Ancora sulle radici primitive dell'unità

Lemma: Sia ζ_m una radice m-esima primitiva e ζ_n una radice n-esima primitiva. Allora vale che
- $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{MCD(n,m)})$
- $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mcm(n,m)})$

Dunque prodotto e intersezione di estensioni ciclotomiche è ciclotomica.

Dim: Segue dalle torri di estensioni

Teorema: Costruzione con Riga e Compasso: (inutile per esercizi, ma bel risultato):
Un numero complesso α è COSTRUIBILE se e solo se esiste una torre di estensioni

$$\mathbb{Q} = \mathbb{k}_0 \subseteq \mathbb{k}_1 \subseteq \_\_\_ \subseteq \mathbb{k}_n$$

con $\alpha \in \mathbb{k}_n$ e tale che $[\mathbb{k}_i : \mathbb{k}_{i-1}] = 2 \quad \forall i = 1, \_, n$

Polinomi Biquadratici: Discussione per capire il gruppo di Galois. Vedi dispense di Lombardo

FINE COSE UTILI CAMPI

Back to groups:

Def: Sia G un gruppo. Dati $a, b \in G$ definiamo il COMMUTATORE tra a e b così:

$$[a,b] = a^{-1}b^{-1}ab$$

Definiamo inoltre il DERIVATO di G o il sottogruppo dei commutatori il sottogruppo

$$[G,G] = \langle [a,b] \mid a, b \in G \rangle$$

Oss: Se non prendessimo il generato dei commutatori, non è detto che i commutatori siano un sottogruppo.

Oss: Se G è abeliano, allora $[G,G] = 0$ in quanto tutto commuta.

Proposizione: Valgono i seguenti fatti:
- $[G,G]$ è caratteristico in G
- Sia $H \trianglelefteq G$, G/H è abeliano se e solo se $[G,G] \subseteq H$

Dim:
- $\forall \varphi \in Aut(G)$ vale che $\varphi([a,b]) = \varphi(a^{-1}b^{-1}ab) = \varphi(a)^{-1}\varphi(b)^{-1}\varphi(a)\varphi(b) = [\varphi(a), \varphi(b)]$. Dato che φ è bigezione, allora i commutatori vengono mandati esattamente nei commutatori e dunque $[G,G]$ è caratteristico
- $\Rightarrow$ Se G/H è abeliano allora $\forall xH, yH \in G/H$ si ha che

e dunque $[G, G]$ è caratteristico

- $\boxed{\Rightarrow}$ Se G/H è abeliano allora $\forall xH, yH \in G/H$ si ha che

$$xHyH = yHxH \iff xyH = yxH \iff y^{-1}x^{-1}yx \in H$$

cioè $[G,G] \subseteq H$

$\boxed{\Leftarrow}$ Sia $[G,G] \subseteq H$ allora $\forall xH, yH$ si ha che

$$xHyH = xyH = xy(y^{-1}x^{-1}yx)H = yxH = yHxH$$

cioè G/H è abeliano. $\square$

Oss: In altri termini $[G,G]$ è il più piccolo sottogruppo di G tale che $G/[G,G]$ è abeliano, o ancora $G/[G,G]$ è il più grande quoziente abeliano di G.