathbb{Z}[i]$ è ED, allora non è irriducibile ed uno dei suoi fattori deve avere norma che divide p, p stesso non può essere quindi deve avere norma 1, ma se $N(z) = 1 \implies z \in \{\pm 1, \pm i\}$ ovvero è invertibile, quindi z è primo.

4.4.1 esempio : 2 non è primo infatti $2 = (1+i)(1-i)$. 3 è primo infatti $N(3) = 9$ quindi se non fosse primo avrebbe dei fattori che hanno norma che divide 9, e per l'osservazione di prima deve avere norma 3 questo fattore, ma $a^2 + b^2 = 3$ non ha soluzione. 5 non è primo infatti $5 = (1 + 2i)(1 - 2i)$.

4.4.1 Proposizione : Sia J un ideale di $\mathbb{Z}[i]$ allora :

1) $J \cap \mathbb{Z} \neq \emptyset$.

2) $\mathbb{Z}[i]/_J$ è finito.

Dimostrazione :

1) Sia $(a + ib) \in J$ allora $J \ni (a + ib)(a - ib) = a^2 + b^2 \in \mathbb{Z}$.

2) Sia $z = a + ib \in \mathbb{Z}[i]$, sappiamo che esiste $n \in \mathbb{Z} \cap J$ quindi $[z]_{\mathbb{Z}[i]/_J} = [r + ir_1]$, $a = qn + r$ e $b = q_1n + r_1$ con $0 \leq r, r_1 \leq n$ di conseguenza $\mathbb{Z}[i]/_J$ ha al più n^2 elementi.

□

4.4.1 esercizio : $J = (1 + 3i) \implies \mathbb{Z}[i]/_J \cong \mathbb{Z}/_{10\mathbb{Z}}$

soluzione : Considero $f : \mathbb{Z}[i]/J \longrightarrow \mathbb{Z}/_{10\mathbb{Z}}$ dove $f(1) = 1$ e $f(i) = 3$ (la scelta dell'immagine di i è dovuta al fatto che in $\mathbb{Z}/_{10\mathbb{Z}}$, $\sqrt{-1} \equiv \sqrt{10 - 1} = \sqrt{9} = 3$), quindi in generale $f(a + ib) = a + 3b$. Per come è stata definita, f è surgettiva, studiamo il Ker; osserviamo che $Ker(f) \supset J$ infatti $f(1 + 3i) = 1 + 3 \cdot 3 = 10 \equiv 0$, adesso se $a + 3b \equiv 0\ (10) \implies a \equiv -3b\ (10)$ quindi esiste h tale che $a = -3b + 10h$ di conseguenza se $z \in Ker(f) \implies z = -3b + 10h + ib =$

$ib(1+3i)+(1-3i)(1+3i)h \in (1+3i) = J$ quindi il $Ker(f) = J$ e per il teorema di omomorfismo si ha la tesi.

4.4.2 Proposizione : $x \in \mathbb{Z}[i]$ ha norma pari $\iff$ x è divisibile per $(1+i)$ (che è l'unico primo di norma pari a meno di unità).

Dimostrazione : ($\Longleftarrow$) : Se $x = (1+i)y \Longrightarrow N(x) = N((1+i))N(y) = 2N(y)$.
($\Longrightarrow$) : Sia $x = m + in$ tale che $m^2 + n^2 \equiv 0\ (2)$ che implica $m \equiv n\ (2)$, cerco u, v tale che $m+in = (1+i)(u+iv) = (u-v)+i(u+v)$ quindi $\begin{cases} u-v=m \\ u+v=n \end{cases} \Longrightarrow \begin{cases} 2u = m+n \\ 2v = n-m \end{cases}$ siccome $m+n$ e $n-m$ sono pari allora basta dividere per 2 ed ho finito.

□

4.4.1 Teorema : (Caratterizzazione dei primi di $\mathbb{Z}[i]$)

1) Se p è primo di $\mathbb{Z}$, $p \equiv 1\ (4) \Longrightarrow\ p = (a+ib)(a-ib)$, dove $(a+ib), (a-ib)$ sono primi distinti di $\mathbb{Z}[i]$ ed in particolare p non è primo di $\mathbb{Z}[i]$.

2) Se p è primo di $\mathbb{Z}$, $p \equiv 3\ (4) \Longrightarrow p$ è primo di $\mathbb{Z}[i]$.

3) Se $z \in \mathbb{Z}[i],\ N(z) = p$, p primo di $\mathbb{Z}$ allora z è primo di $\mathbb{Z}[i]$.

4) Non ci sono altri primi.

Dimostrazione :

1) Innanzi tutto osserviamo che $p = (a+ib)(a-ib) = a^2 + b^2$, se p è somma di due quadrati non è primo. Se $p \equiv 1\ (4)$ allora l'equazione $x^2 \equiv -1\ (p)$ ha soluzione infatti consideriamo il polinomio $t^{p-1} - 1$, ha $p-1$ radici distinte inoltre $t^{p-1} - 1 = (t^{\frac{p-1}{2}} - 1)(t^{\frac{p-1}{2}} + 1)$ perché $p-1$ è pari, ora osserviamo che $t^{\frac{p-1}{2}} + 1$ ha soluzione in $\mathbb{Z}/_{p\mathbb{Z}}$ quindi esiste c tale che $(c^{\frac{p-1}{2}} \equiv -1\ (p)$ quindi $x = c^{\frac{p-1}{4}}$ e $x^2 \equiv -1\ (p)$. Adesso dico che se $a^2 \equiv -1\ (p)$ allora p è somma di due quadrati $a^2 \equiv -1\ (p) \Longrightarrow\ p|a^2+1 = (a+i)(a-i)$, se p fosse primo di $\mathbb{Z}[i] \Longrightarrow\ p|(a+i)$ oppure $p|(a-i)$, impossibile perché coprimi. Allora se p non fosse primo di $\mathbb{Z}[i]$, $p = (s+it)(u+iv)$,ma $p = N(s+it) = N(u+iv)$ quindi $(s-it) = (u+iv)$ di conseguenza $p = s^2 + t^2$ cioè è somma di due quadrati. Per concludere osserviamo che se p primo e somma di due quadrati allora $p \equiv 1\ (4)$ quindi ho dimostrato che $p \equiv 1\ (4) \Longrightarrow\ p$ è somma di due quadrati.

2) Sia p primo tale che $p \equiv 3\ (4)$, supponiamo che $p = (c+id)(e+if)$, se $(a+ib)$ è un fattore proprio di p allora $N(a+ib)|N(p) = p^2$, se fosse p allora $p = a^2 + b^2$ ma per quanto detto nel punto precedente $p \equiv 1\ (4)$ assurdo, se fosse 1 sarebbe invertibile e non va bene, se

fosse p^2 allora $p = a + ib$ assurdo. Quindi è primo di $\mathbb{Z}[i]$.

3) Già visto nella osservazione 4.4.2.

4) Voglio vedere che non ci sono altri primi. Sia $a + ib \in \mathbb{Z}[i]$, se $N(a + ib) = p$ primo di $\mathbb{Z}$ allora è primo di $\mathbb{Z}[i]$, se $N(a+ib)$ non è primo allora esiste p primo in $\mathbb{Z}$ tale che $p|N(a+ib)$ allora $p|(a + ib)(a - ib)$, se p anche in $\mathbb{Z}[i]$ allora $p|a$ e $p|b$ se invece p non è primo in $\mathbb{Z}[i]$ si ha che $p = (q_1 + iq_2)(q_1 - iq_2)$ dove $(q_1 + iq_2), (q_1 - iq_2)$ sono primi distinti. In conclusione $N(a+ib)$ è prima in $\mathbb{Z}[i]$ oppure è divisa da un primo in $\mathbb{Z}[i]$ o ancora divisa da un primo di $\mathbb{Z}$ che ha due fattori primi in $\mathbb{Z}[i]$.

□

4.4.3 Proposizione : Sia $I = (a + ib)$ un ideale di $\mathbb{Z}[i]$ allora l'indice di I è $[\mathbb{Z}[i] : I] = N(a + ib) = a^2 + b^2$.

Dimostrazione : Sia $m = MDC(a, b)$ allora $I = m(\frac{a}{m} + i\frac{b}{m}) \subset (m) \subset \mathbb{Z}[i]$ di conseguenza $[\mathbb{Z}[i] : I] = [\mathbb{Z}[i] : (m)][(m) : I] = m^2[(m) : I]$, quindi ci riduciamo a studiare l'indice di $I = (a+ib)$ con $(a, b) = 1$. Consideriamo $\gamma : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/N$ dove $\gamma(x+iy) = x+cy$ e $N = (a^2+b^2)$ la norma del generatore di I, in particolare $a + cb \equiv 0\ (N)$ quindi $c \equiv -ab^{-1}\ (N)$, e lo posso fare perché $(b, N) = 1$. L'omomorfismo così definito è surgettivo inoltre $Ker(\gamma) \supset I$, vediamo il contenimento opposto; se $x + cy \equiv 0\ (N) \Longrightarrow x \equiv ab^{-1}y\ (N) \Longrightarrow x = a\tilde{b}y + Nh$,$b^{-1} \equiv \tilde{b}\ (N)$, quindi se $Ker(\gamma) \ni z = x + iy \Longrightarrow z = a\tilde{b}y + Nh + iy = a\tilde{b}y + Nh + i(b\tilde{b} - Nh')y = \tilde{b}y(a + ib) + (a + ib)(a - ib)(h + ih') \in I$. Quindi l'indice di I è $N = a^2 + b^2$ che vale anche nel caso di a, b non comprimi infatti ritornando al ragionamento iniziale si ha $[\mathbb{Z}[i] : I] = [\mathbb{Z}[i] : (m)][(m) : I] = m^2(\frac{a}{m}^2 + \frac{b}{m}^2) = a^2 + b^2$.

□

4.4.2 Teorema : (di Pitagora) Le soluzioni della equazione $x^2 + y^2 = z^2$ sono della forma $x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2$ al variare di $u, v \in \mathbb{Z}$.

Dimostrazione : Una soluzione di questa equazione prende il nome di *terna pitagorica*, osserviamo che se un primo p divide due termini fra x, y, z allora divide anche il terzo quindi possiamo dividere e risolvere il problema supponendo che non ci siano fattori primi tra x, y, z trovando quindi soluzioni che prendono il nome di *terne pitagoriche primitive*. Riducendoci così alla ricerca di terne primitive osserviamo che uno tra x, y è pari e z è sempre dispari. Mi sposto in $\mathbb{Z}[i]$ cosicché l'equazione la riscrivo in $(x + iy)(x - iy) = z^2$. Essendo coprimi x, y si ha che $A = MDC(x + iy, x - iy)$ divide $2x = x + iy + x - iy$ e $2y = (x + iy - (x - iy))/i$ quindi $A \in \{1, 2, 1 \pm i\}$, se fosse 2 allora z^2 sarebbe pari, assurdo, se fosse $1 \pm i$ allora $\pm 2i$ dividerebbe z^2 assurdo quindi $A = 1$ quindi $x + iy, x - iy$ sono coprimi in $\mathbb{Z}[i]$. Ora se p è un primo di $\mathbb{Z}[\square]$ che divide z allora $p^2|z^2$ e p^2 divide uno solo tra $x + iy$ e $x - iy$, quindi si ha,

senza perdita di generalità, che $x+iy=ua^2$ con $u,a\in\mathbb{Z}[i]$, u invertibile quindi $u\in\{\pm1,\pm i\}$, e $a=s+it$ qualsiasi, quindi $a^2=s^2-t^2+2ist$ perciò se $u=1\Longrightarrow x=s^2-t^2$ e $y=2st$, se $u=-1\Longrightarrow x=t^2-s^2$ e $y=-2st$, se $u=i\Longrightarrow x=-2st$ e $y=s^2+t^2$, se $u=-i\Longrightarrow x=2st$ e $y=t^2-s^2$. quindi in conclusione siano $u,v\in\mathbb{Z}$ allora le terne pitagoriche primitive sono della forma $x=u^2-v^2,\ y=2uv,\ z=u^2+v^2$ con u,v coprimi ed in generale ogni terna è della forma $x=a(u^2-v^2),\ y=a(2uv),\ z=a(u^2+v^2)$ con $a\in\mathbb{Z}$.

□

4.5 Domini a fattorizzazione unica

4.5.1 Definizione : Il dominio A è un *dominio a fattorizzazione unica*, detto UFD, se per ogni $a\in A/(A^*\cup\{0\})$ a si scrive in modo unico, a meno dell'ordine e di moltiplicazione per invertibili, come prodotto di irriducibili.

4.5.1 osservazione : Esiste sempre l'MCD tra due elementi a,b ma non si può esprimere come combinazione di a e b, cioè non vale l'identità di Bezout.

4.5.1 esempio : Consideriamo l'anello $\mathbb{Z}[x]$, dimostreremo in seguito che è un UFD ma non PID, prendo gli elementi 2 e x, l'$MCD(2,x)=1$ ma l'ideale $(2,x)\neq(1)$ infatti $1=2f+xg$ non ha soluzione con $f,g\in\mathbb{Z}[x]$.

4.5.1 Teorema : (Caratterizzazione degli UFD) Sia A un dominio, sono fatti equivalenti :

1) A è UFD.

2) Ogni irriducibile è primo e ogni catena discendente di divisibilità è stazionaria, cioè se $\{a_n\}_{n\geq0}$ con $a_{n+1}|a_n$ per ogni n allora esiste un n_0 tale che per ogni $n\geq n_0$ si ha che $a_n\sim a_{n_0}$ (detta condizione della catena discendente).

Dimostrazione : 2) $\Longrightarrow$ 1) (la condizione della catena ascendente implica l'esistenza di una fattorizzazione). Procedo per assurdo, sia $x\in A/(A^*\cup\{0\})$, supponiamo che x non si fattorizzi quindi non è irriducibile allora posso scrivere $x=y_0z_0$ dove y_0,z_0 sono elementi di $A/(A^*\cup\{0\})$ non irriducibili, in particolare $y_0=y_1z_1$ dove y_1,z_1 sono elementi di $A/(A^*\cup\{0\})$ non irriducibili, è procedendo così otteniamo delle catena discendente di divisibilità $y_{n+1}|y_n$, ma sappiamo essere stazionarie quindi ad un certo punto non posso più ridurre i fattori ottenendo così una fattorizzazione di x che è assurdo per ipotesi quindi x possiede una fattorizzazione. Dimostriamo ora l'unicità della fattorizzazione; (ogni irriducibile è primo implica l'unicità della fattorizzazione) per ogni $x\in A/(A^*\cup\{0\})$ consideriamo $l_x=min(\{s\mid p_1\cdots p_s,\ p_i \text{ irriducibile}\})$,

che sarebbe il minimo delle lunghezze delle possibili fattorizzazioni di x, e procedo per induzione. Se $l_x = 1$ allora x è irriducibile, allora suppongo che la fattorizzazione sia unica per $l_x < n$ e vediamo per n, sia quindi $x = p_1 \cdots p_n = q_1 \cdots q_s$ con p_i, q_i irriducibili, ora p_n è irriducibile quindi primo perciò $p_n | q_1 \cdots q_s$, supponiamo senza perdita di generalità che $p_n | q_s$ quindi $p_s = q_n u$ siccome q_s è irriducibile allora u è invertibile, p_n non può esserlo per ipotesi, quindi $p_n = q_s$ ed in particolare $x = p_1 \cdots p_n = q_1 \cdots q_s \Longrightarrow p_1 \cdots p_{n-1} = q_1 \cdots p_{s-1}$ e si conclude per ipotesi induttiva.

1) $\Longrightarrow$ 2) Osservo che se $x|y$ allora $\{$fattorizzazione di $x\} \subseteq \{$fattorizzazione di $y\}$ quindi consideriamo una catena discendente di divisibilità $\{a_n\}_{n\geq 0}$ con $a_{n+1}|a_n$, per quanto detto prima si ha che $\cdots \subseteq \{$fattori di $a_1\} \subseteq \{$fattori di $a_0\}$, adesso sia $N_k = \#\{$insieme di fattori a_k contati con molteplicità$\}$, N_k è una catena discendete di naturali quindi è stazionaria ovvero esiste m_0 tale che $N_n = N_{m_0}$ quindi in particolare $a_n \sim a_0$ per ogni $n > m_0$ ovvero la catena di ideali è stazionaria. Adesso se x è irriducibile e $x|ab$ si ha che $ab = xy$ quindi considerando i fattori irriducibili $a_1 \cdots a_s b_1 \cdots b_r = x y_1 \cdots y_t$ allora $x \sim a_i | a$ quindi $x|a$ oppure $x \sim b_i | b$ quindi $x|b$ perciò x è primo.

□

4.5.2 osservazione : $a|b \longrightarrow (b) \subseteq (a)$ quindi $\{a_n\}_{n\geq 0}$ con $a_{n+1}|a_n$ per ogni n allora vale $(a_{n+1}) \subseteq (a - n)$ per ogni n, per ciò la condizione della catena discendente è equivalente a dire che ogni catene ascendente di ideali principali è stazionaria, detta condizione della catena ascendente.

4.5.2 Definizione : Un anello A si dice *noetheriano* se A verifica la condizione della catena ascendente.

4.5.1 Corollario : $PID \Longrightarrow UFD$.

Dimostrazione : Dimostrare che un PID è un UFD è uguale a dimostrare, per il teorema precedente, che ogni irriducibile è primo e vale la condizione della catena ascendente. Già abbiamo dimostrato che in un PID ogni irriducibile è primo resta ra dimostrare la condizione. Consideriamo quindi una catena ascendente di ideali principali $(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots$, sia allora $I = \bigcup_{i\geq 0} (a_i)$, questo è un ideale di A e siccome A è PID esiste a tale che $I = (a)$ allora esiste un n_0 tale che $a \in (a_{n_0})$, quindi $(a_n) \subseteq (a)$ per ogni n e $(a_{n_0}) = (a)$ per ogni $n \geq n_0$ quindi la catena è stazionaria è con ciò ho la tesi.

□

4.5.2 esempio : (anello non UFD che non verifica la condizione della catena discendente di visibilità) Sia $A = \mathbb{K}[\{\sqrt[p]{x}\}_{n\geq 1}]$ dove $\mathbb{K}$ è un campo, questo non è UFD perché la catena $\{\sqrt[2^n]{x}\}_{n\geq 1}$ è discendente infinita. É interessante notare che invece l'anello $\mathbb{K}[x_1, x_2, \cdots]$, infinite

variabili, è un UFD.

4.5.3 esempio : (anello non UFD in cui gli irriducibili non sono primi) Sia $A = \mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b \mid a, b \in \mathbb{Z}\}$, è un anello dove è definita una norma $N(a + \sqrt{-5}b) = (a + \sqrt{-5}b)(a - \sqrt{-5}b) = a^2 + 5b^2$, notiamo che $N(1 + \sqrt{-5}) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 + 5 = 6 = 2 \cdot 3$, mostro che 2 è irriducibile ma non primo; supponiamo che non sia irriducibile, allora $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ quindi la norma $4 = (a^2 + 5b^2)(c^2 + 5d^2)$ le possibilità sono $a = \pm 1, b = 0, c = \pm 1, d = 0$ quindi 2 è irriducibile ma non è primo infatti $2|(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ ma $2 \not| (1 \pm \sqrt{-5})$ perché il risultato della divisione sarebbe $(\frac{1}{2} \pm \frac{\sqrt{-5}}{2}) \notin \mathbb{Z}[\sqrt{-5}]$.

4.5.3 Definizione : Sia A UFD, $f \in A[x]$, $f = \sum_{i=0}^{n} a_i x^i$. Allora $c(f) = MCD\{a_0, \cdots, a_n\}$ è detto *contenuto di* f. $c(f)$ è definito a meno di associati e $f = c(f)f'$ dove $c(f') = 1$.

4.5.4 Definizione : f si dice *primitivo* se $c(f) = 1$.

4.5.1 Lemma : (di Gauss) Sia A un UFD allora :

1) Se $f, g \in A[x]$ primitivi allora fg primitivo.

2) $c(fg) = c(f)c(g)$.

3) Se $f, g \in A[x]$ con $c(f) = 1$ e $f|g$ in $\mathbb{K}[x]$ dove $\mathbb{K} = Q(A)$ allora $f|g$ in $A[x]$.

4) Se $f \in A[x]$ e $f = gh$ in $\mathbb{K}[x]$ allora esistono $g_1, h_1 \in A[x]$ tale che $g_1 \sim g$ e $h_1 \sim h$ in $\mathbb{K}[x]$.

4.5.1 Proposizione : (elementi irriducibili di di $A[x]$) Sia A un UFD allora $f \in A[x]$ è irriducibile $\iff$ se f è irriducibile in A oppure f è irriducibile in $\mathbb{K}[x]$ con $c(f) = 1$.

Dimostrazione :

f costante : devo dimostrare che f è irriducibile in $A[x] \iff f$ irriducibile in A. ($\Longrightarrow$) Sia $f = ab$ in A. Allora poiché f è irriducibile in $A[x] \Longrightarrow a \vee b \in A[x]^* = A^* \Longrightarrow f$ irriducibile in A (sia no $f, g \in A[x]^*$ allora $fg = 1 \Longrightarrow deg(fg) = deg(f) + deg(g) = 0 \Longrightarrow f, g \in A^*$ inoltre $A^* \subset A[x]^*$ quindi $A^* = A[x]^*$). ($\Longleftarrow$) Sia $f = a(x)b(x) \in A[x]$ per questioni di grado $a(x) = a, b(x) = b \in A$ e per l'irriducibilità di f in A si ha che $a \vee b \in A^* = A[x]^*$ quindi f è irriducibile in $A[x]$.

$deg(f) \geq 1$: devo dimostrare che f irriducibile in $A[x] \iff c(f) = 1$ e f irriducibile in $\mathbb{K}[x]$. ($\Longrightarrow$) Sia $f = c(f)f'$ in $A[x]$, $deg(f') = deg(f) \geq 1 \Longrightarrow c(f) = 1$ a meno di moltipli-

cazione per invertibili. Se fosse $f = gh$ in $\mathbb{K}[x]$ con $deg(g) \geq 1$ e $deg(h) \geq 1$ (che è come dire che f, g sono non invertibili) allora per il lemma di Gauss $f = g'h'$ con $deg(g') = deg(g) \geq 1$ e $deg(h') = deg(h) \geq 1$ in $A[x]$ ovvero è riducibile in $A[x]$ assurdo quindi è irriducibile in $\mathbb{K}[x]$. ($\Longleftarrow$) Sia f con $c(f) = 1$ e irriducibile in $\mathbb{K}[x]$. Se $f = g(x)h(x)$ in $A[x]$ avrei che $deg(g) \geq 1$ e $deg(h) \geq 1$, poiché $c(f) = 1$ non possono esserci fattori costanti in f allora f si riduce anche in $\mathbb{K}[x]$ perché g, h non essendo costanti sono non invertibili in $\mathbb{K}[x]$, assurdo, quindi è irriducibile in $A[x]$.

□

4.5.3 osservazione : $f|g$ in $A[x] \iff c(f) = c(g)$ e $f'|g'$ infatti $f|g \iff g = fh$ in $A[x] \iff c(g) = c(f)c(h)$ e $c(g)g' = c(f)f'c(h)h' \iff c(f)|c(g)\ f'|g'$.

4.5.2 Teorema : $A\ UFD \Longrightarrow\ A[x]\ UFD$

Dimostrazione : Sappiamo che $A[x]$ è un dominio e $A[x]^* = A^*$, per dimostrare che è UFD usiamo la caratterizzazione del teorema 4.5.1. (Ogni irriducibile è primo) Sia $f \in A[x]$ irriducibile allora per la proposizione 4.5.1 è irriducibile pure in $\mathbb{K}[x]$ e primitivo, siccome $\mathbb{K}[x]$ è ED allora f è primo in $\mathbb{K}[x]$. Supponiamo che $f|gh$ in $A[x]$ allora per il lemma di Gauss $f|gh$ in $\mathbb{K}[x]$ ma essendo primo in $\mathbb{K}[x]$ allora $f|g$ oppure $f|h$ ma siccome f è primitivo, per il lemma di Gauss $f|g$ oppure $f|h$ in $A[x]$ quindi f è primo in $A[x]$. (Ogni catena discendente di divisibilità è stazionaria) Sia $\{f_n\}_{n\geq 1},\ f_{n+1}|f_n$ in $A[x]$, considero la successione dei contenuti $\{c(f_n)\}_{n\geq 1}$, so per l'osservazione 4.5.3 che $c(f_{n+1})|c(f_n)$ e $f'_{n+1}|f'_n$ per ogni n, essendo A un UFD $\{c(f_n)\}_{n\geq 1}$ è stazionaria quindi esiste n_0 tale che $c(f_n) \sim c(f_{n_0})$ per ogni $n \geq n_0$ inoltre essendo $\mathbb{K}[x]$ UFD la successione $\{f'_n\}_{n\geq 1}$ è stazionaria quindi esiste n_1 tale che $f'_n \sim f'_{n_1}$ per ogni $n \geq n_1$ in $\mathbb{K}[x]$. Adesso ho che in $A[x]$ $b_n f'_n = a_n f'_{n_1}$ con $a_n, b_n \in A$ e uguagliando i contenuti si ha che $b_n \cancel{c(f'_n)} = a_n \cancel{c(f_{n_1})}\epsilon$, con $\epsilon \in A^*$ quindi $a_n|b_n$ e quindi $f_n \sim f_{n_1}$ in $A[x]$. In conclusione se prendo $n_2 = max\{n_0, n_1\}$ ho che per ogni $n \geq n_2$, $c(f_n) \sim c(f_{n_2})$ e $f'_n \sim f'_{n_2}$ quindi per ogni $n \geq n_2$ si ha che $f_n \sim f_{n_2}$ in $A[x]$ quindi la catena è stazionaria.

□

4.5.2 Corollario : $A\ UFD \Longrightarrow\ A[x_1, \cdots, x_n]\ UFD$

Dimostrazione : Si procede per induzione; $A[x]$ è UFD per il teorema precedente. Ora consideriamo l'anello $A[x_1, \cdots, x_n] = A[x_1, \cdots .x_{n-1}][x_n]$, so che per il passo induttivo $A[x_1, \cdots .x_{n-1}]$ è UFD quindi per il teorema precedente $A[x_1, \cdots, x_n] = A[x_1, \cdots .x_{n-1}][x_n]$ è UFD.

□

4.5.4 osservazione : $\mathbb{K}[x, y]$ è UFD ma non è PID.

4.5.3 Teorema : (Criterio di Eisenstein) Sia A un UFD, $f(x) \in A[x]$ e f primitivo dove

$f = \sum_{i=0}^{n} a_i x^i$ e sia p primo di A, se :

1) $p \not| a_n$

2) $p | a_i$ per ogni $i = 0, \cdots, n-1$

3) $p^2 \not| a_0$

allora f è irriducibile in $A[x]$ (anche in $\mathbb{K}[x]$).(Dimostrazione vuoi farla Da vedere)

4.5.4 esempio : Sia $A = \mathbb{K}[x]$ e consideriamo $f(t) = t^n - x$ in $A[t]$, so che x è primo in A quindi per Eisenstein $f(t)$ è irriducibile.

4.5.1 esercizio :(Da vedere)

1) $A[\{x_i\}_{i\in\mathbb{N}}]$ non è noetheriano.

2) $A[\{x_i\}_{i\in\mathbb{N}}]$ è UFD.

soluzione :

1) Considero la catena $\{I_n\}_{n\geq 1}$ dove $I_n = \{x_1, \cdots, x_n\}$, questa è ascendente ma non stazionaria.

2) Siano $f, g \in A[\{x_i\}_{i\in\mathbb{N}}]$ tale che $fg = 0$ e $deg(f) = n$, $deg(g) = m$ allora $fg = 0$ anche in $A[x_1, \cdots, x_{n+m}]$ ma questo è un dominio quindi $f = 0 \vee g = 0$ quindi $A[\{x_i\}_{i\in\mathbb{N}}]$ è un dominio. Sia $f \in A[\{x_i\}_{i\in\mathbb{N}}]$ irriducibile con $deg(f) = n$ e supponiamo $f = gh$, allora f irriducibile e $f = gh$ anche in $A[x_1, \cdots, x_n]$ che è UFD quindi $f|g$ oppure $f|h$ quindi f è primo in $A[\{x_i\}_{i\in\mathbb{N}}]$. Sia $\{f_n\}_{n\geq 1}$ una catena discendete di divisibilità quindi $f_{n+1}|f_n$, in particolare $f_0 \in A[x_1, \cdots, x_{def(f_0)}]$ e siccome $f_0 = f_{n+1}h_{n+1}$ allora $\{f_n\}_{n\geq 1} \subset A[x_1, \cdots, x_{def(f_0)}]$ che è UFD quindi $\{f_n\}_{n\geq 1}$ è stazionaria e $A[\{x_i\}_{i\in\mathbb{N}}]$ è UFD.

4.6 Serie formali

4.6.1 Definizione : Sia $\mathbb{F}$ un campo allora definiamo $\mathbb{F}[[x]] = \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in \mathbb{F}\}$ che è *l'insieme delle serie formali a coefficienti in* $\mathbb{F}$ (non sono altro che polinomi di grado infinito).

4.6.1 Proposizione :

1) $f \in \mathbb{F}[[x]]$ è invertibile $\iff$ $a_0 \neq 0$.

2) (x) è l'unico ideale massimale.

3) $\mathbb{F}[[x]]$ è un anello euclideo e ogni ideale è potenza di (x).

Dimostrazione :

1) ($\Longrightarrow$) Se f invertibile allora esiste $g \in \mathbb{F}[[x]]$ tale che $fg = 1$, con $f = \sum_{i\geq 0} a_i x^i$ e $g = \sum_{i\geq 0} b_i x^i$, quindi $fg = a_0b_0 + (a_0b_1 + a_1b_0)x + \sum_{i\geq 2}(\sum_{k\geq 0}^{i} a_{i-k}b_k)x^i = 1$ in particolare $a_0b_0 = 1$ siccome $\mathbb{F}$ è un campo $a_0 \neq 0$.
($\Longleftarrow$) Posso esprimere $f \in \mathbb{F}[[x]]$ come $f = a_0 + xg$ con $g \in \mathbb{F}[[x]]$ e $a_0 \neq 0$, noto allora che $f^{-1} = \sum_{i=0}^{\infty} a_0^{i+1}(xg)^i$ infatti se $f_k^{-1} = \sum_{i=0}^{k} a_0^{i+1}(xg)^i$allora $f \circ f_k^{-1} = 1 + (-a_0^{-1}xg)^k + 1$.

2) Per il punto precedente un elemento per essere invertibile deve avere termine noto non 0, quindi un ideale proprio ha elementi di termine noto 0 e sono tutti contenuti in (x).

3) Sappiamo che ogni ideale è contenuto in uno massimale ma siccome l'unico ideale massimale è (x) ogni ideale è potenza di questo. Definiamo adesso $\partial_f = grado\ di\ f = max\{n \mid a_k = 0\ \forall\ k \leq n\}$ allora $\partial(fg) = \partial(f) + \partial(g) \geq \partial(g)$ inoltre sia $0 \neq f = x^{\partial(f)}u$ con $u \in (\mathbb{F}[[x]])^*$ allora $f : g = x^{\partial(f)}u_f : x^{\partial(g)}u_g = x^{\partial(f)-\partial(g)}u_f u_g^{-1}$ se $\partial(f) > \partial(g)$. In conclusione ∂_f così definita ci assicura che $\mathbb{F}[[x]]$ è ED.

□

4.7 Esercizi

4.7.1 esercizio : Studio di $A[x]$, l'anello dei polinomi a coefficienti in A, dove A è un anello commutativo.

soluzione : Facciamo delle prime considerazioni; $u \in A^*$ e x nilpotente allora $x + u$ è invertibile, infatti se x nilpotente implica che per un opportuno $n \in \mathbb{N}$, $x^n = 0$ quindi $1 = 1 + x^n = (1 + x)(x^n - x^{n-1} + \cdots + x^2 - x + 1)$ ovvero $1 + x$ è invertibile. Adesso consideriamo $u + x = u(1 + xu^{-1})$, si osserva che xu^{-1} è nilpotente e per l'osservazione di prima $1 + xu^{-1}$ è invertibile quindi anche $u(1 + xu^{-1}) = u + x$ è invertibile.

chi sono i nilpotenti di $A[x]$?

$f = a_0 + a_1x + \cdots + a_kx^k$ nilpotente con $a_k \neq 0$ se e solo se tutti i coefficienti di f sono nilpotenti, infatti l'insieme degli elementi nilpotenti in $A[x]$ è un ideale se tutti i coefficienti sono nilpotenti per la proprietà di assorbimento lo è anche f, viceversa,procedendo per induzione sul grado di f, se f è nilpotente allora per un certo m si ha che $f^m = 0$. Notiamo che a_k^m è il coefficiente del monomio di grado più alto di f^m e quindi deve essere 0 ovvero $a_k^m = 0$ quindi a_k è nilpotente allora anche $f - a_kx^k$ è nilpotente ed è un polinomio di grado $k-1$ e per induzione tutti i suoi coefficienti sono nilpotenti e si ha la tesi.

chi sono gli invertibili ?

Se $p(x)$ è invertibile allora esiste $q(x)$ tale che $p(x)q(x) = 1$, supponiamo allora che $p(x) = \sum_{i=0}^{n} a_ix^i$ e $q(x) = \sum_{i=0}^{m} b_ix^i$ dove $a_1, \cdots, a_n, b_1, \cdots, b_m \in A$ allora si ha che $p(x)q(x) = \sum_{k=0}^{n+m} (\sum_{i=0}^{k} a_ib_{k-i})x^k = 1$ dove $b_i = 0$ se $i > m$ e $a_i = 0$ se $i > n$. Quindi si ha che :

$$\begin{cases} a_0b_0 = 1 \\ a_1b_0 + b_1a_0 = 0 \\ \cdots \\ \sum_{i=0}^{k} a_ib_{k-i} \\ \cdots \\ a_nb_m = 0 \end{cases}$$

Osserviamo che una condizione è $a_{n-1}b_m + a_nb_{m-1} = 0$, se moltiplichiamo a_n a questa otteniamo $a_{n-1}(a_nb_m) + (a_n)^2b_{m-1} = (a_n)^2b_{m-1} = 0$ dato l'ultima condizione dice che $a_nb_m = 0$, quella precedente ancora è $a_{n-2}b_m + a_{n-1}b_{m-1} + a_nb_{m-2}$ e moltiplicando a_n^2 si ottiene che $a_n^3b_{m-2} = 0$ e continuando così si ottiene $a_n^mb_0 = 0$ e moltiplicando per a_0 e usando la prima relazione si ha che $a_n^m(a_0b_0) = a_n^m = 0$ quindi a_n è nilpotente. Sappiamo che $p(x) - a_nx^n$ è invertibile per la considerazione iniziale quindi ri-itero il ragionamento su questo nuovo polinomio e ottengo che a_{n-1} è nilpotente e continuo arrivando alla conclusione che se $p(x)$ è invertibile allora è della forma $p(x) = u + v$ dove $u \in (A[x])^*)A^*$ e $v \in N[x]$ che è l'insieme dei nilpotenti di $A[x]$.

chi sono i divisori di zero ?

Sia $p(x) = \sum_{i=0}^{n} a_ix^i$ un divisore di 0, prendo $q(x) = \sum_{i=0}^{m} b_ix^i \in A[x] \neq 0$, con $b_0 \neq 0$, di gra-

do minimo possibile e tale che $p(x)q(x) = 0$. Può accadere che :

$$\begin{cases} a_0q(x) = 0 \\ a_1q(x) = 0 \\ \dots \\ a_nq(x) = 0 \end{cases} \Longrightarrow \begin{cases} a_0b_0 = 0 \\ a_1b_0 = 0 \\ \dots \\ a_nb_0 = 0 \end{cases}$$

quindi tutti gli a_i sono divisori di 0; oppure esiste un a_j tale che $a_jq(x) \neq 0$ allora prendo il più altro N tale che $a_Nq(x) \neq 0$, quindi $p(x)q(x) = (\sum_{i=0}^{N} a_ix^i + \sum_{i=N+1}^{n} a_ix^i)q(x) = (\sum_{i=0}^{N} a_ix^i)((\sum_{i=0}^{m} b_ix^i) = 0$, a_Nb_m è il coefficiente di x^{N+m} che è il termine di grado più alto, ma per ipotesi $a_nq(x) \neq 0$ quindi l'unico caso e che $m = 0$ cioè $q(x) = b_0$ tutti gli a_i sono divisori di 0 in A ed esiste b_0 tale che $b_0a_i = 0$ per ogni i.

4.7.2 esercizio : (Da vedere) Gli ideali di $M_{n\times n}(\mathbb{K})$.

soluzione : Sia $\mathbb{K}$ un campo. Consideriamo l'anello non commutativo $M_{n\times n}(\mathbb{K}) = R$. mi chiedo chi siano gli ideali di R. Ricordiamo che I è un ideale destro di R se per ogni $A \in I$ e $B \in R$ si ha $AB \in I$. Sia $V \in \mathbb{K}^n$ dico che $I_V = \{A \in R \mid Imm(A \subset V)\}$ è un ideale destro e che tutti gli ideali destri di R sono di questa forma. Osserviamo innanzi tutto che I_V è un sottogruppo e che in generale $Imm(AB) \subset Imm(A) \subset V$ quindi I_V è ideale, resta da dimostrare che un qualsiasi ideale destro lo possiamo esprimere in questa maniera. Sia I un ideale destro di R, considero $V =< \bigcup_{A\in I} Imm(A) >$ il sottogruppo generato dall'unione delle immagini di ogni elemento dell'ideale. Voglio dire che $I = I_V$; ovviamente per costruzione $I \subset I_V$. Considero adesso una base di V $e_1, \cdots, e_k$ ed esisteranno quindi della $A_i \in I$ tale che $e_i \in Imm(A_i)$ ovvero esistono dei v_i tale che $A_i(v_i) = e_i$. Prendo $C \in I_V$ e suppongo senza perdita di generalità che per certi i $C(e_i) = v \in V$ e per certi j $C(e_j) = 0$ allora $C = A_1B_1 + \cdots + A_kB_k$ dove $B_i(e_j) = a_jv_j$ se i=j e $B_i(e_j) = 0$ se $i \neq j$ quindi per la proprietà di assorbimento $C \in I$ e si ha la tesi. Si dimostra in modo analogo che gli ideali sinistri sono tutti della forma $I_W = \{A \in R \mid W \subset Ker(A)\}$. (ai voglia di dimostrarlo? $W = \bigcap_{A\in I}$)

4.7.1 osservazione : $\mathbb{K}/_{(f(x))}$ ogni classe del tipo $r(x) + (f(x))$, con $r(x) = 0$ oppure $deg(r(x)) < deg(f(x))$, è divisore di 0 se e solo se $(r(x), f(x) \neq 1$, ed è invertibile se e solo se $(r(x), f(x) = 1$.

4.7.3 esercizio : Sia $f : A \longrightarrow B$ un omomorfismo surgettivo :

1) M massimale in A allora $f(M)$ massimale in B.

2) N massimale in B allora $f^{-1}(N)$ massimale in A.

3) É vero che se N massimale in B allora $N = f(M)$ con M massimale in A?

4) É vero che per ogni M massimale in A, $M = f^{-1}(N)$ con N massimale in un opportuno B?

soluzione :

1) Falso, infatti consideriamo $\pi\mathbb{Z} \longrightarrow \mathbb{Z}/_{2\mathbb{Z}}$, l'ideale ($3\mathbb{Z}$ di $\mathbb{Z}$ è massimale ma $\pi(3\mathbb{Z}) = \mathbb{Z}/_{2\mathbb{Z}}$ che non è massimale.

2) Vero, consideriamo :

$$A \xrightarrow{f} B \longrightarrow B/N$$
$$\gamma$$

il $Ker(\gamma) = \{a \mid f(a) \in N\} = f^{-1}(N)$ quindi $A/_{f^{-1}(N)} \cong B/N$ perciò se N massimale in B allora B/N è un campo quindi anche $A/_{f^{-1}(N)}$ è un campo perciò $f^{-1}(N)$ è massimale.

3) Vero, infatti per il punto 2) se N è massimale in B allora $f^{-1}(N)$ è massimale in A quindi siccome $N = Id_B(N) = f \circ f^{-1}(N) = f(f^{-1}(N))$ basta quindi porre $M = f^{-1}(N)$ e si ha che $N = f(M)$ con N massimale in B e M massimale in A.

4) Vero, basta prendere $B = A$ e $f = Id_A$.

4.7.4 esercizio : Siano A, B anelli finiti e $f : A \longrightarrow B$ un omomorfismo tale che $f(1_A) = 1_B$ allora :

1) f induce un omomorfismo di gruppi $f^* : A^* \longrightarrow B^*$.

2) $|Ker(f^*)| \leq |Ker(f)|$.

3) se A ha un unico ideale massimale allora $|Ker(f^*)| = |Ker(f)|$.

soluzione :

1) Sia $a \in A^*$ allora esiste $b \in A$ tale che $ab = 1$ quindi $1_B = f(1_A) = f(ab) = f(a)f(b)$

perciò $f(a) \in B^*$. Quindi considero $f^* : A^* \longrightarrow B^*$ con $f^*(a) = f(a)$ e questo è l'omomorfismo cercato.

2) $Ker(f) = \{a \in A \mid f(a) = 0_B\}$ e $Ker(f^*) = \{a \in A^* \mid f(a) = 1_B\}$, considero $\gamma : A^* \longrightarrow A$ dove $\gamma(a) = a - 1$, questa è una mappa iniettiva, inoltre se $a \in Ker(f^*)$ allora $\gamma(a) = a - 1 \in Ker(f)$ infatti $f(a-1) = f(a) - 1 = 1 - 1 = 0$.

3) (Da vedere) Osserviamo innanzi tutto che $A^* = A/M$ dove M è ideale massimale. Consideriamo $\gamma : Ker(f^*) \longrightarrow Ker(f)$ dove $\gamma(a) = a - 1$, prendo $b \in Ker(f)$ e vedo che $f(b+1) = f(b) + 1 = 1$, (in generale $b + 1 \notin A^*$) ma se A è ha un unico ideale massimale e sapendo che ogni ideale è contenuto in uno massimale allora tutti gli ideali sono contenuti in M quindi $b \in Ker(f) \subset M$ e $b+1 \in ker(f^*) \subset M$ assurdo perché se $b, b+1 \in M \Longrightarrow 1 \in M$ quindi...

4.7.2 osservazione : Un anello A che ha un unico ideale massimale è detto *locale*.

4.7.5 esercizio : (secondo compitino 2011) Siano $\xi_5, \xi_8 \in \mathbb{C}$ radici dell'unità.

1) Determinare $I \subset \mathbb{Z}[x]$ tale che $\mathbb{Z}[\xi_5] \cong \mathbb{Z}/I$.

2) Dimostrare che $\mathbb{Z}[\xi_5]/_{(11)}$ non è un campo.

3) $\mathbb{Z}[\xi_5]/_{(11)} \ncong \mathbb{Z}[\xi_8]/_{(11)}$.

soluzione :

1) (Per questo c'è un metodo standard) Consideriamo $\gamma : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\xi_5]$ l'omomorfismo di sostituzione dove $\gamma(f(x)) = f(\xi_5)$, questo è surgettivo, allora $I = Ker(\gamma) = \{p(x) \mid p(\xi_5) = 0\}$. Osservo che $\mu = x^4 + x^3 + x^2 + x + 1 \in I$ quindi $(\mu) \subset I$ ora sia $p \in I$ quindi $p(\xi_5) = 0$ allora $\mu | p$ in $\mathbb{Q}$ ma μ è primitivo è sta in $\mathbb{Z}[x]$ quindi per il lemma di Gauss $\mu | p$ anche in $\mathbb{Z}[x]$ quindi $I = (\mu)$.

2) Per il punto precedente so che $\mathbb{Z}[\xi_5] \cong \mathbb{Z}[x]/_{(\mu)}$ quindi $\mathbb{Z}[\xi_5]/_{(11)} \cong (\mathbb{Z}[x]/_{(\mu)})/_{(11)} \cong \mathbb{Z}[x]/_{(\mu,11)} \cong \mathbb{Z}/_{11\mathbb{Z}}[x]/_{(\bar{\mu})}$. Gli isomorfismi di prima sono giustificati dall'omomorfismo $\tau : \mathbb{Z}[x]/_{(\mu)} \longrightarrow \mathbb{Z}[x]/_{(\mu,11)}$ il $Ker(\tau) = \frac{(\mu,11)}{(\mu)} = (11)$. Quindi ci riduciamo a studiare $\mathbb{F}[x]/_{(\bar{\mu})}$ dove $\bar{\mu} = x^4 + x^3 + x^2 + x + 1$. Osserviamo che $\xi_p \in \mathbb{F}_q \iff x^p - 1 \equiv 0\ (q) \iff p \equiv 0\ (q-1)$ inoltre se $(f, g) = 1$ allora per il teorema cinese $\mathbb{K}[x]/_{(f(x)g(x)} \cong \mathbb{K}[x]/_{(f(x))} \times \mathbb{K}[x]/_{(g(x))}$. Quindi μ e riducibile in $\mathbb{F}_{11}$ perché $5|11 - 1$ quindi $\xi_5 \in \mathbb{F}_{11}$, perciò il polinomio minimo di ξ_5 ha grado 1 e μ si fattorizza in 4 polinomi di grado 1 coprimi, per il criterio della derivata, perciò segue che $\mathbb{F}_{11}[x]/_{\mu} \cong \mathbb{F}_{11}/_{(p_1)} \times \mathbb{F}_{11}/_{(p_2)} \times \mathbb{F}_{11}/_{(p_3)} \times \mathbb{F}_{11}/_{(p_4)} \cong \mathbb{F}_{11}^4$ che non è un campo.

3) (Da vedere) $8 \not| 11-1$ quindi $\xi_8 \notin \mathbb{F}_{11}$ quindi il polinomio minimo in $\mathbb{Z}[x]$ è lo stesso che in $\mathbb{F}_{11}[x]$ ed è irriducibile, quindi $\mathbb{Z}[\xi_8]/_{(11)} \cong \mathbb{F}_{11}[\xi_8]$ chè un campo è non può essere isomorfo a $\mathbb{F}_{11}^4$ che non lo è.

4.7.6 esercizio : Trovare le soluzioni intere di $x^2 - 2y^2 = \pm 1$.

soluzione : Mettiamoci in $\mathbb{Z}[\sqrt{2}] = A$. In questo anello posso definire un coniugio, dato $u = a + \sqrt{2}b \Longrightarrow \bar{u} = a - \sqrt{2}b$ ed anche una norma $N(u) = u\bar{u} = a^2 - 2b^2 \in \mathbb{Z}$. Osserviamo che la norma così definita è moltiplicativa, $N(uv) = N(u)N(v)$ (facile verifica), allora $A^* = \{u \in A \mid N(u) = \pm 1\}$ infatti vale sicuramente $\supset$ e se $u \in A^*$ allora $N(u) \in \mathbb{Z}^* = \pm 1$ quindi si ha che x, y sono soluzioni $x^2 - 2y^2 = \pm 1 \Longleftrightarrow u = x + \sqrt{2}y \in A^*$, quindi ci resta da capire chi è A^*; dico che $A^* \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}$. Consideriamo la mappa $\mu : \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z} \longrightarrow < \gamma >$ tale che $\mu((\pm 1, n)) = \pm(\gamma)^n$ dove $\gamma = 1 + \sqrt{2} \in A^*$, μ è un ovvio omomorfismo di gruppo. Adesso consideriamo π_1, π_2 omomorfismi di proiezione tale che $\pi_1(a + \sqrt{2}b) = a$ e $\pi_2(a + \sqrt{2}b) = b$, osserviamo che $\pi_1(\gamma(a + \sqrt{2})b) = a + 2b$ e $\pi_2(\gamma(a + \sqrt{2})b) = a + b$ quindi $\pi_1(\gamma u) = \pi_1(u) + 2\pi_2(u)$ e se $\pi_1(u) > 0$ e $\pi_2(u) > 0 \Longrightarrow \pi_1(\gamma u) > \pi_1(u)$ perciò se impongo $u = \gamma$, dato che $\pi_1(\gamma) = \pi_2(\gamma) = 1 > 0$, si ha che $0 < \pi_1(\gamma) < pi_1(\gamma^2) < \cdots$ per ogni n perciò $\gamma^n \neq \pm 1$, analogamente per $-\gamma^n$ si ha $0 > \pi_1(\gamma) > pi_1(\gamma^2) > \cdots$, quindi μ è iniettiva dato che $Ker(\mu)\{(\pm 1, n) \mid \gamma((\pm 1, n)) = 1\} = \{1\}$ per il discorso precedente. μ è ovviamente surgettiva resta da vedere che $< \gamma >= A^*$; intanto $< \gamma > \subset A^*$ inoltre $(\pm\gamma^n)^{-1} = \pm\gamma^{-n} \in < \gamma >$ e $\pm\bar{\gamma}^n = \pm\bar{\gamma}^n = \pm(-\gamma^{-1})^n = \pm(-1)^n\gamma^{-n} \in < \gamma >$ quindi è chiuso per coniugio è inversa perciò $A^* = < \gamma >$.

4.7.3 osservazione : Sia $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = p(x)$ con $a_i \in \mathbb{Z}$, sappiamo che se $q \in \mathbb{Q}$ è radice di $p(x)$ allora $q = \frac{a}{b}$ con $a|a_0$ e $b|a_n$. Lo stesso vale in $A[x]$ dove A è UFD.

4.7.1 Definizione : Dato un dominio $A \subset \mathbb{K}$ campo, diciamo che A è *integralmente chiuso in* $\mathbb{K}$ se presa $\alpha \in \mathbb{K}$ radice di un polinomio monico $p(x) \in A[x]$ allora $\alpha \in A$.

4.7.1 Teorema : $A\ UFD \Longrightarrow A$ integralmente chiuso in $Frac(A)$.

4.7.1 esempio : Prendiamo $A = \mathbb{Z}[\sqrt{4n+1}]$ con $4n+1$ non quadrato in $\mathbb{Z}$. É integralmente chiuso in $Frac(A)$? Prendiamo $\alpha = \frac{1}{2}(1 + \sqrt{4n+1})$, α è radice di $t^2 - t - n$, dico che $\alpha \notin A$ (chiaramente $\alpha \in Frac(A)$). $\{1, \sqrt{4n+1}\}$ è una base di $\mathbb{K}$ su $\mathbb{Q}$ quindi $A = \{a + b\sqrt{4n+1} \mid a, b \in \mathbb{Z}\}$ quindi $\alpha \notin A$ e per il teorema precedente A non è UFD.

4.7.7 esercizio : $\mathbb{Z}[\sqrt{-2}]$ è ED ?

soluzione : Definisco innanzi tutto un coniugio $a + \bar{b}\sqrt{-2} = a - b\sqrt{-2}$ ed una norma $N(a + b\sqrt{-2}) = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + b^2$, osservo che $\frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \frac{(a+b\sqrt{-2})(c-d\sqrt{-2})}{c^2+2d^2} = e + f\sqrt{-2}$, ma $e, f \in \mathbb{Q}$. Prendo $g, h \in \mathbb{Z}$ tale che $|e - g|, |f - h| \leq \frac{1}{2}$ e prendo $q = g + h\sqrt{-2}$ quindi

$a+b\sqrt{-2} = q(c+d\sqrt{-2})+r$, perciò $r = a+b\sqrt{-2}-q(c+d\sqrt{-2})$ e $N(r) = N((c+d\sqrt{-2})((e-g)+(f-h)\sqrt{-2})) = N(c+d\sqrt{-2})N((e-g)+(f-h)\sqrt{-2}) \leq N(c+d\sqrt{-2})\frac{3}{4} < N(c+d\sqrt{-2})$. Allora l'anello è euclideo.

4.7.8 esercizio : Sia $a \in \mathbb{Z}$ con $a \geq 3$. $A = \mathbb{Z}[\sqrt{-a}]$ è ED ?

soluzione : Dico che in questo anello la fattorizzazione non è unica quindi non è un ED. Pongo $\omega = \sqrt{-a}$ e definisco la norma $N(x+\omega y) = x^2 + ay^2$, osservo che 2 è irriducibile infatti $N(2) = 4$ e $N(x+\omega y) \geq x^2 + 3y^2 \geq 3$ a meno di $u = 0,\ u = \pm 1$ allora 2 non si fattorizza. Se a è dispari $(1+\omega)(1-\omega) \in (2)$ infatti $(1+\omega)(1-\omega) = 1-a$ che è pari, poi $N(2) = 4$ e $N(\omega) = a$ ed essendo a dispari $\omega \notin (2)$ quindi $1-\omega, 1+\omega \notin (2)$ perciò (2) non è primo, ma è irriducibile quindi A non è UFD. se a pari, $\omega \notin (2)$ ma $\omega^2 \in (2)$ e si conclude come prima. In conclusione A per ogni $a \geq 3$ non è UFD.

4.7.2 Definizione : Sia A un anello commutativo con unità. Q è un *ideale primario* di A se $xy \in Q \Longrightarrow x \in Q$ oppure esiste n tale che $y^n \in Q$.

4.7.2 esempio : Sia $A = \mathbb{K}[x,y,z]/_{(xy-z^2)},\ \bar{P} = (\bar{x},\bar{z}),\ Q = \bar{P}^2.\ \bar{x}\bar{y} = \bar{z}^2$ ma $\bar{x},\bar{y} \notin \bar{P}^2$ quindi Q non è primario. Se nella definizione di primario avessi scritto "uno tra x e y deve essere tale che esiste n ..." allora Q di questo esempio sarebbe stato primario, infatti $\bar{x}^2 \in Q$.

4.7.1 Proposizione :

1) Q è primario $\Longleftrightarrow$ in A/Q i divisori di zero tutti e soli i nilpotenti.

2) Q primario $\Longrightarrow\ \sqrt{Q}$ è primo.

3) se $\sqrt{Q}$ è massimale $\Longrightarrow\ Q$ è primario.

Dimostrazione :

1) (Da vedere)

2) $xy \in \sqrt{Q} \Longleftrightarrow$ esiste n tale che $(xy)^n \in Q \Longrightarrow x^n y^n \in Q$ essendo Q primario si ha che o x^n in Q quindi $x \in \sqrt{Q}$ oppure esiste m tale che $y^{mn} \in Q$ quindi $y \in \sqrt{Q}$, quindi $\sqrt{Q}$ è primo (l'esempio precedente dimostra che non è vero il viceversa).

3) (Da vedere) Sia $M = \sqrt{Q}$ massimale, allora $\bar{M} \subset A/Q$ è massimale ed è intersezione di tutti gli ideali primi di A/Q, infatti sappiamo che $\bar{M} = \sqrt{\bar{0}}$, ma gli ideali primi che contengono 0 sono tutti quindi M è massimale ed è intersezione di tutti gli ideali primi quindi A/Q ha

un solo ideale primo, dico che $\bar{x} \in A/Q \Longrightarrow \bar{x} \notin \bar{M} \Longleftrightarrow \bar{x}$ è nilpotente o invertibile, invece $\bar{x} \in \bar{M} = \sqrt{\bar{0}}$ quindi i divisori di $\bar{0}$ in A/Q sono nilpotenti quindi Q è primario.

4.7.9 esercizio : (Da vedere) $Aut(\mathbb{Q}[x])$

soluzione :

4.7.10 esercizio : (Da vedere) Sia $A = \mathbb{Z}[\sqrt{7}]$, sia il coniugio $a + \bar{b}\sqrt{7} = a - b\sqrt{7}$ e la norma $N(u) = u\bar{u}$ allora :

1) N è moltiplicativa.

2) u invertibile $\Longleftrightarrow N(u) = \pm 1$.

3) Sia $P \in \mathbb{Z}$ primo, p è riducibile in $A \Longleftrightarrow$ esiste $u \in A$ tale che $N(u) = p$.

4) 2 è riducibile, 3 è riducibile, 5 è irriducibile.

soluzione :

4.7.11 esercizio : Sia $A = \mathbb{Q}[x, y]$. $I = (x^2 + y^2 - 1)$, $J = (x^2 - 3, y^2 - x)$ sono primi o massimali ?

soluzione : $I \subsetneq (x, y - 1)$ che è massimale quindi I non è massimale ma è primo infatti $x^2 + y^2 - 1$ è irriducibile infatti se prendo il primo $y - 1$ per Eisenstein si ha l'irriducibilità, essendo $\mathbb{Q}[x, y]$ UFD allora è anche primo. J è massimale infatti sia $\alpha = \sqrt[4]{3}$ e $\gamma : A \longrightarrow \mathbb{Q}[\alpha]$ dove $\gamma(p(x, y)) = p(\alpha^2, \alpha)$, si ha che $Ker/\gamma \supset J$, inoltre se $f(x, y) \in Ker(\gamma)$ allora $f(x, y) = a+bx+cy+dxy+g(x, y)$ con $g(x, y) \in J$ allora $\gamma(f(x, y)) = a+b\alpha^2+c\alpha+d\alpha^3 = 0$ ed essendo $1, \alpha, \alpha^2, \alpha^3$ una base di A come $\mathbb{Q}$ spazio vettoriale si ha che $a = b = c = d = 0$.

4.7.12 esercizio : Sia $A = \mathbb{Q}[x^2, x^3] \subset \mathbb{Q}[x]$ un sotto-anello e siano $I = (x^3 + 2)$, $J = (x^2 + x^3)$ ideali di A, chi è primo o massimale ?

soluzione : J non è primo quindi neanche massimale infatti $(x^3 + x^2)(x^3 - x^2) \in J$ ma $(x^3 + x^2)(x^3 - x^2) = (x^6 - x^4) = x^4(x^2 - 1)$ e $x^4, x^2 - 1 \notin J$. Consideriamo adesso $\tilde{I} = (x^3 + 2) \in \mathbb{Q}[x]$ allora $I = \tilde{I} \cap A$. Sia $\gamma : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\alpha]$ dove $\gamma(p(x)) = p(\alpha)$ e $\alpha = \sqrt[3]{2}$, $Ker(\gamma) = \tilde{I}$ e $\mathbb{Q}[\alpha]$ è un campo allora anche A/I è massimale quindi I è massimale quindi anche primo, si noti che $I = \tilde{I}^C$.

Campi

Capitolo 5

Campi di spezzamento

5.1 Estensioni di campi

5.1.1 Definizione : Siano K, L campi. $\alpha \in L$ si dice *algebrico su* K se esiste $f \in K[x]/\{0\}$ tale che $f(\alpha) = 0$. $\alpha \in L$ si dice *trascendente* se non è algebrico. L/K si dice *algebrica* se per ogni $\alpha \in L$, α è algebrico su K. $[L : K] = dim_K(L)$, L come $K-$spazio vettoriale, se $[L : K] < \infty$ allora si dice che L/K è $finito$.

5.1.2 Definizione : Sia K un campo e sia $\alpha \notin K$ allora $K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f(x, g(x)) \in K[x],\ g(x) \neq 0\}$ è detta *estensione semplice di* K ed è un campo.

5.1.1 osservazione : Sia $\gamma : K[x] \longrightarrow k[\alpha] \subset L$ allora $K[\alpha] \cong K[x]/_{Ker(\gamma)}$. $Ker(\gamma) = \{0\} \iff \alpha$ trascendente oppure $Ker(\gamma) = (\mu(x))$ dove (μ) è primo perché $K[\alpha]$ è un dominio. (μ) è un ideale primo non 0 quindi, essendo $K[x]$ un PID, (μ) è massimale e perciò $K[\alpha]$ è un campo e $K[\alpha] = K(\alpha)$, inoltre μ è irriducibile e i generatori di (μ) sono $c\mu$ con $c \in K^*$.

5.1.3 Definizione : Chiamiamo *polinomio minimo di* α l'unico generatore monico di $Ker(\gamma)$.

5.1.2 osservazione : Sia K un campo $\alpha \notin K$ e μ_α il suo polinomio minimo allora $[K[\alpha] : K] = deg(\mu_\alpha)$, $K[\alpha] \cong K[x]/_{(\mu_\alpha)}$. $K[x]/_{(\mu_\alpha)}$ ha base $1, \bar{x}, \cdots, \bar{x}^{n-1}$ con $n = deg(\mu_\alpha)$ allora $1, \alpha, \cdots, \alpha^{n-1}$ è base di $K[\alpha]$.

5.1.1 Proposizione : (Aritmetica) Siano $L \supseteq F \supseteq K$ campi. Allora L/K finita $\iff$ L/F e F/K sono finite.

Dimostrazione : $(\Longrightarrow)$: Se L/K finita allora $[L : K] = n < \infty$ ma $[L : K] = [L : F][F : K]$ quindi anche L/F e F/K sono finite.

($\Longleftarrow$) : L/F e F/K sono finite quindi consideriamo $\{\alpha_i\}_{i=1}^n$ base di L/F e $\{\beta_j\}_{j=1}^m$ base di F/K allora ogni elemento v di L lo esprimo come $v = \sum_{i=1}^{n} a_i\alpha_i$, con $a_i \in F$, ma ogni a_i lo posso esprimere come $a_i = \sum_{j=1}^{m} b_{ij}\beta_j$, con $b_{ij} \in K$ quindi $v = \sum_{i=1}^{n} \alpha_i(\sum_{j=1}^{n} b_{ij}\beta_j) = \sum_{i,j=0}^{i=n,j=m} b_{ij}\alpha_i\beta_j$ quindi $\{\alpha_i\beta_j\}_{i=1,\cdots,n}^{j=1,\cdots,m}$ è una K-base di L quindi L/K è finita.

□

5.1.2 Proposizione : L/K finita $\Longrightarrow$ L/K algebrica.

Dimostrazione : L/K finita quindi $[L : K] = n < \infty$ allora per ogni $\alpha \in L$, $1, \alpha, \cdots, \alpha^n$ sono linearmente dipendenti perché sono $n + i$ elementi, quindi esistono $a_i \in K$ non tutti nulli tale che $\sum_{i=1}^{n} a_i\alpha^i = 0$ quindi $f(x) = \sum_{i=1}^{n} a_i x^i \in K[x]/\{0\}$ è tale che $f(\alpha) = 0$ quindi L/K algebrica.

□

5.1.3 osservazione : L/K algebrica $\not\Longrightarrow$ L/K finita. Infatti consideriamo il campo $\mathbb{Q}$; $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$ dove $\bar{\mathbb{Q}}$ è la chiusura algebrica di $\mathbb{Q}$ (spiegheremo poi il concetto di chiusura algebrica) infatti $\bar{\mathbb{Q}}/\mathbb{Q}$ è algebrica per definizione ma non è finita in quanto $x^n - 2$ sono tutti irriducibili per Eisenstein, quindi se α_n e radice di $x^n - 2$ allora $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ per ogni n e siccome $\mathbb{Q}(\alpha_n) \subset \bar{\mathbb{Q}}$, sempre per definizione, allora $[\bar{\mathbb{Q}} : \mathbb{Q}] = [\bar{\mathbb{Q}} : \mathbb{Q}(\alpha_n)][\mathbb{Q}(\alpha_n) : \mathbb{Q}] = [\bar{\mathbb{Q}} : \mathbb{Q}(\alpha_n)]n$ pe ogni $n \in \mathbb{N}$ quindi non è finita.

5.1.3 Proposizione : Data L/K, non necessariamente algebrica, allora $A = \{\alpha \in L \mid \alpha$ è *algebrico su K* è una estensione algebrica di K.

Dimostrazione : (Da vedere) Bisogna vedere che è un campo. Presi $\alpha, \beta \in A \Longrightarrow \alpha, \beta \in K(\alpha, \beta) \subset A$ ed il contenimento vale perché α, β sono algebrici su K quindi L'estensione $K(\alpha, \beta)$ è finita perché per il teorema delle torri di estensione $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K]$ sono estensioni semplici quindi finite e perciò algebriche. Itero con tutti gli $\alpha \in L$ ed ottengo $A \supseteq K(\alpha_i)$ e siccome A è chiuso per somma e prodotto vale l'uguaglianza.

□

5.1.4 Definizione : Sia $S \subset L$ sottoinsieme di un campo. Definiamo $K(S) = \bigcap_{K,S \subset F \subset L} F$ che è il più piccolo sottocampo di L che contiene K e S.

5.1.4 Proposizione : L/K algebrica + finitamente generata $\Longrightarrow$ L/K finita.

Dimostrazione : (Da vedere) (Aritmetica : estensione semplice e algebrica è finita) L/K è finitamente generata quindi $L = K(\alpha_1, \cdots, \alpha_t)$ ora per induzione su t. Se $t = 1$ allora l'estensione è semplice e dato che α_1 è algebrico su K allora L/K è finita; per il passo induttivo

si ha che $[K(\alpha_1, \cdots, \alpha_{t-1}) : K]$ è finita quindi $[K(\alpha_1, \cdots, \alpha_t) : K] = [K(\alpha_1, \cdots, \alpha_{t-1})(\alpha_t) : K(\alpha_1, \cdots, \alpha_{t-1})][K(\alpha_1, \cdots, \alpha_{t-1}) : K] = l < \infty$, dato che α_t è algebrico su $K(\alpha_1, \cdots, \alpha_{t-1})$ e $K(\alpha_1, \cdots, \alpha_{t-1})(\alpha_t)$ è una estensione semplice di $K(\alpha_1, \cdots, \alpha_{t-1})$, perciò L/K è finita.

□

5.1.1 Teorema : (Torri di estensioni algebriche) Siano $L \supset F \supset K$ campi. Allora L/K algebrica $\iff$ L/F e F/K algebriche.

Dimostrazione : ($\Longrightarrow$) : Sia $\alpha \in L$ essendo algebrico su K lo è anche su F, inoltre se $\alpha \in F$, essendo $F \subset L$, α è algebrico in K.
($\Longleftarrow$) : $\alpha \in L$ è algebrico su F quindi esiste $p(x) = a_0 + a_1x + \cdots + a_mx^m \in F[x]/\{0\}$ tale che $p(\alpha) = 0$. Pongo $F_0 = K(a_0, \cdots, a_m) \subset F$, α è algebrico su F_0, allora $[F_0(\alpha) : K] = [F_0(\alpha) : F_0][F_0 : K]$ ora $F_0(\alpha)/F_0$ è algebrica e semplice quindi finita e $[F_0 : K]$ è finito quindi $[F_0(\alpha) : K]$ è finito quindi $F_0(\alpha)/K$ algebrica perciò α è algebrico su K.

□

5.2 Campi di spezzamento

5.2.1 Definizione : Un campo Γ si dice *algebricamente chiuso* se per ogni $f \in \Gamma[x]$, $\partial(f) \geq 1 \Longrightarrow f$ ha almeno una radice in Γ.

5.2.1 esempio : $\mathbb{C}$ è algebricamente chiuso. $\mathbb{Q}, \mathbb{R}, \mathbb{F}_q, \mathbb{Q}(\sqrt[19]{317})$ non lo sono.

5.2.2 Definizione : $\bar{K}$ è una *chiusura algebrica* di K se :

1) $\bar{K}$ è algebricamente chiuso

2) $\bar{K}/K$ è algebrica.

5.2.1 Proposizione : Γ algebricamente chiuso e $f \in \Gamma[x]$, $\partial(f) \geq 1 \Longrightarrow$ f si spezza in fattori lineari in $\Gamma[x]$

Dimostrazione : Procediamo per induzione; $\partial(f) = 1$ ok, quindi per $\partial(f) \leq n - 1$ vale la tesi, dimostriamolo per $\partial(f) = n$. Γ è algebricamente chiuso quindi f ha almeno una radice perciò $f = (x-\alpha)g(x)$,a per ipotesi induttiva $g(x)$ si scompone in fattori lineari quindi anche f.

□

5.2.3 Definizione : Sia $f \in K[x]$, $\partial(f) \geq 1$ e $K \subset \bar{K}$. Si dice *campo di spezzamento di f su K* il campo $K(\alpha_1, \cdots, \alpha_n)$ dove $\{\alpha_i\}$ è l'insieme delle radici di f su $\bar{K}$. Se $\Gamma = \{f_i\}_{i \in I}$ e $\{\alpha_{ij}\}_{j \in J}$

radici di f_i su $\bar{K}$, allora $K(\{\alpha_{ij}\})_{i\in I}^{j} \in J$ è il campo di spezzamento di Γ su K.

5.2.1 osservazione : Sia $f \in K[x]$, $\partial(f) = n$ e $K \subset \bar{K}$ con $\{\alpha_i\}_{i\in I}$ radici di f. Allora $[K(\{\alpha_i\}_{i\in I}) : K] \leq n!$ infatti posso scrivere $K_J = K(\{\alpha_i\}_{i\leq j}$ allora $[K_n : K] = [k_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K : K]$ e $[K_i : K_{i-1}] = deg(\mu_{\alpha_i})$ e siccome K_i è estensione semplice di K_{i-1} allora $deg(\mu_{\alpha_i}) = 1 + deg(\mu_{\alpha_{i-1}})$.

5.2.2 Proposizione : Sia K un campo, $\alpha \in \bar{K}$ e $d =$ #radici distinte di μ_α in $\bar{K}$. Allora esistono esattamente d immersioni $\gamma_1, \cdots, \gamma_d : K(\alpha) \longrightarrow \bar{K}$ tale che $\gamma_i|_K = Id$. Se $\{\alpha_i\}_{i\in I}$ sono le radici di μ_α allora $\gamma_i(\alpha) = \alpha_i$.

Dimostrazione : Consideriamo $\gamma : K(\alpha) \hookrightarrow \bar{K}$ tale che $\gamma(1) = 1$ e $\gamma(\alpha) = \beta$. Sappiamo che $K(\alpha) \cong K[x]/_{(\mu_\alpha(x))}$ quindi consideriamo $\tilde{\gamma} : K[x] \longrightarrow \bar{K}$ tale che $\tilde{\gamma} = \beta$, esiste γ se e solo se $Ker(\tilde{\gamma}) = (\mu_\alpha(x))$ ma $Ker(\tilde{\gamma}) = \{p(x) \mid \tilde{\gamma}(p(x)) = p(\beta) = 0\} = (\mu_\beta(x))$ con μ_β polinomio minimo di β in $K[x]$; allora $(\mu_\alpha(x)) = (\mu_\beta(x)) \iff \beta$ è radice di μ_α.

□

5.2.3 Proposizione : (Criterio della derivata) Sia K un campo, $f \in K[x]$, $\partial \geq 1$. Allora f fa radici multiple in $\bar{K} \iff (f, f') \neq 1$.

Dimostrazione : $f(x) = (x-\alpha)^k g(x)$ con $k \geq 1$ e $g(\alpha) \neq 0$, allora $f'(x) = k(x-\alpha)^{k-1}g(x) + (x-\alpha)^k g'(x)$ perciò $f'(\alpha) = k(\alpha-\alpha)^{k-1}g(\alpha)+(\alpha-\alpha)^k g'(\alpha) = 0 \iff k(\alpha-\alpha)^{k-1} = 0 \iff k > 1$, per $k = 1$ si ha $f'(\alpha) = 1 \neq 0$. Le radici multiple sono anche radici della derivata.

□

5.2.2 osservazione : Se f è irriducibile abbiamo che $(f, f') \in \{1, f\}$ infatti se $f' > 0$, siccome f irriducibile, non ha radici multiple quindi $(f.f') = 1$, invece se $f' = 0$ allora $(f, f') = f$.

5.2.2 esempio :

1) Sia $K = \mathbb{F}_p(t)$, p primo, e consideriamo in $K[x]$ il polinomio $x^p - t$, t indeterminata. $f'(x) = px^{p-1} = 0$ quindi ha radici multiple ma siccome t è primo, $A = \mathbb{F}_p[t]$ è UFD, allora $x^p - t$ è irriducibile per Eisenstein quindi è irriducibile in $K[x]$ per il lemma di Gauss.

2) $f \in \mathbb{Q}[x]$ irriducibile allora $f'(x) \neq 0$.

3) $f \in \mathbb{F}_q[x]$, q primo e $f'(x) = 0$ allora $f(x) = g(x)^q$ quindi non è irriducibile.

5.2.3 esempio : Sia $x^p - t \in \mathbb{F}_p(t)[x]$ e $\alpha \in \mathbb{F}_p(\bar{t})[x]$ radice, allora $\alpha^p - t = 0 \Longrightarrow \alpha^p = t$ quindi $x^p - t = x^p - \alpha^p = (x - \alpha)^p$ in $\mathbb{F}_p(\bar{t})[x]$.

5.2.3 osservazione :

Se $char(K) = 0$ e $deg(f) \geq 1 \Longrightarrow f' \neq 0$. Se f è irriducibile allora f non ha radici multiple quindi ha $deg(f)$ radici distinte.

Se $char(K) = p$ oltre al caso di $char(K) = 0$ succede anche che $f' = 0$ e f irriducibile quindi f ha radici multiple.

5.2.4 Proposizione : Sia $f \in \mathbb{F}_q[x],\ deg(f) \geq 1$ con $q = p^n,\ p$ primo e supponiamo che $f' = 0$. Allora $f(x) = g(x)^p$ in $\mathbb{F}_q[x]$.

Dimostrazione : Sia $f(x) = \sum_{i=0}^{n} a_i x^i$ tale che $0 = f'(x) = \sum_{i=0}^{n} i a_i x^{i-1}$ quindi $ia_i = 0$ per ogni i di conseguenza, siccome $\mathbb{F}_q$ campo, si ha $a_i = 0$ per ogni i tale che $p \not| i$ quindi $f(x) = \sum_{k=0}^{m} a_{kp} x^{kp}$ con $mp \leq n$ e $(m+1)p > n$. Ora so che per ogni $a \in \mathbb{F}_q \Longrightarrow a = a^q = a^{p^n} = (a^{p^{n-1}})^p = b^p$ quindi $f(x) = \sum_{k=0}^{m} a_{kp} x^{kp} = \sum_{k=0}^{m} (b_k x^k)^p = (\sum_{k=0}^{m} b_k x^k)^p = g(x)^p$.

□

5.2.4 osservazione : Se K è un campo finito e $f \in K[x]$ irriducibile allora ha tutte le radici distinte in $\bar{K}$.

5.2.4 Definizione : f irriducibile si dice *separabile* se ha tutte le radici distinte in $\bar{K}$. L/K si dice *separabile* se per ogni $\alpha \in L$ si ha che il polinomio minimo di α, μ_α, è separabile in K.

5.2.5 osservazione : Se K ha caratteristica 0, ogni sua estensione è separabile. Se L è un campo finito allora L/K è separabile.

5.2.5 Proposizione : Sia $\alpha \in \bar{K}$ $n = [K(\alpha) : K],\ K(\alpha)/K$ separabile. Per ogni immersione di $\gamma : K \hookrightarrow \bar{K}$ esistono esattamente n omomorfismi $\gamma_i, \cdots, \gamma_n : K(\alpha) \longrightarrow \bar{K}$ tale che $\gamma_i|_K = \gamma$.

Dimostrazione : (Da vedere) Intanto $K(\alpha)/K$ separabile assicura che μ_α ha esattamente $[K(\alpha) : K] = n$ radici distinte in $\bar{K}$. Con le stesse osservazioni della Proposizione 5.2.2 costruiamo $\Phi : K[x] \longrightarrow \bar{K}$ con $\Phi(k) = \gamma(k)$ e $\Phi(x) = \beta$, essendo μ_α irriducibile e γ iniettiva allora $\gamma(\mu_\alpha)$ irriducibile quindi $\gamma(\mu_\alpha(\beta)) = 0$ e abbiamo che $(\mu_\alpha) \subset Ker(\Phi) = (\mu_\beta)$, ma μ_α è massimale dato che $K(\alpha)$ è campo quindi $(\mu_\alpha) = (\mu_\beta)$ perciò β varia tra le n radici distinte di μ_α generando così n immersioni distinte.

□

5.2.1 Corollario : E/K estensione finita e separabile e $[E : K] = n$ allora per ogni immersione di $\gamma : K \hookrightarrow \bar{K}$ esistono esattamente n omomorfismi $\gamma_i, \cdots, \gamma_n : E \longrightarrow \bar{K}$ tale che $\gamma_i|_K = \gamma$.

Dimostrazione : Procediamo per induzione su n :

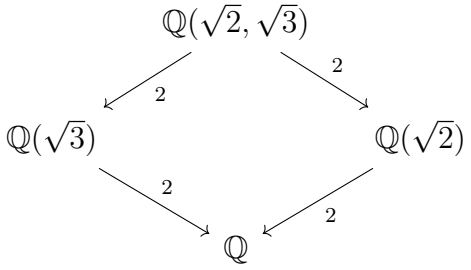
Passo Base : $n = 1$ ok.

Passo Induttivo : Sia $\alpha \in E/K$, si ha $K \subsetneq K(\alpha) \subsetneq E$ e supponiamo $[K(\alpha) : K] = m$ e $[E : K(\alpha)] = d$ con $n = md$, per la proposizione precedente esistono m immersioni $\gamma_i : K(\alpha) \hookrightarrow \bar{K}$ per ogni $\gamma : K \hookrightarrow \bar{K}$, per ipotesi induttiva per ogni γ_i esistono d immersioni $\gamma_{i_1}, \cdots, \gamma_{i_d} : E \hookrightarrow \bar{K}$ con $\gamma_{i_j}|_{K(\alpha)} = \gamma_i$. Ora abbiamo $\{\gamma_{i_j}\}_{i=1,\cdots,m}^{j=1,\cdots,d}$ che sono n immersioni di E su$\bar{K}$ osserviamo che $\gamma_{i_j}|_K = (\gamma_{i_j}|_{K(\alpha)})|_K = \gamma_i|_K = \gamma$ inoltre se $\gamma_{i_j} = \gamma_{e_t} \Longrightarrow \gamma_{i_j}|_{K(\alpha)} = \gamma_{e_t}|_{K(\alpha)} \Longrightarrow \gamma_i = \gamma_e \Longrightarrow i = e$, quindi si ha $\gamma_{i_j} = \gamma_{i_t} \Longrightarrow j = t$ quindi sono n immersioni distinte e vale la tesi.

□

5.2.4 esempio : Sia $\gamma : \mathbb{Q} \hookrightarrow \bar{\mathbb{Q}}$ e consideriamo $\tau : \mathbb{Q}(\sqrt{2}) \hookrightarrow \bar{\mathbb{Q}}$, dato che $\mu_{\sqrt{2}} = x^2 - 2$ si ha che $\tau(\sqrt{2}) = \pm\sqrt{2}$ quindi si ha $\tau_{1,2} : \mathbb{Q}(\sqrt{2}) \hookrightarrow \bar{\mathbb{Q}}$ tale che $\tau_{1,2}|_{\mathbb{Q}} = Id$ e $\gamma_1(a + \sqrt{2}b) = a + \sqrt{2}b$ e $\gamma_2(a + \sqrt{2}b) = a - \sqrt{2}b$.

5.2.5 esempio : Vediamo $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \hookrightarrow \bar{\mathbb{Q}}$. Osserviamo intanto che $\sqrt{3} \notin \sqrt{\not{2}}$ e viceversa infatti se per assurdo $\sqrt{3} = a + \sqrt{2}b \Longrightarrow 3 = \sqrt{3}\sqrt{3} = (a + \sqrt{2}b)(a + \sqrt{2}b) = a^2 + 2b^2 + (a + b)\sqrt{3}$ quindi $a + b = 0$ ovvero $a = -b$ quindi $3 = a^2 + 2b^2 = 3a^2 \Longrightarrow a = \pm 1$ quindi $\sqrt{3} = \pm + \mp\sqrt{2}$ ma è assurdo. Consideriamo $L = \mathbb{Q}(\sqrt{2})$ quindi si ha $L(\sqrt{3})$ e vediamo le immersioni in $\bar{\mathbb{Q}}$, si ha che $\mu_{\sqrt{3}} = x^2 - 3$ ed ha radici $\pm\sqrt{3}$ quindi esistono due immersioni di $L(\sqrt{3})$ su $\bar{\mathbb{Q}}$, osserviamo che esistono due immersioni di L su $L(\sqrt{3})$ quindi ci sono quattro immersioni di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ su $\bar{\mathbb{Q}}$ che fissano $\mathbb{Q}$ tale che $\gamma(\sqrt{2}) = \pm\sqrt{2}$ e $\gamma(\sqrt{3}) = \pm\sqrt{3}$. Il risultato si può esprimere schematicamente con :



Abbiamo che $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ è una $\mathbb{Q}-$base di $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Sia $\alpha \in E$, $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, le quattro immersioni sono della forma :

$$\begin{array}{cccc} \tilde{\gamma_1} = Id & \sqrt{2} \longrightarrow & \sqrt{2}, & \sqrt{3} \longrightarrow \sqrt{3} \\ \tilde{\gamma_2} & \sqrt{2} \longrightarrow & -\sqrt{2}, & \sqrt{3} \longrightarrow \sqrt{3} \\ \tilde{\gamma_3} & \sqrt{2} \longrightarrow & \sqrt{2}, & \sqrt{3} \longrightarrow -\sqrt{3} \\ \tilde{\gamma_4} & \sqrt{2} \longrightarrow & -\sqrt{2}, & \sqrt{3} \longrightarrow -\sqrt{3} \end{array}$$

In particolare $\tilde{\gamma_2}(\alpha) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$

5.2.6 osservazione : $\tilde{\gamma_i}(\sqrt{2} + \sqrt{3}) = \pm\sqrt{2} + \pm\sqrt{3}$ che sono quattro elementi distinti, il polinomio minimo di $\sqrt{2}+\sqrt{3}$ ha quattro radici distinte, con un conto ne trovi almeno quattro, poi più di quattro non le trovi dato che è contenuto in una estensione di grado quattro, allora $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

5.2.5 Definizione : Dati L/K e $\alpha \in L$ allora i *coniugati di α su K* sono le radici di μ_α il polinomio minimo di α su K.

5.2.7 osservazione : Se $[L : K] = n$ e $\gamma_i : L \longrightarrow \bar{K}$ sono le immersioni di L/K allora $\{\gamma_i(\alpha)\}$ è l'insieme dei coniugati di α.

5.2.6 Definizione : Una estensione algebrica F/K si dice *normale* se per ogni $\gamma : F \longrightarrow \bar{K}$ tale che $\gamma|_K = Id$ si ha $\gamma(F) = F$.

5.2.6 Proposizione : Tutte le estensioni di grado due sono normali.

Dimostrazone : (Da vedere) Sia $\omega \in \bar{\mathbb{Q}}/\mathbb{Q}$ tale che $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, allora il polinomio minimo di ω è della forma $\mu_\omega = ax^2 + bx + c$. Per la proposizione 5.2.5 esistono due immersioni di $\mathbb{Q}(\omega)$ in $\bar{\mathbb{Q}}$ date dall'immagine di ω nelle due radici di μ_ω, osserviamo che le radici di μ_ω sono $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ supponiamo senza perdita di generalità $\omega = \frac{-b+\sqrt{b^2-4ac}}{2a}$ allora $\frac{-b-\sqrt{b^2-4ac}}{2a} = -\frac{b}{a} - \omega \in \mathbb{Q}(\omega)$ quindi $\mathbb{Q}(\omega)$ è normale.

□

5.2.6 esempio :

1) Sia $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ è normale perché $\gamma(\sqrt{2}) = \pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ quindi $\gamma(\mathbb{Q}(\sqrt{2})) = \mathbb{Q}(\sqrt{2})$.

2) Non tutte le estensioni di grado tre sono normali infatti $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è normale dato che il polinomio minimo di $\sqrt[3]{2}$ è x^3-2 e ha come radici $\sqrt[3]{2}, \xi_3\sqrt[3]{2}, \xi_3^2\sqrt[3]{2}$ quindi esiste $\gamma : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \bar{\mathbb{Q}}$ tale che $\gamma(\sqrt[3]{2}) = \xi_3\sqrt[3]{2}$ ma $xi_3\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

5.2.7 Proposizione : Sia F/K normale. Allora ogni polinomio $f(x) \in K[x]$ irriducibile in $K[x]$ che ha una radice in F le ha tutte in F, cioè in F si spezza in fattori lineari.

Dimostrazione : Sia $finK[x]$ irriducibile e $\alpha_1, \cdots, \alpha_n \in \bar{K}$ radici di f quindi $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$ in $\bar{K}$. Consideriamo ora $\alpha = \alpha_1 \in F$, $K \subset K(\alpha) \subset F$ e F/K normale, per la proposizione 5.2.5 esistono e sono uniche $\gamma_1, \cdots, \gamma_n : K(\alpha) \longrightarrow \bar{K}$ tale che $\gamma_i(\alpha) = \alpha_i$ allora per ogni i esiste almeno una $\bar{\gamma_i} : F \longrightarrow \bar{K}$ tale che $\bar{\gamma_i}|_{K(\alpha)} = \gamma_i$ e $\bar{\gamma_i}(\alpha) = \alpha_i$ ma F/K è normale quindi $\bar{\gamma_i}(F) = F$ perciò $\bar{\gamma_i}(\alpha) = \alpha_i \in F$ per ogni i quindi tutte le radici stanno in F.

□

5.2.1 Teorema : F/K algebrica. F/K normale $\Longleftrightarrow$ F è campo di spezzamento di una famiglia di polinomi di $K[x]$

Dimostrazione : (Dimostrazione del caso F/K finita ovvero algebrica e finitamente generata)

($\Longrightarrow$) $F = K(\alpha_1, \cdots, \alpha_s)$ estensione algebrica è finitamente generata e $\mu_i, \cdots, \mu_s$ i polinomi minimi rispettivamente di $\alpha_1, \cdots, \alpha_s$ su K. $K \subset F \subset L = K(\{\alpha_{ij}\})$, L campo di spezzamento e $\{\alpha_{ij}\}_{i=1,\cdots,s}^{j=1,\cdots,d_i}$ le radici di μ_i in K con $deg(\mu_i) = d_i$. Ora F/K è normale quindi per ogni i contiene una radice dei μ_i che sono irriducibili in K quindi per la proposizione precedente le contiene tutte quindi $L \subset F$ di conseguenza $L = F$ quindi è campo di spezzamento.

($\Longleftarrow$) Sia $\gamma : F \hookrightarrow \bar{K}$ con $\gamma|_K = Id$, devo vedere che $\gamma(F) = F$. F è campo di spezzamento di $\{f_i\}_{i=1,\cdots,s}$ quindi $F = K(\{\alpha_{ij}\})_{i=1,\cdots,s}^{j=1,\cdots,d_i}$ le radici di f_i in K con $deg(f_i) = d_i$, osserviamo che $\gamma(F) = K(\{\gamma(\alpha_{ij})\})_{i=1,\cdots,s}^{j=1,\cdots,d_i}$ ma $\gamma(\alpha_{ij}) = \alpha_{it} \in F$ quindi $\gamma(F) \subset F$ e siccome hanno lo stesso grado si ha $\gamma(F) = F$ quindi F è normale.

□

5.2.2 Teorema : (Esistenza ed unicità della chiusura algebrica) Sia K un campo. Allora esiste $\bar{K}$ chiusura algebrica di K, e $\bar{K}$ è unica a meno di isomorfismo.

Dimostrazione :

(Unicità) Sia $\bar{K}$ e $\bar{\bar{K}}$ due chiusure algebriche di K, voglio vedere che $\bar{K} \cong \bar{\bar{K}}$. Prendo $\sigma : K \hookrightarrow \bar{K}$, $\bar{\bar{K}}/K$ è algebrica quindi esiste $\tilde{\sigma} : \bar{\bar{K}} \hookrightarrow \bar{K}$ tale che $\tilde{\sigma}(\bar{\bar{K}})$ è algebrica su $\sigma(K)$. Ora

se dimostro che $\tilde{\sigma}(\bar{\bar{K}})$ è algebricamente chiuso ho finito infatti, per ogni $\alpha \in \bar{k},\ \alpha$ è algebrico su K quindi anche su $\tilde{\sigma}(\bar{\bar{K}})$ quindi $\alpha \in \tilde{\sigma}(\bar{\bar{K}})$. Dimostro allora che $\tilde{\sigma}(\bar{\bar{K}})$ è algebricamente chiuso : $\tilde{\sigma}(p(x)) \in (\tilde{\sigma}(\bar{\bar{K}}))[x],\ p(x \in \bar{\bar{K}})[x] \Longrightarrow$ esiste $\alpha \in \bar{\bar{K}}$ tale che $p(\alpha) = 0 \Longrightarrow \tilde{\sigma}(\alpha) \in \tilde{\sigma}(\bar{\bar{K}})$ è radice di $\tilde{\sigma}(p(x))$.

(Esistenza) Costruisco E_1/K tale che ogni $p(x) \in K[x]$ con $\partial p(x) \geq 1$ abbia almeno una radice in E_1. Sia $\{p(x) \in K[x] \mid \partial p(x) \geq 1\} = \{p_\lambda(x) \mid \lambda \in \Lambda\}$ e sia $X = \{x_\lambda \mid \lambda \in \Lambda\}$ e sia infine $K[X]$. Considero $p_\lambda(x_\lambda) \in K[X]$ e $I = (p_\lambda(x_\lambda))_{\lambda\in\Lambda} \subset K[X]$, noto che $I \neq (1)$. Infatti se $1 \in I$ esisterebbero $\lambda_1, \cdots, \lambda_n$ e $f_1, \cdots, f_n \in K[x]$ tali che $1 = \sum f_i(x)p_{\lambda_i}(x_{\lambda_i})$ ma se consideriamo l'omomorfismo di valutazione $val : K[x] \longrightarrow L$ dove L contiene una radice di ogni $\{p_{\lambda_i}\}_{i=1,\cdots,n}$ (come nell'osservazione 5.2.11) e tale che $val(1) = 1$ e $val(x_\lambda) = 0$ se $\lambda \neq \lambda_i$ se non $val(x_\lambda) = \alpha_{\lambda_i}$ che è la radice di p_{λ_i} che appartiene a L, allora $1 = val(1) = val(\sum f_i(x)p_{\lambda_i}(x_{\lambda_i})) = \sum val(f_i(x))val(p_{\lambda_i}(x_{\lambda_i})) = \sum val(f_i(x)) \cdot 0 = 0$ assurdo. Allora esiste $M \subset K[X]$ massimale tale che $M \supset I$, prendo $E_1 = K[X]/M$. Sicuramente è un campo, devo dimostrare che contiene K e che ogni polinomio in $K[x]$ ha almeno una radice in E_1. Considero $\phi : K \longrightarrow K[X] \longrightarrow K[X]/M = E_1$ tale che $1 \longrightarrow 1 \longrightarrow 1 + M \neq M$ e $x_\lambda \longrightarrow \bar{x_\lambda}$, si ha che $\phi \neq 0 \Longrightarrow \phi$ è iniettivo e $K \subset E_1$ (come nell'osservazione 5.2.10). Prendo ora $p_\lambda \in K[x]$, $p_\lambda(x_\lambda) \in I \subset M$, quindi $\bar{x_\lambda} \in E_1 = K[\{\bar{x_\lambda}\}_{\lambda\in\Lambda}]$, ma $p_\lambda(\bar{x_\lambda}) = 0$ perché $p_\lambda(x_\lambda) \in I \subset M$. Ora posso costruire induttivamente $E_1 \subset E_2 \subset \cdots$ tale che ogni polinomio di grado ≥ 1 di E_n abbia una radice in E_{n+1} (come nell'osservazione 5.2.11). Sia $\Omega = \bigcup_{n\geq 1} E_n$, Ω è algebricamente chiuso (come nell'osservazione 5.2.9), per ogni $f(x) \in \Omega[x]$, f ha almeno una radice in Ω ($f \in E_{n_0},\ E_{n_0+1}$ contiene una radice di f) $\Longrightarrow \bar{K} = \{\alpha \in \Omega \mid \alpha$ algebrico su $K\}$ è il campo cercato (si dimostra come nell'osservazione 5.2.8).

□

5.2.8 osservazione : $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha$ è algebrico su $\mathbb{Q}\}$, $\bar{\mathbb{Q}}$ è la chiusura algebrica di $\mathbb{Q}$: è algebrica per costruzione, se $\alpha, \beta \in \bar{\mathbb{Q}} \Longrightarrow \alpha + \beta, \alpha\beta, \frac{1}{\alpha} \in \mathbb{Q}(\alpha, \beta) \subset \bar{\mathbb{Q}}$ quindi è un campo, inoltre è algebricamente chiuso infatti sia $p(x) \in \bar{Q}$ allora esiste $\alpha \in \mathbb{C}$ tale che $p(\alpha) = 0$ con $\partial p(x) \geq 1$, ma $L = \mathbb{Q}$(coefficienti di $p(x)$) è algebrica su $\mathbb{Q} \Longrightarrow L(\alpha)$ è algebrica su L e quindi su $\mathbb{Q} \Longrightarrow \alpha \in \bar{Q}$.

5.2.9 osservazione : $\bar{\mathbb{F}_p} = \bigcup_n \mathbb{F}_{p^n}$ infatti $p(x) \in \bar{\mathbb{F}_p} \Longrightarrow$ esiste n tale che $p(x) \in \mathbb{F}_{p^n}$, allora il campo di spezzamento di $p(x)$ è $\mathbb{F}_{p^{nd}} \subset \bar{\mathbb{F}_p}$.

5.2.10 osservazione : Dato $p(x) \in K[x]$ posso costruire un campo che contiene K e una radice di $p(x)$, fattorizzo $p(x)$ in $K[x]$. P_1 è un fattore irriducibile di $p(x)$ allora $K \longrightarrow K[x]/(p_1(x)) \longrightarrow K'$ tale che $1 \longrightarrow 1 \longrightarrow 1 + p_1(x)$.

5.2.11 osservazione : Presa una famiglia finita di polinomi $\{f_1, \cdots, f_n\}$, posso costruire

E/K tale che per ogni i, f_i abbia una radice in E. Infatti siano f_{i1} fattori irriducibili di ogni f_i, allora $K \longrightarrow K[x]/(f_{11}(x)) = K' \longrightarrow K'/(f_{21}(x)) = K'' \longrightarrow \cdots$.

Capitolo 6

Teoria di Galois

6.1 Il gruppo di Galois

6.1.1 Definizione : Sia E/K una estensione normale e separabile si dice allora che E/K è *di Galois*.

6.1.1 osservazione : E/K è normale $\iff$ ogni $\gamma : E \longrightarrow \bar{K}$ tale che $\gamma|_K = Id$ è un automorfismo di E/K. Se E/K è separabile allora $\#Hom_K\{E \longrightarrow \bar{K}\} = [E : K]$.

6.1.2 Definizione : Sia E/K di Galois allora $Aut_K(E) = Gal(E/K) = \{\gamma : E \longrightarrow \bar{K}\}$ è il *gruppo di Galois di* E/K, che è un gruppo e $|Aut_K(E)| = [E : K]$.

6.1.3 Definizione : Sia $f \in K[x]$ allora $Gal_K(f) = Gal(E/K)$ con E campo di spezzamento di f su K.

6.1.2 osservazione : Sia f irriducibile, $\partial(f) = n$, $\alpha_i, \cdots, \alpha_n \in \bar{K}$ radici di f e E campo di spezzamento di spezzamento di f su K. allora consideriamo $\Phi : Gal_k(f) = Gal(E/K) \hookrightarrow S_{\{\alpha_1,\cdots,\alpha_n\}} \cong S_n$ tale che $\Phi(\gamma) = \gamma|_{\{\alpha_1,\cdots,\alpha_n\}}$, questa è una applicazione ben definita che permuta le radici di f, è un omomorfismo iniettivo infatti $\gamma|_{\{\alpha_1,\cdots,\alpha_n\}} = Id \Longrightarrow \gamma(\alpha_i) = \alpha_i \Longrightarrow Ker(\Phi) = \{Id\}$, inoltre per ogni i, j esiste $\gamma \in Gal_K(f)$ tale che $\gamma(\alpha_i) = \alpha_j$ quindi $\Phi(Gal_K(f))$ è un *sottogruppo transitivo* di S_n ovvero per ogni i $\{\alpha_1, \cdots, \alpha_n\} = orb(\alpha_i)$.

6.1.1 Corollario : $f \in K[x]$ con $\partial(f) = n$ allora $Gal_K(f) < S_n$ in particolare $|Gal_K(f)|\ |n!$

6.1.3 osservazione : Sia E/K di Galois e $\alpha \in E$ allora per ogni $\sigma \in Gal(E/K)$, $\{\sigma(\alpha)\}$ è l'unione dei coniugati di α su K, cioè è l'insieme delle radici di $\mu_\alpha(x) \in K[x]$.

6.1.1 esempio :

1) E/K tale che $[E : K] = 2$ allora E/K è normale inoltre è separabile dato che se mu_α, $\alpha \in E$ ma $\notin K$, non avesse radici distinte allora $mu_\alpha = (x-\alpha)^2 = x^2 + 2\alpha x + \alpha^2 \Longrightarrow \alpha \in K$, quindi E/K è di Galois e $Gal(E/K) \cong \mathbb{Z}/_{2\mathbb{Z}}$.

2) $deg(f) = 3$ e E il suo campo di spezzamento allora $Gal(E/K) < S_3$ e $3|\ |Gal(E/K)|$ quindi $gal(E/K)$ può essere S_3 o A_3 infatti se consideriamo $f = x^3 - 2$ si ha che $E = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ e $[E : \mathbb{Q}] = 6$ quindi $Gal(E/K) \cong S_3$ invece se considero ξ_7 si ha che $[\mathbb{Q}(\xi_7) : \mathbb{Q}] = 6$ dato che $\mu_{\xi_7}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ inoltre $\mathbb{Q}(\xi_7) \cap \mathbb{R} \neq \emptyset$ infatti $\xi_7 + \xi_7^{-1} \in \mathbb{R}$, osserviamo che $[\mathbb{Q}(\xi_7) : \mathbb{Q}(\xi_7 + \xi_7^{-1})] = 2$ dato che $\mu_{\xi_7} = x^2 - (\xi_7 + \xi_7^{-1})x + 1$ è il suo polinomio minimo, quindi si ha $E = \xi_{\not p} \xrightarrow{2} F = \mathbb{Q}(\xi_7 + \xi_7^{-1}) \xrightarrow{3} \mathbb{Q}$ e $E/_{\mathbb{Q}}$ è di Galois ed il suo gruppo e formato da automorfismi di $E/_{\mathbb{Q}}$ tale che $\gamma_i(\xi_7) = \xi_7^i$ con $i = 1, \cdots, 6$. Osserviamo infine che $orb(\xi_7 + \xi_7^{-1}) = \{\gamma_i(\xi_7 + \xi_7^{-1})\} = \{\xi_7 + \xi_7^{-1}, \xi_7^2 + \xi_7^{-2}, \xi_7^3 + \xi_7^{-3}\} \in \mathbb{Q}(\xi_7 + \xi_7^{-1})$ infatti $(\xi_7 + \xi_7^{-1})^2 = \xi_7^2 + \xi_7^{-2}$ e $(\xi_7 + \xi_7^{-1})^3 = \xi_7^3 + \xi_7^{-3}$ quindi $\mathbb{Q}(\xi_7 + \xi_7^{-1})/_{\mathbb{Q}}$ è di Galois e $Gal(\mathbb{Q}(\xi_7 + \xi_7^{-1})/_{\mathbb{Q}}) \cong A_3$.

6.1.1 Proposizione : (Torri di estnsioni di Galois) Sia L/K di Galois e $G = Gal(L/K)$ se $K \subset F \subset L$ allora L/F è di Galois invece non è sempre vero che F/K è di Galois e non è detto che se F/K e L/F di Galois allora L/K di Galois.

6.1.2 esempio : $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[4]{2})/_{\mathbb{Q}(\sqrt{2})}$ e $\mathbb{Q}(\sqrt{2})/_{\mathbb{Q}}$ sono estensioni di grado due quindi di Galois ma $\mathbb{Q}(\sqrt[4]{2})/_{\mathbb{Q}}$ non è di Galois dato che il polinomio minimo di $\sqrt[4]{2}$ è $x^4 - 2$ che ha campo di spezzamento $\mathbb{Q}(\sqrt[4]{2}, \xi_4)$.

6.1.4 osservazione : L/K di Galois e $K \subset F \subset L$ allora $Gal(L/F) < Gal(L/K)$.

6.1.1 Teorema : (dell'elemento primitivo) Sia E/K una estensione finita e separabile allora esiste $\alpha \in E$ tale che $E = K(\alpha)$.

Dimostrazione : Se K è finito e $char(K) = 0$ allora E è finito quindi E^* è ciclico ovvero $E =< \alpha >$ quindi $E = K < \alpha >$.
Se K infinito supponiamo $[E : K] = n$ in quanto estensione finita, quindi esistono $\gamma_1, \cdots, \gamma_n : E \longrightarrow \bar{K}$ tale che $\gamma_i|_K$ e siccome è separabile $\gamma_i \neq \gamma_j \Longrightarrow i \neq j$ quindi si ha $E = K(\alpha_i, \cdots, \alpha_n)$; si procede ora per induzione su n. Il passo base è ovvio quindi passiamo al passo induttivo, ora sia $E = K(\alpha_i, \cdots, \alpha_n) = K(\alpha_i, \cdots, \alpha_{n-1})(n)$ che per il passo induttivo su ha $E = K(\beta, \alpha_n)$ e riscrivo per semplicità $E = K(\beta\alpha)$ con $\alpha = \alpha_n$. Considero il polinomio $\alpha + x\beta$ ed l'applicazione $\bar{K} \ni F(x) = \prod_{i<j} (\gamma_i(\alpha + x\beta) - \gamma_j(\alpha + x\beta)) \neq 0$ infatti se lo fosse allora $\gamma_i(\alpha + x\beta) - \gamma_j(\alpha + x\beta) = 0 \Longleftrightarrow \gamma_i(\alpha) + x\gamma_i(\beta) - \gamma_j(\alpha) + x\gamma_j(\beta) \Longleftrightarrow \gamma_i = \gamma_j \Longleftrightarrow i = j$ assurdo quindi $F(x) \neq 0$ ed ha grado $\binom{2}{2}$ quindi esiste un t tale che $F(t) \neq 0$ e questo t e tale che

$\delta = \alpha + t\beta$ e $E = K(\delta)$ infatti $K(\delta) \subset E$ inoltre siccome $F(t) \neq= 0$ e $deg(F(x)) > n = [E : K]$ allora dato che $\gamma_i(\delta)$ sono tutti diversi come già notato primi allora l'orbita di δ ha almeno n elementi quindi il suo polinomio minimo ha grado almeno n quindi $E \subset K(\delta)$ per ciò $E = K(\delta)$. □

Gruppi risolubili (parentesi fuori programma) :

6.1.4 Definizione : Sia G un gruppo finito, si dice *risolubile* se ammette una serie normale con quozienti abeliani ovvero $\{e\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ e G_{i-1}/G_i è abeliano.

Proprietà :

1) G risolubile $\iff$ esiste $H \triangleleft G$ tale che H è risolubile.

2) G risolubile $\iff$ esiste n tale che $D^n(G) = \{e\}$ con $D^1(G) = [G : G]$ e $D^n(G) = [D^{n-1}(G) : D^{n-1}(G)]$.

6.1.5 Definizione : L/K si dice *risolubile per radicali* se esiste $E \subseteq L$ tale che $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = E$ e $K_i = K_{i-1}(\alpha)$ dove $\alpha = \sqrt[n]{a},\ \xi_n \in K_{i-1}$ oppure $K_i = K_{i-1}(\xi_n)$ ed E/K è di Galois.

6.1.2 Teorema : L/K risolubile $\iff$ è risolubile per radicali.

6.1.5 osservazione : S_5 non è risolubile $\implies$ non esiste una formula per per le soluzioni di un polinomio di quinto grado in quanto S_5 è un gruppo di *Galois* del generico polinomio di grado cinque.

6.2 Teorema di corrispondenza di Galois

6.2.1 Lemma : Sia M/F una estensione di Galois e $H < Gal(M/F) = G$ allora $M^H = F \iff H = G$.

Dimostrazione :

($\Longleftarrow$) : Supponiamo $H = G$ allora è chiaro che $M^G \supset F$. Sia allora $\alpha \in M^G$, se $\alpha \notin F$ allora vale $F \subset F(\alpha) \subset M$ quindi esiste $\gamma : F(\alpha) \longrightarrow \bar{F}$ tale che $\gamma|_F = Id$ e $\gamma(\alpha) \neq \alpha$. Posso estendere γ a $\tilde{\gamma} : M \longrightarrow \bar{F}$ tale che $\tilde{\gamma}|_F = Id$ e $\tilde{\gamma}(\alpha) \neq \alpha$, ora M/F è di Galois quindi $\tilde{\gamma}(M) = M$ quindi $\tilde{\gamma} \in G$ e perciò $\tilde{\gamma}$ fissa M ma $\tilde{\gamma}(\alpha) \neq \alpha$ assurdo, quindi $M^G = F$.

($\Longrightarrow$) : Sia $M = F(\alpha)$, considero $M[x] \ni f(x) = \prod_{\sigma \in H}(x - \sigma(\alpha))$ e si ha $deg(f(x)) = |H|$,

voglio dimostrare che $f(x) \in M^H[x] = F[x]$. Per ogni $\delta \in H \Longrightarrow \delta(f(x)) = \prod_{\sigma \in H}(x - \delta(\sigma(\alpha))) = \prod_{\sigma \in H}(x - \sigma(\alpha)) = f(x)$ quindi $|G| = [M : K] = deg(\mu_\alpha) < deg(f(x)) = |H|$ quindi $H = G$.

□

6.2.2 Lemma : L/K di Galois, $H < Gal(L/K)$ e $\sigma \in Gal(L/K)$. Allora $L^{\sigma H \sigma^{-1}} = \sigma L^H$.

Dimostrazione : $\sigma L^H = \sigma\{\alpha \in L \mid \gamma(\alpha) = \alpha \ \forall \gamma \in H\} = \{\sigma(\alpha) \in L \mid \gamma(\alpha) = \alpha \ \forall \gamma \in H\} = \{\beta \in L \mid \gamma(\sigma^{-1}(\beta)) = \sigma^{-1}(\beta) \ \forall \gamma \in H\} = \{\beta \in L \mid \sigma\gamma(\sigma^{-1}(\beta)) = \beta \ \forall \gamma \in H\} = L^{\sigma H \sigma^{-1}}$.

6.2.1 Teorema : (Di corrispondenza di Galois) Sia L/K di Galois finita. Allora :

1) $\Gamma : \Xi_{L/K} = \{F \mid K \subseteq F \subseteq L\} \longrightarrow G_{L/K} = \{H < Gal(L/K)\}$ tale che $\Gamma(F) = Gal(L/F)$ è una applicazione ben definta.

2) Γ è bigettiva e la sua inversa è tale che $\Gamma^{-1}(H) = L^H = Fix(H) = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \ \sigma \in H\}$, che è un campo.

3) Inoltre in questa corrispondenza si ha che $H \triangleleft G \iff L^H/K$ è di Galois, ed in questo caso $Gal(L^H/K) \cong \frac{Gal(L/K)=G}{Gal(L/L^H)=H}$ che si riassume nello schema :

$$K \xrightarrow{G/H} L^H \xrightarrow{H} L$$
$$\qquad\qquad\quad \overset{\frown}{\qquad\qquad} \qquad\quad$$
$$\qquad\qquad\quad G$$

Dimostrazione :

1) Per l'osservazione 6.1.4 l'applicazione è ben definita.

2) $\Gamma \circ \Gamma^{-1}(H) = \Gamma(L^H) = Gal(L/L^H) = H$, l'ultima uguaglianza è vera perché $H \subset Gal(L/L^H)$ dato che se $\gamma \in H$ allora $\gamma|_L^H = Id$ inoltre per il lemma 6.2.1 se $F = L^H \Longrightarrow H < gal(L/F)$ quindi $H = Gal(L/F)$ e vale l'uguaglianza. $\Gamma^{-1}\Gamma(F) = \Gamma^{-1}(Gal(L/F)) = L^{Gal(L/F)} = F$ per il lemma 6.2.1. Quindi Γ è bigettiva e Γ^{-1} è la sua inversa.

3) $H \triangleleft G \iff \sigma H \sigma^{-1} = H \ \forall \sigma \in G \iff \sigma L^H = L^H \ \forall \sigma \in G \iff L^H/K$ è di Galois, quindi ci riduciamo a dimostrare l'ultimo se e solo se.

($\Longleftarrow$) : ovvio per il lemma 6.2.2.

($\Longrightarrow$) : Se $\gamma : L^H \longrightarrow \bar{K}$ tale che $\gamma|_K$ allora γ si estende ad una $\sigma : L \longrightarrow \bar{K}$ tale che $\sigma|_{L^H} = \gamma$

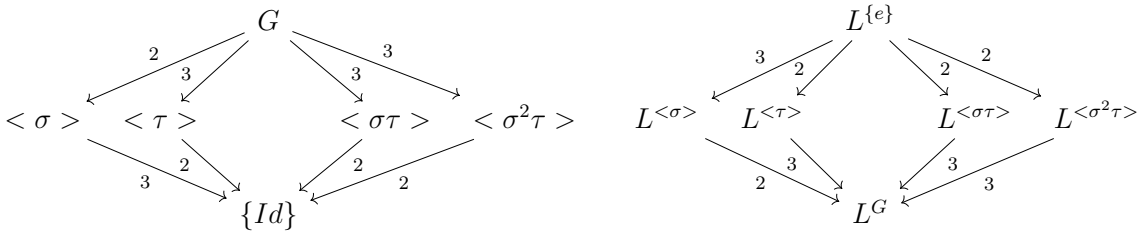
e $\sigma|_K = Id$. Considero ora $res : Gal(L/K) \longrightarrow Gal(L^H/K)$ tale che $res(\sigma) = \sigma|_{L^H}$, res è un omomorfismo ed è surgettivo infatti per ogni $\delta \in Gal(L^H/K)$, δ si estende a $\tilde{\delta} \in Gal(L/K)$ tale che $\tilde{\delta}|_{L^H} = \delta$ e $\tilde{\delta}|_K = Id$. Ora $Ker(res) = \{\sigma \in Gal(L/K) \mid res(\sigma) = \sigma|_{L^H} = Id\} = Gal(L/L^H)$ quindi $Gal(L^H/K) \cong \frac{Gal(L/K)}{Gal(L/L^H)}$ è di Galois.

□

6.2.1 esempio : Sia $L = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ il campo di spezzamento su $\mathbb{Q}$ di $x^3 - 2$. Sappiamo che $gal(L/\mathbb{Q}) \cong S_3$ considero allora :

$$\begin{array}{rcl} \sigma : \xi_3 & \longrightarrow & \xi_3 \\ \sqrt[3]{2} & \longrightarrow & \xi_3\sqrt[3]{2} \\ \xi\sqrt[3]{2} & \longrightarrow & \xi_3^2\sqrt[3]{2} \\ \xi_3^2\sqrt[3]{2} & \longrightarrow & \sqrt[3]{2} \end{array} \qquad \begin{array}{rcl} \tau : \xi_3 & \longrightarrow & \xi_3^2 \\ \sqrt[3]{2} & \longrightarrow & \sqrt[3]{2} \\ \xi_3\sqrt[3]{2} & \longrightarrow & \xi_3^2\sqrt[3]{2} \\ \xi_3^2\sqrt[3]{2} & \longrightarrow & \xi_3\sqrt[3]{2} \end{array}$$

Possiamo schematizzare l'insieme delle sotto estensioni in relazione ai sottogruppi in questo modo : ($G = Gal(L/K) \cong S_3$ e $L = L^{\{e\}}$)



$< \sigma > \triangleleft Gal(L/K) = G$ perché ha indice due quindi $L^{<\sigma>}/\mathbb{Q}$ è normale. $< \tau >, < \sigma\tau >, < \sigma^2\tau >$ non sono normali in G quindi fissano sotto estensioni non normali su $\mathbb{Q}$. $L^{<\sigma\tau>} = \{\alpha \in L \mid \sigma\tau(\alpha) = \alpha\}$, osserviamo che $\sigma\tau(\xi_3\sqrt[3]{2}) = \sqrt[3]{2}$ e $\sigma\tau(\xi_3^2\sqrt[3]{2}) = \xi_3^2\sqrt[3]{2}$ quindi $\mathbb{Q}(\xi_3^2\sqrt[3]{2}) \subseteq L^{<\sigma\tau>}$.

6.2.2 esempio : $f(x) = x^4 - 2$, L campo di spezzamento su $\mathbb{Q}$ allora $L = \mathbb{Q}(\sqrt[4]{2}, i)$. $Gal(L/K)$ è sottogruppo di S_4 ed ha ordine 8, quindi è il suo 2-sylow perciò $Gal(L/K) \cong D_4$.

6.2.1 Corollario : (Da vedere) Dal teorema di corrispondenza derivano tre proprietà; sia L/K di Galois e $H, S < Gal(L/K)$ allora :

1) $H \subset S \iff L^H \supset L^S$.

2) $L^H L^S = L^{H \cap S}$.

3) $L^H \cap L^S = L^{<H,S>}$

Dimostrazione :

1) Per ogni $\omega \in L^S$ e per ogni $\gamma \in S$ si ha che $\gamma(\omega) = \omega$ ma siccome $H \subset S$ allora per ogni $\tau \in H$ si ha che $\tau(\omega) = \omega$ quindi $\omega \in L^H$ perciò $L^S \subset L^H$.

2) Banalmente $L^{H \cap S} \subset L^H L^S$, ora per ogni $\alpha\beta \in L^H L^S$ e per ogni $\gamma \in H \cap S$ si ha che $\gamma(\alpha\beta) = \gamma(\alpha)\gamma(\beta) = \alpha\beta$ quindi $L^H L^S \subset L^{H \cap S}$ e quindi $L^H L^S = L^{H \cap S}$.

3) Sia $\alpha \in L^{<H,S>}$, in particolare per ogni $\gamma \in H$ e per ogni $\tau \in S$ si ha che $\gamma(\alpha) = \tau(\alpha) = \alpha$. Ora per ogni $\alpha \in L^H \cap L^S$, se prendiamo $\sigma \in < H, S >$ allora $\sigma = h_1 s_1 \cdots h_n s_n$ dove $h_i \in H$ e $s_i \in S$, ma per ogni i, $h_i(\alpha) = s_i(\alpha) = \alpha$ quindi $\sigma(\alpha) = \alpha$ perciò $L^H \cap L^S = L^{<H,S>}$.

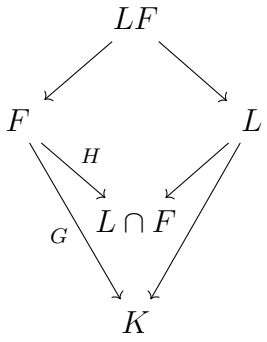
□

6.2.1 Proposizione : Sia L/K estensione di Galois finita e siano $L, F \subset E$. Allora

1) LF/F è di Galois.

2) $Gal(LF/F) \cong Gal(L/L \cap F)$.

Dimostrazione : Consideriamo innanzi tutto il diagramma delle inclusioni (da vedere grafico)



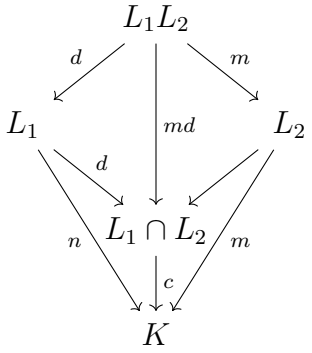
LF/F è normale infatti per ogni $\gamma : LF \longrightarrow \bar{F}$ tale che $\gamma|_F = Id_F$ si ha che $\gamma|_L \in Aut(L/K)$ perchè $\gamma|_K = Id$ dato che $K \subset F$ e quindi si ha che $\gamma : L \longrightarrow \bar{K}$, siccome L/K è normale $\gamma|_L \in Aut(L/K) = Gal(L/K)$ quindi $\gamma|_L = Id_L$ in conclusione $\gamma(LF) = \gamma(L)\gamma(F) = \gamma|_L(L)\gamma|_F(F) =$

$Id|_L(L)Id|_F(F) = LF$, quindi LF/F è di Galois. Ora voglio vedere che $res : Gal(LF/F) \hookrightarrow Gal(L/K)$ tale che $res(\gamma) = \gamma|_L$, $Ker(res) = \{\gamma \in Gal(LF/F) \mid \gamma|_L = Id\} = Id$ dato che $\gamma|_F = Id$ allora è l'identità su tutto LF, dico che se $H = res(Gal(LF/F)) \Longrightarrow L^H = L \cap F$. Infatti sia $\alpha \in L \cap F$ allora per ogni $\gamma(\alpha) = \alpha$ quindi $\alpha \in L^H$ infine sia $\beta \in L^H$ allora $\beta \in L \Longrightarrow \beta \in LF$ e $\beta \in FIX(Gal(LF/F)) \Longrightarrow \beta \in F$ infatti $L^H = \{\alpha \in L \mid \gamma|_L(\alpha) = \alpha \ \forall \ \gamma|_L \in H\} = \{\alpha \in L \mid \gamma|_L(\alpha) = \alpha \ \forall \ \gamma \in Gal(LF/F)\} \subset LF^{Gal(LF/F)} = F$ (In conclusione $Fix(res(Gal(LF/F))) = L \cap F \Longrightarrow res(Gal(LF/F)) = L/L \cap F$ da vedere).

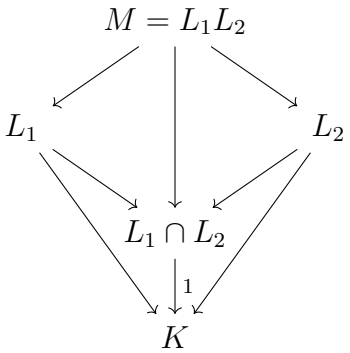
□

6.2.2 Proposizione : L_1/K, L_2/K di Galois, se $M = L_1L_2 \Longrightarrow M/K$ è di Galois e vale $Gal(L_1L_2/K) \hookrightarrow Gal(L_1/K) \times Gal(L_2/K)$ inoltre si ha l'isomorfismo se e solo se $L_1 \cap L_2 = K$, questa condizione dice che L_1/K e L_2/K sono *linearmente disgiunte su* K.

Dimostrazione : Consideriamo innanzi tutto il diagramma delle inclusioni



si ha che $c|(m,n)$, se $(m,n) = 1 \Longrightarrow L_1/K$ e L_2/K sono linearmente disgiunte quindi si ha $c = 1$ e $d = n$. Ora consideriamo $res : Gal(L_1L_2/K) \longrightarrow Gal(L_1/K) \times Gal(L_2/K)$ tale che $res(\gamma) = (\gamma|_{L_1}, \gamma|_{L_1})$ e il diagramma

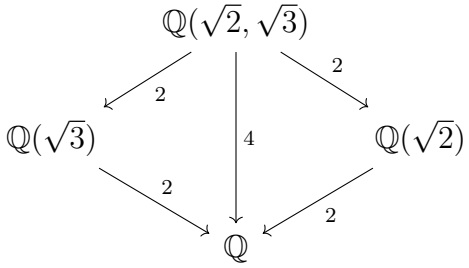


si ha allora che $Ker(res) = \{\gamma \in Gal(L_1L_2/K) \mid \gamma|_{L_1} = Id,\ \gamma|_{L_2} = Id\} = Id$, inoltre $G = Gal(L_1L_2/K) = Gal(M/K)$ e considero $H_1,\ H_2 \triangleleft G$ late che $L_1 = M^{H_1}$ e $L_2 = M^{H_2}$ si ha quindi che $Gal(L_i/K) = G/H_i$ e perciò $G \hookrightarrow G/H_1 \times G/H_2$ ora il nucleo è $H_1 \cap H_2 = \{e\}$ perch'e $M^{H_1 \cap H_2} = M^{H_1}M^{H_2} = L_1L_2$ quindi $K = L_1 \cap L_2 = M^{H_1} \cap M^{H_2} = M^{<H_1,H_2>} \iff H_1H_2 = G$ ma $H_1 \cap H_2 = e \Longrightarrow G \cong H_1 \times H_2$ dove vale $G/H_1 \cong H_2$ e $G/H_2 \cong H_1$.

□

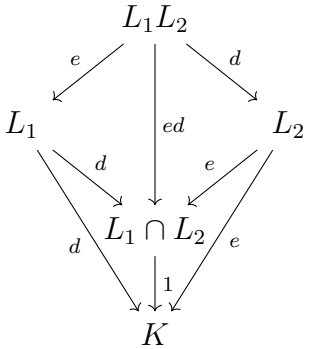
6.2.1 osservazione : L'essere linearmente disgiunte no ha a che fare con la normalità.

6.2.3 esempio :



6.2.1 esercizio : Siano L_1/K e L_2/K, sono linearmente disgiunte $\iff [L_1L_2 : L_1 \cap L_2] = mn$.

soluzione : ($\Longleftarrow$) è ovvia, per ($\Longrightarrow$) considerando il diagramma delle inclusioni



si ha la tesi.

6.3 Applicazioni di Galois

*Estensioni di radici primitive ennesime dell'unit*à :

Sia ξ_n una radice primitiva ennesimo dell'unità, $\xi_n \in \bar{\mathbb{Q}}^*$ e ha ordine n, il suo polinomio minimo in $\mathbb{Q}$ divide il polinomio $x^n - 1 = \prod_{i=0}^{n}(x - \xi_n^i)$ ed ha grado pari al numero dei coniugati di ξ_n. Voglio dire che il numero dei coniugati di ξ_n, ovvero gli ξ_n^i tale che $ord(\xi_n^i) = ord(\xi_n)$, è $\phi(x)$ e che quindi $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n) = deg(\mu_{\xi_n}(x))$ dove $\mu_{\xi_n}(x)$ è il polinomio minimo di ξ_n in $\mathbb{Q}$.

6.3.1 Proposizione : Tutte le radici di $\mu_{\xi_n}(x)$ hanno ordine multiplo di n, ovvero sono del tipo ξ_n^i con $(i, n) = 1$ quindi sono al più $\phi(n)$.

Dimostrazione : Devo dimostrare che per ogni i con $(i, n) = 1$ si ha che ξ_n^i è radice di $\mu_{\xi_n}(x)$ o equivalentemente che non è radice di $g(x) = \frac{x^n-1}{\mu_{\xi_n}(x)}$. Mostro innanzi tutto che se ξ è radice di $\mu_{\xi_n}(x)$ e $(p, n) = 1$, p primo, allora ξ^p ràdice di $\mu_{\xi_n}(x)$. Procedo per assurdo, supponiamo che ξ^p non é radice di $\mu_{\xi_n}(x)$ allora $g(\xi^p) = 0$, quindi ξ è radice di $g(x^p)$ quindi $\mu_{\xi_n}(x)|g(x^p) = \mu_{\xi_n}(x)h(x)$, riduco modulo p ed ottengo che $g(\bar{x^p}) = (g(\bar{x}))^p = \bar{\mu_{\xi_n}}(x)\bar{h}(\bar{x})$ quindi $(\bar{\mu_{\xi_n}}(x), (g(\bar{x}))) \neq 1$ di conseguenza $x^n \bar{-} 1 = \bar{\mu_{\xi_n}}(x)g(\bar{x})$ ha radici multiple, ma $x^n \bar{-} 1' = n(x^n - 1) \neq 0$ perchè $(p, n) = 1$ quindi è assurdo perciò ξ^p è radice di $\mu_{\xi_n}(x)$ per ogni p primo tale che $(p, n) = 1$. Ora abbiamo che per ogni i tale che $(i, n) = 1$ si ha che ξ_n^i è radice di $\mu_{\xi_n}(x)$ infatti supponiamo che $i = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, p_i primi distinti con $p_i \not| n$, usando quanto detto prima se ξ_n è radice allora $\xi_n^{p_1}$ e radice ma a sua volta $\xi_n^{p_1^2}$ è radice e iterando si ha ξ_n^i è radice di $\mu_{\xi_n}(x)$, quindi $\mu_{\xi_n}(x) = \prod_{\substack{(i,n)=1 \\ i=2,\cdots,n}}(x - \xi_n^i)$, con ciò si ha che siano $\sigma_i : \mathbb{Q}(\xi_n) \longrightarrow \bar{\mathbb{Q}}$ tale che $\sigma_i(\xi_n) = \xi_n^i$ allora $Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}) = \{\sigma_1 \mid (i, n) = 1\} \cong \mathbb{Z}/^*_{n\mathbb{Z}}$, ísomorfismo manda σ_i in i, e si ha anche che $\sigma_i \circ \sigma_j = \sigma_{ij}$ infatti $\sigma_i \circ \sigma_j(\xi_n) = \sigma_i(\xi_n^j) = \xi_n^{ij}$.

□

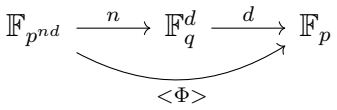
Gruppi di Galois per campi finiti :

6.3.1 Teorema : $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) =< \Phi >$ dove $\Phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ tale che $\Phi(x) = x^p$ è l'omomorfismo di Frobenius.

Dimostrazione : Sia *Phi* l'omomorfismo di Frobenius, dimostro che $\Phi \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Per ogni $a \in \mathbb{F}_p$, $\Phi(a) = a^p = a$, per ogni $x, y\mathbb{F}_{p^n}$ si ha che $\Phi(x + y) = (x + y)^p = x^p + y^p = \Phi(x) + \Phi(y)$, poi $\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$, si ha inoltre che $|Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$, ora supponiamo che $ord(\Phi) = k$ allora $\Phi^k(x) = x^{p^k} = x$ per ogni $x \in \mathbb{F}_{p^n}$ quindi il polinomio $x^{p^k} - x$ ha p^n radici in $\mathbb{F}_{p^n}$ quindi $k > n$ quindi $k = n$.

□

6.3.1 Corollario : Sia $q = p^d$ si ha che $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) < Gal(\mathbb{F}_{p^{nd}}/\mathbb{F}_p) \Longrightarrow Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = < \Phi^d >$ come si vede dal diagramma

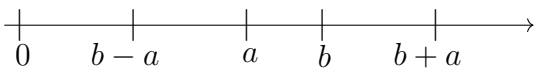


6.4 Costruzioni con riga e compasso

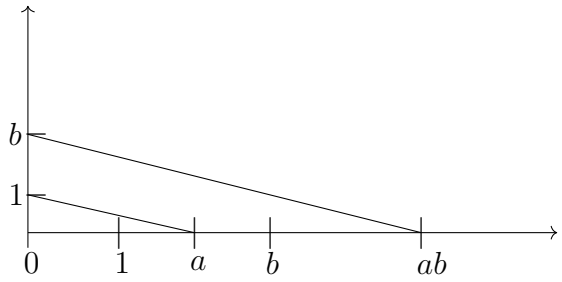
Vogliamo formalizzare matematicamente la costruzione con riga e compasso, diciamo innanzi tutto che il compasso si punto solo su punti costruiti o dati e la riga traccia rette per due punti costruiti o dati. Dati una retta ed un punto esterno alla retta, sappiamo costruire la retta perpendicolare e passante per quel punto, dato un segmento sappiamo costruire il punto medio, e data una retta sappiamo costruire parallele e perpendicolari delle parallele.

6.4.1 teorema : Sia $K = \{x \in \mathbb{R} \mid x \text{ è costruibile}\}$. Allora $\mathbb{Q} \subset K$ è un campo ed è chiuso rispetto alla radice quadrata di $a \in K$ se $a \geq 0$.

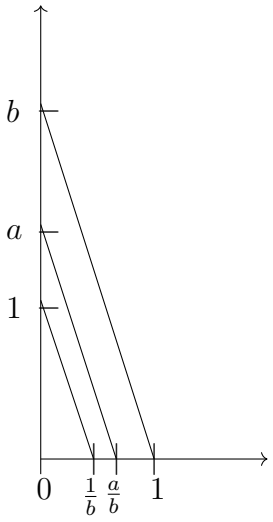
Dimostrazione : consideriamo $a, b \in \mathbb{R}$, allora posso costruire $b-a$ e $b+a$ infatti se considero la retta reale e due punti a e b, se punto il compasso in b e lo apro fino ad a, allora se traccio la circonferenza, questa si ri-interseca sulla retta in $a + b$, se invece come prima lo punto in b con apertura fino ad a ma poi lo punto in 0 mantenendo l'apertura e traccio la circonferenza, allora questa interseca la retta in $b - a$ nella parte positiva, come in figura



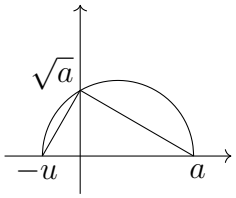
Quindi posso sottrarre e sommare. Ora se considero il piano reale, come in figura



Considero a eb sull'asse orizzontale e traccio la retta passante per a e per 1 dell'asse verticale, e poi traccio la retta parallela a quella tracciata prima e passante per b che stà sull'asse verticale, l'intersezione di quest'ultima retta con l'asse orizzontare e ab. Analogamente posso dividere, sempre a e b traccio la retta passante per 1 dell'asse orizzontale e b sull'asse verticale e traccio la retta parallela a questa e passante per a dell'asse verticale, l'intersezione di quest'ultima con l'asse orizzontale è $\frac{a}{b}$, come nel disegno



Quindi è un campo. Osserviamo adesso che perso a, posso costruire $\sqrt{a}$, consideriamo il disegno :



Consideriamo a, u è l'unità ovvero $\frac{a}{a} = u$ e considero il segmento da $-u$ a a, costruisco la circonferenza che ha come centro il punto medio tra $-u$ ed a e raggio $\frac{a+u}{2}$, allora l'intersezione della circonferenza con l'asse verticale è $\sqrt{a}$ infatti come nel disegno ci si può inscrivere un triangolo rettangolo allora per le proprietà di similitudine (consideriamo x l'intersezione tra la circonferenza e l'asse verticale) si ha che$u : x = x : a \Longrightarrow x^2 = ua = a \Longrightarrow x = \sqrt{a}$.

□

6.4.2 Teorema : Sia $L = \{\alpha \in \mathbb{C} \mid \alpha \text{ è costruibile}\}$, L è un campo e per ogni $\alpha \in L \Longrightarrow \sqrt{a} \in L$.

Dimostrazione : $\alpha = a + ib \in L \Longleftrightarrow a, b \in K$ quindi L è campo perché K è campo, inoltre $\sqrt{a}$ lo so costruire perché so costruire le bisettrici.

□

6.4.1 osservazione : I punti p costruibili sono intersezioni di rette e circonferenze con coefficienti in K.

6.4.3 Teorema : $\alpha \in L \Longleftrightarrow$ esiste una successione $L_0 = \mathbb{Q} \subset L_1 \subset \cdots \subset L_n$ di campi con $\alpha \in L_n$ e $[L_{i+1} : L_i] = 2$ per ogni i.

Dimostrazione :

($\Longrightarrow$) : Supponiamo α costruibile. Siano $z_0, z_1, \cdots, z_n$ i punti costruiti per ottenere α, ora z_{i+1} è costruito a partire da $z_0, \cdots, z_i$ e quindi è intersezione di rette e circonferenze co coefficienti in $\mathbb{Q}(z_0, \cdots, z_i) = L_i$ siccome le rette e le circonferenze sono equazioni di secondo grado si ha che $L_{i+1} = L_i$ e $[L_{i+1} : L_i] \in \{1, 2\}$.

($\Longleftarrow$) : Si ha $\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_n$, prendo $\alpha \in L_n$ e dico che α è costruibile. Procedo per induzione , se $n = 0$ ok. Ora fino a L_{n-1} sono costruibili, consideriamo quindi $L_n = L_{n-1}(\alpha)$ e $\alpha = \sqrt{\beta}$ con $\beta \in L_{n-1}$ ma β è costruibile quindi $\alpha = \sqrt{\beta}$ è costruibile.

□

6.4.1 Corollario : $z \in L \Longrightarrow [\mathbb{Q}(z) : \mathbb{Q}] = 2^n$.

6.4.2 osservazione : Non si può costruire con riga e compasso un poligono di 7 lati regolare infatti $[\mathbb{Q}(\xi_7) : \mathbb{Q}] = \phi(7) = 6 \neq 2^k$ per ogni k.

6.4.3 osservazione : Il viceversa del corollario 6.4.1 è falso infatti sia $p(x) \in \mathbb{Q}[x]$ irriducibile con $\partial p = 2^m$, α radice di $p(x)$ quindi$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$. Se $Gal(K_{p(x)}/K) \cong S_{2^m} \Longrightarrow \alpha$ non è costruibile, perchè non è risolubile.

6.5 Esercizi

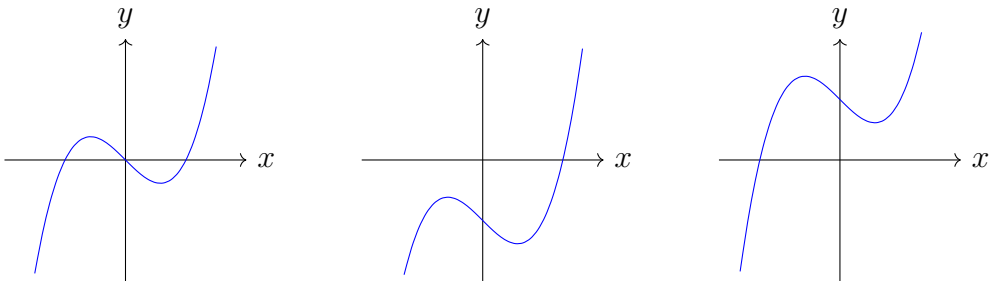
Sia $P(x) = x^3 + ax^2 + bx^+c \in \mathbb{Q}[x]$, se facciamo la sostituzione $x = x' + \frac{a}{3}$ allora $p(x') = x^3 + b'x + c'$ quindi possiamo sempre supporre $a = 0$ tanto con una traslazione ci riportiamo a tutti i casi. Sappiamo inoltre che se $p(x)$ è irriducibile su $\mathbb{Q}$ il gruppo di Galois di L/K dove L è il campo di spezzamento di $p(x)$ è isomorfo a S_3 oppure ad A_3.

6.5.1 esercizio : Determinare il gruppo di Galois di :

1) $x^3 - x + 1$.

2) $x^3 - 3x + 1$.

soluzione : Consideriamo in generale $x^3 + ax + b$, si ha che $f' = 3x^2 + a$ e $f'(x) = 0 \iff x_{1,2} = \pm\sqrt{-\frac{a}{3}}$, ed abbiamo che $f(x_1) = -\frac{a}{3}\sqrt{-\frac{a}{3}} + a\sqrt{-\frac{a}{3}} + b$ e $f(x_2) = \frac{a}{3}\sqrt{-\frac{a}{3}} - a\sqrt{-\frac{a}{3}} + b$, se li moltiplichiamo abbiamo $f(x_1)f(x_2) = b^2 + \frac{4a^3}{27} = \Delta$. Il Δ è il prodotto del massimo e minimo relativo della curva



come si vede dal disegno se il massimo relativo e minore di 0 o il minimo relativo e maggiore di 0 si ha una soluzione reale se no tre e questo si può distinguere con la positività del

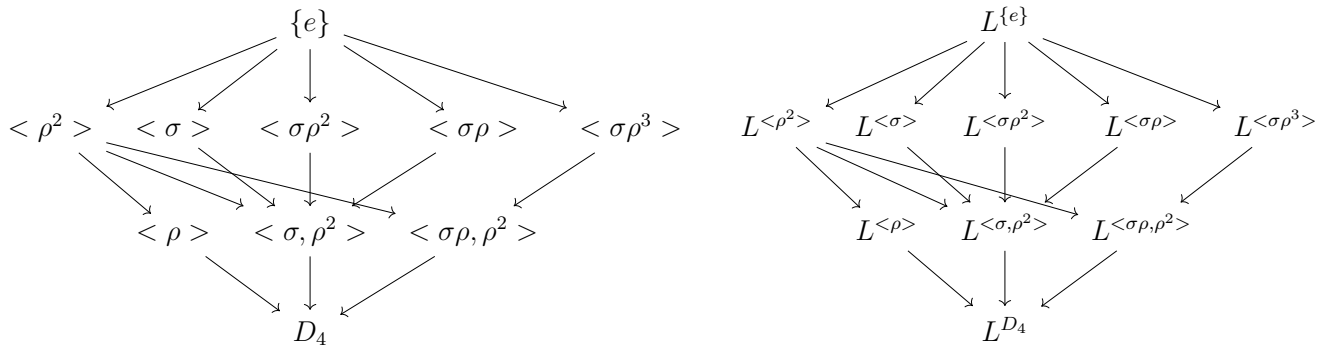
Δ infatti se è positivo implica una soluzione reale se no tre reali. Ritornando all'esercizio si ha che per $x^3 - x + 1$ il $\Delta = 1 - \frac{4}{27} > 0 \Longrightarrow S_3$ infatti il suo gruppo di Galois si immerge in S_3, 3 divide la sua cardinalità ed inoltre il coniugio che scambia le due radici complesse è un elemento del gruppo ed ha ordine due, invece per $x^3 - 3x + 1$ il $\Delta = 1 - 4 < 0$ quindi ha tre radici reali $\alpha_1, \alpha_2, \alpha_3 \in K$, K campo di spezzamento di $x^3 - 3x + 1$, ma non possiamo concludere niente. Consideriamo $\sigma = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in K$ consideriamo ora il gruppo di Galois $G = Gal(K/\mathbb{Q})$ e facciamolo agire su K, allora $\sigma \longrightarrow \pm\sigma$ si ha che se tutte le permutazioni sono pari si ha $G = A_3$ e $\sigma \in \mathbb{Q}$ se no $G = S_3$ e $\sigma \notin \mathbb{Q}$. Ora $\sigma^2 = -4a^3 - 27b^2 = -27\Delta$ perché so che $\alpha_1 + \alpha_2 + \alpha_3 = 0, \alpha_1\alpha_2\alpha_3 = -b$ e $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = a$ quindi in conclusione se σ^2 è un quadrato in $\mathbb{Q} \Longrightarrow \sigma \in \mathbb{Q} \Longrightarrow G = A_3$, $\sigma^2 \in \mathbb{Q}$ ma non è un quadrato $\Longrightarrow \sigma \notin \mathbb{Q} \Longrightarrow G = S_3$, in conclusione per $x^3 - x + 1$ ho $\sigma^2 = 4 - 27 = -23$ non è un quadrato $\Longrightarrow G = S_3$, in $x^3 - 3x + 1$ ho $\sigma^2 = 4 \cdot 3^3 - 3^3 = 3^4 = (3^2)^2$ è un quadrato $\Longrightarrow G = A_3$.

6.5.2 esercizio : Determinare le corrispondenze di Galois tra le sotto estensioni del campo di spezzamento L di $x^4 - 2$ ed i sottogruppi del gruppo di Galois $G = Gal(L/\mathbb{Q})$.

soluzione : Osserviamo che $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$, quindi $L = \mathbb{Q}(i, \sqrt[4]{2})$ (da vedere), si ha inoltre che $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$, si immerge in S_4 quindi è un D_4, voglio vedere come sono fatti gli automorfismi. Abbiamo che una radice deve avere immagine in un'altra radice quindi se $\gamma \in G$ allora $\gamma(\sqrt[4]{2})$ ha quattro possibili immagini poi $\gamma(-\sqrt[4]{2}) = -\gamma(\sqrt[4]{2})$ ed è già determinato dal precedente, poi si ha $\gamma(i\sqrt[4]{2}) = \gamma(i)\gamma(\sqrt[4]{2})$ che ha altre due possibili immagini, ed infine $\gamma(-i\sqrt[4]{2}) = -\gamma(i\sqrt[4]{2})$; supponiamo ora di rinominare le radici $\{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$ rispettivamente con $\{1, 2, 3, 4\}$ si ha che :

$$\begin{array}{ll} \sigma : \begin{array}{c}\sqrt[4]{2} \longmapsto -\sqrt[4]{2} \\ i \longmapsto -i\end{array} & (1,2) \\ \rho : \begin{array}{c}\sqrt[4]{2} \longmapsto i\sqrt[4]{2} \\ i \longmapsto i\end{array} & (1,3,2,4) \\ \rho^2 : \begin{array}{c}\sqrt[4]{2} \longmapsto -\sqrt[4]{2} \\ i \longmapsto i\end{array} & (1,2)(3,4) \\ \rho^3 : \begin{array}{c}\sqrt[4]{2} \longmapsto -i\sqrt[4]{2} \\ i \longmapsto i\end{array} & (1,4,2,3) \end{array} \qquad \begin{array}{ll} \sigma\rho : \begin{array}{c}\sqrt[4]{2} \longmapsto i\sqrt[4]{2} \\ i \longmapsto -i\end{array} & (1,3)(2,4) \\ \sigma\rho^2 : \begin{array}{c}\sqrt[4]{2} \longmapsto \sqrt[4]{2} \\ i \longmapsto -i\end{array} & (3,4) \\ \sigma\rho^3 : \begin{array}{c}\sqrt[4]{2} \longmapsto -i\sqrt[4]{2} \\ i \longmapsto -i\end{array} & (1,4)(2,3) \\ Id : \begin{array}{c}\sqrt[4]{2} \longmapsto \sqrt[4]{2} \\ i \longmapsto i\end{array} & e \end{array}$$

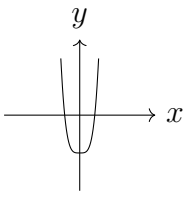
In D_4 i sottogruppi di indice due sono $< \rho >$, $< \sigma, \rho^2 >$, $< \sigma\rho, \rho^2 >$, i sottogruppi di indice quattro sono $< \rho^2 >$, $< \sigma >$, $< \sigma\rho >$, $< \sigma\rho^2 >$, $< \sigma\rho^3 >$ e poi c'è $\{e\}$ quindi si ha il diagramma di inclusioni



esplicitamente si ha $L^{<\rho^2>} = \mathbb{Q}(\sqrt{2}, i),\ L^{\sigma} = \mathbb{Q}(i\sqrt[4]{2}),\ L^{<\sigma\rho^2>} = \mathbb{Q}(\sqrt[4]{2}),\ L^{<\sigma\rho>} = \mathbb{Q}(\sqrt[4]{2}(i+1)),\ L^{<\sigma\rho^3>} = \mathbb{Q}(\sqrt[4]{2}(i-1)),\ L^{<\rho>} = \mathbb{Q}(i),\ L^{<\sigma,\rho^2>} = \mathbb{Q}(\sqrt{2}),\ L^{<\sigma\rho,\rho^2>} = \mathbb{Q}(i\sqrt{2})$.

6.5.3 esercizio : Trovare il gruppo di Galois del campo di spezzamento del polinomio $p(x) = x^5 - 4x + 2$.

soluzione : Il polinomio è irriducibile su $\mathbb{Q}$ per Eisenstein, sappiamo che il gruppo di Galois si immerge in S_5 ed ha almeno un elemento di ordine 5. Ora $p'(x) = 5x^4 - 4$ che ha due radici come si vede dal grafico



Allora $p(x)$ ha una o tre radici reali, ma $p(1) < 0$ quindi ha tre radici reali e due complesse. Abbiamo un elemento di ordine 5 e siccome ci sono due radici complesse c'è il coniugio che le scambia ed ha ordine 2, osserviamo che S_5, siccome 5 è primo, è generato da un 5-ciclo ed un qualsiasi 2-ciclo quindi $G = S_5$.

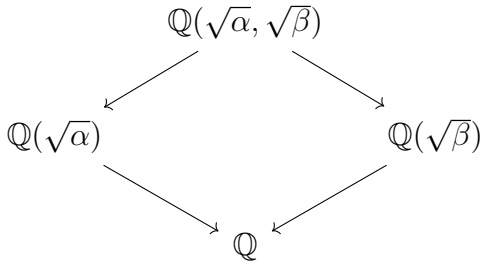
6.5.4 esercizio : Studiare il gruppo di Galois dei seguenti polinomi :

1) $x^4 + 4x^2 + 1$

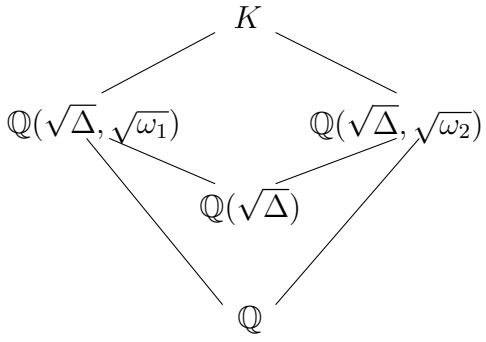
2) $x^4 - 4x^2 + 2$

3) $x^4 + 4x^2 - 2$

soluzione : Facciamo uno studio generale partendo da $p(x) = x^4 + ax^2 + b$. Consideriamo il polinomio $q = t^2 + at + b$, il $\Delta = a^2 - 4b$, siccome le radici di q sono della forma $\frac{-a \pm \sqrt{\Delta}}{2}$ allora abbiamo che i campo di spezzamento di q è $\mathbb{Q}(\sqrt{\Delta})$ che è contenuto nel campo di spezzamento di p, ora abbiamo due casi, se Δ è un quadrato in $\mathbb{Q}$ allora p si fattorizza come $(x^2 - \alpha)(x^2 - \beta)$ e abbiamo il diagramma di inclusioni



se nessuno tra α, β è un quadrato abbiamo che $\mathbb{Q}(\sqrt{\alpha})$ e $\mathbb{Q}(\sqrt{\beta})$ sono sotto estensioni normali perché di grado due quindi $G \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$, se uno fra α, β è un quadrato abbiamo che $G \cong \mathbb{Z}/_{2\mathbb{Z}}$ se sono entrambi quadrati si ha $G = \{e\}$. Possiamo allora supporre che Δ non sia un quadrato allora p si fattorizza in $\mathbb{Q}(\sqrt{\Delta})$ come $(x^2 - \omega_1)(x^2 - \omega_2)$ e di conseguenza si ha il diagramma di inclusioni



a questo punto notiamo che $\sqrt{\omega_1}\sqrt{\omega_2} = \sqrt{b}$ quindi ci sono 3 ulteriori casi, se b è un quadrato in $\mathbb{Q}$ allora $\sqrt{\omega_1} \in \mathbb{Q}(\sqrt{\omega_2})$ e viceversa, se b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$ ma non in $\mathbb{Q}$ allora $\sqrt{\omega_1} \in \mathbb{Q}(\Delta, \sqrt{\omega_2})$ e viceversa, infine se b non è un quadrato ne in $\mathbb{Q}(\sqrt{\Delta})$ ne in $\mathbb{Q}$ allora si ha

il campo $\mathbb{Q}(\Delta, \omega_1, b)$. Ora risolviamo gli esercizi :

1) $p(x) = x^4+4x^2+1$, $b = 1$ è un quadrato in $\mathbb{Q}$ e $\Delta = 12$ allora in $\mathbb{Q}(\Delta) = \mathbb{Q}(2\sqrt{3})$ il polinomio si fattorizza in $(x^2+2-\sqrt{3})(x^2+2+\sqrt{3})$, mi chiedo se $x^2+2-\sqrt{3}$ ha soluzione in $\mathbb{Q}(\sqrt{3})$, se fosse vero esisterebbero $a, b \in \mathbb{Q}$ tale che $x = a+b\sqrt{3} \Longrightarrow x^2 = a^2+3b^2+ab\sqrt{3} \Longrightarrow \left\{ \begin{smallmatrix} a^2+b^2=-2 \\ 2ab=1 \end{smallmatrix} \right.$ ma questa non ha soluzione in $\mathbb{Q}$ quindi $x^2+2-\sqrt{3}$ non ha soluzione in $\mathbb{Q}(\sqrt{3})$ allora estendo a $K = \mathbb{Q}(\sqrt{3}, \sqrt{\sqrt{3}-2})$ e questo è il campo di spezzamento, in generale si avrebbe $K = \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}, \sqrt{b}) = \mathbb{Q}(2\sqrt{3}, \sqrt{\sqrt{3}-2}, 1) = \mathbb{Q}(\sqrt{3}, \sqrt{\sqrt{3}-2})$. Ora osserviamo che $[K : \mathbb{Q}] = 4$ e che

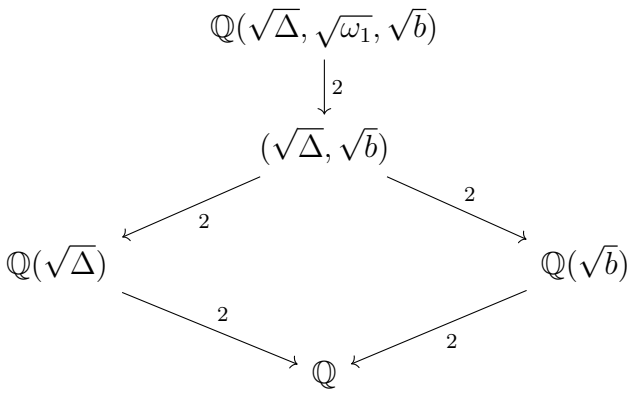
$$\begin{array}{cc} q_1 : \sqrt{\omega_1} \longrightarrow \sqrt{\omega_2} & q_2 : \sqrt{\omega_1} \longrightarrow -\sqrt{\omega_2} \\ \sqrt{\omega_2} \longrightarrow \sqrt{\omega_1} & \sqrt{\omega_2} \longrightarrow -\sqrt{\omega_1} \end{array}$$

$$\begin{array}{cc} q_3 : \sqrt{\omega_1} \longrightarrow -\sqrt{\omega_1} & q_4 : \sqrt{\omega_1} \longrightarrow \sqrt{\omega_1} \\ \sqrt{\omega_2} \longrightarrow -\sqrt{\omega_2} & \sqrt{\omega_2} \longrightarrow \sqrt{\omega_2} \end{array}$$

sono gli elementi di $Gal(K/\mathbb{Q}) \Longrightarrow Gal(K/\mathbb{Q}) \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$.

2) $p(x) = x^4-4x^2+2$, $\Delta = 8 \Longrightarrow \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{2})$, $b = 2$ non è un quadrato in $\mathbb{Q}$ ma lo è in $\mathbb{Q}(\sqrt{\Delta})$, in quest'ultimo $p(x)$ si fattorizza in $(x^2-2x\sqrt{2})(x^2-2-\sqrt{2})$, mi chiedo se $(x^2-2-\sqrt{2})$ si fattorizza in $\mathbb{Q}(\sqrt{2})$, trovo $x = a+b\sqrt{2}$ come prima, allora si ha $x^2 = a^2+2b^2+2ab\sqrt{2} \Longrightarrow \left\{ \begin{smallmatrix} a^2+b^2=2 \\ 2ab=1 \end{smallmatrix} \right.$ svolgendo il sistema si trova che non può esserci soluzione quindi estendo a $K = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})$ ed il gruppo di Galois è $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/_{4\mathbb{Z}}$ infatti $[K : \mathbb{Q}] = 4$ e $\begin{array}{c} q : \sqrt{\omega_1} \longrightarrow \sqrt{\omega_2} \\ \sqrt{\omega_2} \longrightarrow -\sqrt{\omega_1} \end{array}$ ha ordine 4.

3) $p(x) = x^4+4x^2-2$, $\Delta = 24 \Longrightarrow \mathbb{Q}(\Delta) = \mathbb{Q}(\sqrt{6})$, $b = -2$ non è quadrato ne in $\mathbb{Q}$ ne in $\mathbb{Q}(\Delta)$, $p(x)$ si fattorizza in $\mathbb{Q}(\sqrt{6})$ in $(x^2-2-\sqrt{6})(x^2+2-\sqrt{6})$ con dei conti del tutto analoghi ai precedenti si vede che $2+\sqrt{6}$ non è un quadrato in $\mathbb{Q}(\sqrt{6})$ allora estendo a $\mathbb{Q}(\sqrt{6}, \sqrt{-2\sqrt{6}})$, usando lo studio precedente ottengo che il campo di spezzamento è $\mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}, \sqrt{b}) = \mathbb{Q}(\sqrt{6}, \sqrt{-2\sqrt{6}}, \sqrt{-2})$ che ha grado 8 come si vede dal diagramma



si immerge in S_4 quindi è un 2-sylow di S_4 e perciò $Gal(K/\mathbb{Q}) \cong D_4$.

6.5.5 esercizio : Sia $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[4]{6})$, determinare :

1) $[K : \mathbb{Q}]$.

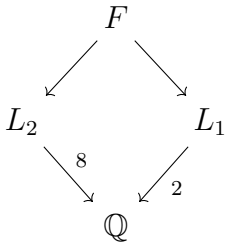
2) F minima estensione di K normale su $\mathbb{Q}$ e determinare $Gal(F/\mathbb{Q})$.

3) Contare e esibire le sotto estensioni $L \subset F$ tale che $[L : \mathbb{Q}] = 2$.

soluzione :

1) Noto subito che $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[4]{6}) = \mathbb{Q}(\sqrt{2}, \sqrt[4]{6})$. Mi chiedo se $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{6})$, se ci appartenesse avremo che anche $\sqrt{3} \in \sqrt[4]{2}$ quindi si ha che $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt[4]{6})$ e $[\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}] = 4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ ma $\mathbb{Q}(\sqrt[4]{6})$ non è di Galois perché il suo polinomio minimo è $x^4 - 6$ ed ha radici $\pm\sqrt[4]{6}, \pm i\sqrt[4]{6}$. In conclusione $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{6})(\sqrt{2}) : \mathbb{Q}(\sqrt[4]{6})][\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}] = 8$.

2) $F/\mathbb{Q}$ è la chiusura di Galois di $K\mathbb{Q}$, F è campo di spezzamento di $(x^2 - 2)(x^4 - 6)$ quindi $F = \mathbb{Q}(\sqrt[4]{6}, \sqrt{2}, i) = K(i)$ e siccome $K \subset \mathbb{R} \Longrightarrow [F : \mathbb{Q}] = 16$ con le torri di estensione, ora $L_1 = \mathbb{Q}(\sqrt[4]{6}, i)$ e $L_2 = \mathbb{Q}(\sqrt{2})$ sono linearmente disgiunte quindi $Gal(F/\mathbb{Q}) \cong Gal(L_1/\mathbb{Q}) \times L_2/\mathbb{Q} \cong D_4 \times \mathbb{Z}/_{2\mathbb{Z}}$ e si ha il diagramma

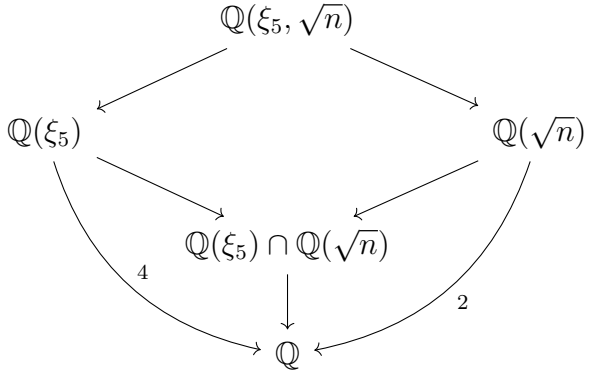


3) Sia $L \subset F$ tale che $[L:\mathbb{Q}] = 2 \Longrightarrow L = F^H$ con $G/H \cong \mathbb{Z}/_{\mathbb{Z}} \Longrightarrow H \supset G' \cong \mathbb{Z}/_{\mathbb{Z}} \times \{0\}$, allora $\{H \triangleleft G \mid [G:H] = 2\} \leftrightarrow \{\bar{H} < G/G' \mid [G/G' : \bar{H}] = 2\}$ quindi $G/G' \cong D_4/\mathbb{Z}/_{\mathbb{Z}} \times \mathbb{Z}/_{\mathbb{Z}} \cong (\mathbb{Z}/_{\mathbb{Z}})^3$ ora devo trovare tutti i sottogruppi di indice 2 e sono della forma $\mathbb{Z}/_{\mathbb{Z}} \times \mathbb{Z}/_{\mathbb{Z}}$ e sono $\frac{(2^3-1)(2^3-2)}{(2^2-1)(2^2-2)} = 7$ che sono tutti i modi di scegliere due elementi distinti fratto tutti i possibili generatori di $\mathbb{Z}/_{\mathbb{Z}} \times \mathbb{Z}/_{\mathbb{Z}}$.

6.5.1 osservazione : Sia $F = K(t_1, \cdots, t_n)$ una estensione non algebrica di K, si ha che $Gal(\bar{F}/K) < S_n$, allora i coefficienti del polinomio $f(x) = \prod_{i=1}^{n}(x - t_i)$ sono S_n-invarianti, si ha che $f(x) = \sum_{i=1}^{n} s_i x^1$ dove $s_i = \sum_{i=1}^{n}\prod_{k=1}^{n} t_{ik}$ allora $L = K(s_1, \cdots, s_n) \subset F^{S_n}$ e F è il campo di spezzamento di $f(x)$ su L di grado n.

6.5.6 esercizio : $[\mathbb{Q}(\xi_5, \sqrt{n}) : \mathbb{Q}]$ con n non quadrato in $\mathbb{Q}$.

soluzione : Consideriamo il diagramma sottostante, sappiamo che $\mathbb{Q}(\xi_5) \cap \mathbb{Q}(\sqrt{n}) \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{n})\}$ bisogna capire quando vale l'uno o l'altro.



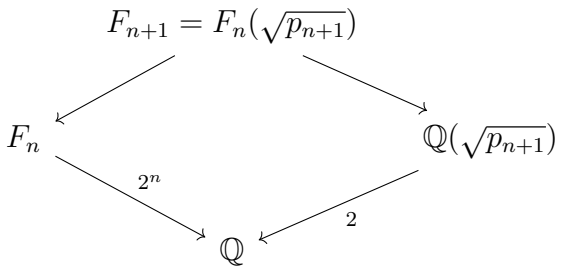
Se l'intersezione è tutto $\mathbb{Q}(\sqrt{n})$ allora questo è una sotto estensione di grado 2 su $\mathbb{Q}$ di $\mathbb{Q}(\xi_5)$, il gruppo di Galois di quest'ultimo è $\mathbb{Z}/_{\{}4\mathbb{Z}\}$ e quindi ne ha una sola che è $\mathbb{Q}(\xi_5^2) = \mathbb{Q}(\sqrt{5})$ quindi per $n = 5$ l'intersezione non è banale e si ha $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/_{\{}4\mathbb{Z}\}$ se no si ha che $\mathbb{Q}(\xi_5)$ e $\mathbb{Q}(\sqrt{n})$ sono linearmente disgiunti e quindi $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/_{\{}4\mathbb{Z}\} \times \mathbb{Z}/_{\{}2\mathbb{Z}\}$ (da vedere).

6.5.2 osservazione : Mi chiedo quando $\mathbb{Q}(\xi_p) \cap \mathbb{Q}(\sqrt{n})$ dove p primo e n non quadrato in $\mathbb{Q}$. So che $Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ è ciclico quindi se l'intersezione non è banale allora $\mathbb{Q}(\sqrt{n})$ è l'unica sotto estensione di $\mathbb{Q}(\xi_p)$ di grado due su $\mathbb{Q}$ (de vedere)

6.5.1 esempio : $Gal(\mathbb{Q}(\xi_{16})/\mathbb{Q}) = (\mathbb{Z}/_{16\mathbb{Z}})^* \cong \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}},\ Gal(\mathbb{Q}(\xi_{17})/\mathbb{Q}) = \mathbb{Z}/_{16\mathbb{Z}}$.

6.5.7 esercizio : Sia $F = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ con $p_1, \cdots, p_n$ primi distinti. Allora $[F : \mathbb{Q}] = 2^n$ e $Gal(F/\mathbb{Q}) \cong (\mathbb{Z}/_{2\mathbb{Z}})^n$.

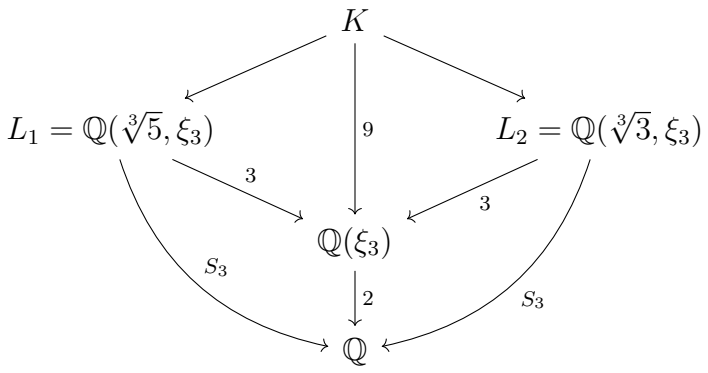
soluzione : Osserviamo intanto che $F/\mathbb{Q}$ è normale perché è campo di spezzamento del polinomio $(x^2 - p_1) \cdots (x^2 - p_n)$, ora procedo per induzione sul numero dei primi. Se $n = 1$ è ovvio, ora consideriamo $F_n = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ e $F_{n+1}(\sqrt{p_{n+1}})$ con $p_1, \cdots, p_n, p_{n+1}$ primi distinti, per induzione $[F_n : \mathbb{Q}] = 2^n$ e $Gal(F_n/\mathbb{Q}) \cong (\mathbb{Z}/_{2\mathbb{Z}})^n$ inoltre si ha $[F_{n+1} : F_n] \leq 2$, è 1 se $\sqrt{p_{n+1}} \in F_n$ se no vale 2, quindi cerchiamo di capire se $\sqrt{p_{n+1}} \in F_n$. Consideriamo le sotto estensioni L di F_n di grado 2 due su $\mathbb{Q}$, in particolare $L/\mathbb{Q}$ ha grado 2 se e solo se esiste un sottogruppo $H < Gal(F_n/\mathbb{Q})$ tale che $[G : H] = 2$, osserviamo che $\mathbb{Q}(\sqrt{p_1^{\epsilon_1} \cdots p_n^{\epsilon_n}})$, con $\epsilon_i \in \{0, 1\}$, sono $2^n - 1$ sotto estensioni e sono tutte distinte perchè in generale $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b}) \iff ab$ è un quadrato, ma in questo caso non accade questo, inoltre queste sotto estensioni sono tutte distinte da $\mathbb{Q}(\sqrt{p_{n+1}})$, se dimostro che queste $2^n - 1$ sono tutte e sole le sotto estensioni di grado 2 su $\mathbb{Q}$ di F_n allora $\sqrt{p_{n+1}} \notin F_n$. Quindi # sotto estensioni di grado 2 su $\mathbb{Q}$ = # sottogruppi di indice 2 di $(\mathbb{Z}/_{2\mathbb{Z}})^n$ = # sottogruppi di ordine 2^{n-1} di $(\mathbb{Z}/_{2\mathbb{Z}})^n = 2^n - 1$ quindi si ha



e si ha che $Gal(F_{n+1}/\mathbb{Q}) = (\mathbb{Z}/_{2\mathbb{Z}})^n \times \mathbb{Z}/_{2\mathbb{Z}}$ e quindi la tesi.

6.5.8 esercizio : Gruppo di Galois del campo di spezzamento di $(x^3-5)(x^3-3)$.

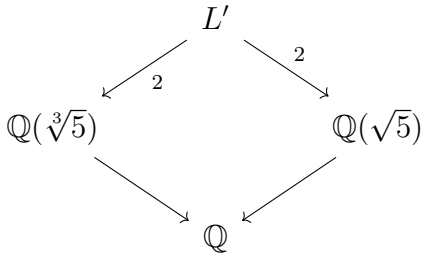
soluzione : Osserviamo innanzi tutto che il campo di spezzamento è $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{3}, \sqrt[3]{-3})$, consideriamo ora il diagramma :



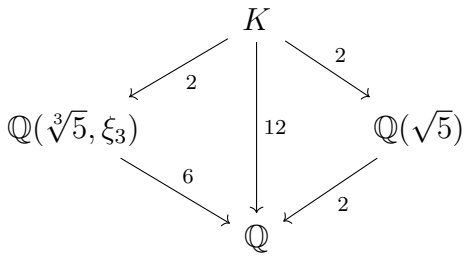
Si ha che $H = Gal(K/\mathbb{Q}(\xi_3)) \cong Gal(L_1/\mathbb{Q}(\xi_3)) \times Gal(L_2/\mathbb{Q}(\xi_3)) \cong \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$, allora $[K : \mathbb{Q}] = 18$ e quindi $H \triangleleft G$. Consideriamo σ tale che $\sigma(\sqrt[3]{3}) = \xi_3\sqrt[3]{5}$ e $\sigma(\xi_3) = \xi_3$ allora $\sigma^2(\sqrt[3]{3}) = \xi_3\sqrt[3]{5}$ quindi ha ordine 3, inoltre τ tale che $\tau(\xi_3) = \xi_3^2$ e $\tau(\sqrt[3]{5}) = \sqrt[3]{5}$ allora $\tau^2 = Id$, e consideriamo la sua estensione $\tilde{\tau} \in G$ si ha allora $G \cong H \rtimes_\gamma < \tilde{\tau} > \cong (\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}) \rtimes_\gamma \mathbb{Z}/_{2\mathbb{Z}}$ con $\gamma : \mathbb{Z}/_{2\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}})$ tale che $\gamma(\bar{1}) = \gamma_{\bar{1}}$ dove $\gamma_{\bar{1}}((1,0)) = (2,0)$ e $\gamma_{\bar{1}}(0,1) = (0,2)$, visto in G si ha $\gamma_{\tilde{\tau}}(\sigma) = \tilde{\tau}\sigma\tilde{\tau}^{-1} = \sigma^2$.

6.5.9 esercizio : Sia $\alpha = \sqrt[3]{5} + \sqrt{5}$, calcolare il campo di spezzamento K di $\mu_{\{}\alpha\}$ su $\mathbb{Q}$ e $Gal(K/\mathbb{Q})$, contare inoltre le sotto estensioni cicliche di K su $\mathbb{Q}$.

soluzione : Intanto $L = \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[3]{5}\sqrt{5}) = L'$ e $[L' : \mathbb{Q}] = 6$, consideriamo il diagramma :



Si ha allora che $\sigma : L' \longrightarrow \bar{\mathbb{Q}}$ dove $\sigma(\sqrt[3]{5}) = \xi_3^i \sqrt[3]{5}$ e $\sigma(\sqrt{5}) = \pm\sqrt{5}$ quindi l'orbita di α è $\{\sqrt[3]{5}+\sqrt{5}, \xi_3\sqrt[3]{5}+\sqrt{5}, \xi_3^2\sqrt[3]{5}+\sqrt{5}, \sqrt[3]{5}-\sqrt{5}\}$ di conseguenza il campo di spezzamento di μ_α è $K = \mathbb{Q}(\sqrt[3]{5}, \sqrt{5}, \xi_3)$ e $[K : \mathbb{Q}] = [L(\xi_3) : L][L : \mathbb{Q}] = 12$ abbiamo quindi il diagramma



quindi $Gal(K/\mathbb{Q}) \cong S_3 \times \mathbb{Z}/_{\{}2\mathbb{Z}\}$. per concludere osserviamo che $G' = A_3 \times \{0\} \Longrightarrow G/G' \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ quindi $\{H \triangleleft G \mid G/H \text{ ciclico}\} \Longleftrightarrow \{\bar{H} < G/G' \mid (G/G')/H \text{ ciclico}\}$.

6.5.10 esercizio : Sia K un campo e $A = K[x, y, z]$ e sia $I = (x^3y^3, y^4z^2, x^7) \subset (x, y, z)$ allora :

a) Esibire un ideale M massimale tale che $M \supset I$.

b) Esiste P primo non massimale tale che $P \supset I$?

c) Calcolare $\sqrt{I} = \{a \in A \mid a^n \in I \text{ per qualche } n\} \supset (xy, yz, x)$.

soluzione :

a) Consideriamo l'omomorfismo di valutazione $\gamma : K[x, y, z] \longrightarrow K$ tale che $\gamma(p(x, y, z)) = p(0, 0, 0)$, il nucleo di questo omomorfismo è l'ideale (x, y, z), siccome l'immagine è un campo,(x, y, z) è massimale e contiene I.

b) Considero (x, y), si ha che $K[x, y, z]/(x, y) \cong K[z]$ che è un domino ma non un campo quindi (x, y) è primo ma non massimale, inoltre contiene I.

c) $\sqrt{I} = (x, yz)$ (da vedere).