Svolgimento Appello di Algebra 2 del 16 giugno 2014.

1 Esercizio 1

Sia $K := \mathbb{Q}[a_1, \ldots, a_n]$ dove per ogni $i = 1, \ldots, n$ gli a_i siano tali che $a_i^2 \in \mathbb{Q}$. Detto u un arbitrario elemento di K mostrare che il grado del polinomio minimo di u su $\mathbb{Q}$ è una potenza di 2.

Svolgimento. Dobbiamo mostrare che $|\mathbb{Q}(u) : \mathbb{Q}|$ è una potenza di 2. Per la formula dei gradi $|K : \mathbb{Q}| = |K : \mathbb{Q}(u)| \cdot |\mathbb{Q}(u) : \mathbb{Q}|$ e quindi $|\mathbb{Q}(u) : \mathbb{Q}|$ divide $|K : \mathbb{Q}|$. Ne segue che per concludere basta dimostrare che $|K : \mathbb{Q}|$ è una potenza di 2, infatti i divisori di una potenza di 2 sono tutti potenze di 2. Osserviamo che ogni a_i è algebrico su $\mathbb{Q}$ essendo radice del polinomio $X^2 - a_i^2 \in \mathbb{Q}[X]$, per cui $K = \mathbb{Q}[a_1, \ldots, a_n] = \mathbb{Q}(a_1, \ldots, a_n)$. Inoltre per ogni $i = 1, \ldots, n-1$ si ha $\mathbb{Q}(a_1, \ldots, a_i, a_{i+1}) = \mathbb{Q}(a_1, \ldots, a_i)(a_{i+1})$ e a_{i+1} è radice di $X^2 - a_{i+1}^2 \in \mathbb{Q}[X] \subseteq \mathbb{Q}(a_1, \ldots, a_i)[X]$ per cui a_{i+1} ha grado 1 oppure 2 su $\mathbb{Q}(a_1, \ldots, a_i)$, cioè il numero $|\mathbb{Q}(a_1, \ldots, a_{i+1}) : \mathbb{Q}(a_1, \ldots, a_i)|$ è 1 oppure 2. Ne segue, di nuovo per la formula dei gradi, che

$$\begin{aligned} |K : \mathbb{Q}| &= |\mathbb{Q}(a_1, \ldots, a_n) : \mathbb{Q}| \\ &= |\mathbb{Q}(a_1, \ldots, a_n) : \mathbb{Q}(a_1, \ldots, a_{n-1})| \cdot |\mathbb{Q}(a_1, \ldots, a_{n-1}) : \mathbb{Q}(a_1, \ldots, a_{n-2})| \cdots \\ \cdots &\quad |\mathbb{Q}(a_1, a_2) : \mathbb{Q}(a_1)| \cdot |\mathbb{Q}(a_1) : \mathbb{Q}| \end{aligned}$$

e siccome ognuno di questi fattori è 1 oppure 2, $|K : \mathbb{Q}|$ divide 2^n e quindi è una potenza di 2.

2 Esercizio 2

Siano H e K due sottogruppi del gruppo finito G. Provare che se $|G : H|$ e $|G : K|$ sono coprimi allora $G = HK$.

Svolgimento. Osserviamo che $|G : H \cap K| = |G : H| \cdot |H : H \cap K|$ e anche $|G : H \cap K| = |G : K| \cdot |K : H \cap K|$ quindi $|G : H|$ e $|G : K|$ dividono entrambi $|G : H \cap K|$. Siccome per ipotesi $|G : H|$ e $|G : K|$ sono coprimi, anche $|G : H| \cdot |G : K|$ divide $|G : H \cap K|$, in particolare essendo $|HK| \leq |G|$ (perché $HK \subseteq G$)

$$|G : H| \cdot |G : K| \leq |G : H \cap K| = \frac{|G|}{|H| \cdot |K|} \frac{|H| \cdot |K|}{|H \cap K|} = \frac{|G|}{|H| \cdot |K|} |HK| \leq \frac{|G|}{|H|} \frac{|G|}{|K|} = |G : H| \cdot |G : K|.$$

Siccome i due estremi di questa catena di disuguaglianze sono uguali otteniamo che si tratta in realtà di una catena di uguaglianze, in particolare $\frac{|G|}{|H| \cdot |K|} |HK| = \frac{|G|}{|H|} \frac{|G|}{|K|}$ cioè $|G| = |HK|$ e quindi, siccome G è finito e $HK \subseteq G$, $G = HK$.

3 Esercizio 3

Sia $G = \langle a \rangle \times \langle b \rangle$, prodotto diretto di $\langle a \rangle$, ciclico di ordine 10, e $\langle b \rangle$, ciclico di ordine 6, e sia $g = (a^9, b^{10}) \in G$.

1. Determinare $|g|$.

2. Determinare $|g^{24}|$.

3. Quanti sono i sottogruppi di $\langle g \rangle$?

4. È vero che G è un gruppo ciclico?

Svolgimento. **Punto 1**. L'ordine di a^9 è $|a|/(9,|a|) = 10/(9,10) = 10$, e l'ordine di b^{10} è $|b|/(10,|b|) = 6/(10,6) = 6/2 = 3$. L'ordine di g è il minimo intero positivo k tale che $g^k = 1$, cioè $(a^{9k}, b^{10k}) = (1,1)$, in particolare k è diviso da $|a^9| = 10$ e da $|b^{10}| = 3$ per cui è diviso da 30. Siccome $g^{30} = (1,1)$ deduciamo che $|g| = 30$.

Punto 2. L'ordine di g^{24} è $|g|/(24,|g|) = 30/(24,30) = 30/6 = 5$.

Punto 3. I sottogruppi di $\langle g \rangle$, gruppo ciclico di ordine $|g| = 30$, sono tanti quanti i divisori di 30 (in un gruppo ciclico di ordine n c'è esattamente un sottogruppo di ordine un dato divisore di n), cioè 8 (i divisori di 30 sono $1, 2, 3, 5, 6, 10, 15, 30$).

Punto 4. G non è un gruppo ciclico, infatti ha almeno due sottogruppi di ordine 2 (cosa che in un gruppo ciclico non succede, per il motivo esposto nel punto precedente), generati da $(a^5, 1)$ e $(1, b^3)$.

4 Esercizio 4

Sia G un gruppo di ordine $2010 = 2 \cdot 3 \cdot 5 \cdot 67$. Supponiamo che G contenga un sottogruppo normale e abeliano N di ordine 6.

1. Provare che tutti gli elementi di ordine 2 e quelli di ordine 3 di G appartengono a N.

2. Dedurne che G ha un unico elemento di ordine 2 ed esattamente due elementi di ordine 3.

3. Provare che N è contenuto nel centro di G.

4. Osservando che il centro di G è contenuto nel normalizzante di ogni sottogruppo di G provare che $n_5(G) = 1$.

5. Si deduca che G è abeliano.

Svolgimento. **Punto 1**. Sia g un elemento di ordine $p \in \{2, 3\}$ in N. Allora $\langle g \rangle$ è un p-sottogruppo di Sylow di G, infatti ha l'ordine giusto (p^2 non divide $|G|$). Sia h un altro elemento di ordine p in G. Dobbiamo mostrare che $h \in N$. Anche $\langle h \rangle$ è un p-sottogruppo di Sylow di G e quindi per il teorema di Sylow $\langle g \rangle$ e $\langle h \rangle$ sono coniugati in G, cioè esiste $x \in G$ con $x\langle g \rangle x^{-1} = \langle h \rangle$. Ma allora siccome $xNx^{-1} = N$ (essendo N normale), $\langle h \rangle = x\langle g \rangle x^{-1} \subseteq xNx^{-1} = N$ e quindi $h \in N$.

Punto 2. Per il punto precedente gli elementi di G di ordine 2 o 3 stanno in N. Siccome N è abeliano i suoi sottogruppi di Sylow sono normali e quindi per $p \in \{2, 3\}$ gli elementi di ordine p in G stanno nell'unico p-sottogruppo di Sylow di N, che ha ordine p, primo, quindi è ciclico. Un gruppo ciclico di ordine p ha esattamente $\varphi(p) = p - 1$ elementi di ordine p, quindi 1 se $p = 2$ e 2 se $p = 3$.

Punto 3. Siccome N è generato da un elemento di ordine 2 e da uno di ordine 3 (infatti ha ordine $6 = 2 \cdot 3$), per mostrare che $N \subseteq Z(G)$ basta mostrare che gli elementi di ordine 2 e 3 in N stanno nel centro di G. Se $g \in N$ ha ordine 2 allora siccome è l'unico elemento di G di ordine 2, se

$x \in G$ allora $xgx^{-1} = g$ essendo xgx^{-1} un elemento di ordine 2 (il coniugio preserva l'ordine), in altre parole $xg = gx$ per ogni $x \in G$ e quindi $g \in Z(G)$. Ora sia $g \in N$ di ordine 3. Siccome G ha due elementi di ordine 3 essi sono proprio i due elementi di $\langle g \rangle = \{1, g, g^2\}$ di ordine 3, cioè g e g^2, per cui $\langle g \rangle \trianglelefteq G$ (infatti i coniugati di g e g^2 hanno ordine 3 quindi sono g o g^2). Il coniugio induce un omomorfismo $\varphi : G \to \mathrm{Aut}(\langle g \rangle) \cong C_2$ e siamo ridotti a mostrare che $\ker(\varphi) = G$. Se così non fosse allora φ sarebbe suriettivo e quindi $G/\ker(\varphi) \cong C_2$ da cui $|\ker(\varphi)| = |G|/2 = 3 \cdot 5 \cdot 67$ sarebbe dispari. Questo è assurdo perché essendo N abeliano e $g \in N$, N è contenuto in $\ker(\varphi)$ e $|N| = 6$.

Punto 4. Se $H \leq G$ e $z \in Z(G)$, dove $Z(G)$ indica il centro di G, siccome z commuta con ogni elemento di G in particolare commuta con ogni elemento di H per cui $zHz^{-1} = H$, in altre parole $z \in N_G(H)$. Sia P un 5-sottogruppo di Sylow di G. Allora $N \subseteq Z(G) \subseteq N_G(P)$ e quindi $PN \leq N_G(P)$ da cui $|G : PN| = |G : N_G(P)| \cdot |N_G(P) : PN|$ quindi $n_5(G) = |G : N_G(P)|$ divide $|G : PN| = |G|/|PN| = |G|/30 = 67$. Siccome $67 \not\equiv 1 \mod 5$ otteniamo dal teorema di Sylow che $n_5(G) = 1$.

Punto 5. Per i punti precedenti si ha $n_2(G) = n_3(G) = n_5(G) = 1$ e dal teorema di Sylow $n_{67}(G)$ divide 30 ed è congruo a 1 modulo 67 per cui $n_{67}(G) = 1$. Ne segue che i sottogruppi di Sylow di G sono tutti normali quindi G è isomorfo al prodotto diretto dei suoi sottogruppi di Sylow. Siccome i sottogruppi di Sylow di G hanno ordine primo sono abeliani (in realtà ciclici) per cui anche G, prodotto diretto di gruppi abeliani, è abeliano.

5 Esercizio 5

Sia $\epsilon \in \mathbb{C}$ una radice primitiva sesta dell'unità e $u = \sqrt[6]{5}$.

1. Si determini il polinomio minimo $f_1(x)$ di ϵ su $\mathbb{Q}$.
2. Si determini il polinomio minimo $f_2(x)$ di u su $\mathbb{Q}$.
3. Siano E_1 ed E_2 i campi di spezzamento di $f_1(x)$ e $f_2(x)$ su $\mathbb{Q}$. Si determinino $|E_1 : \mathbb{Q}|$, $|E_2 : \mathbb{Q}|$ e $|E_1 \cap E_2 : \mathbb{Q}|$.

Svolgimento. **Punto 1**. $f_1(x)$ è il sesto polinomio ciclotomico $\Phi_6(x)$. Abbiamo dalla teoria che $\prod_{d|n} \Phi_d(x) = x^n - 1$ da cui $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = x^6 - 1$ e $\Phi_1(x) = x - 1$, $\Phi_1(x)\Phi_2(x) = x^2 - 1$ da cui $\Phi_2(x) = x + 1$, $\Phi_1(x)\Phi_3(x) = x^3 - 1$ da cui $\Phi_6(x) = (x^6 - 1)/((x-1)(x+1)(x^2+x+1)) = x^2 - x + 1$.

Punto 2. u è radice di $x^6 - 5$. Per il criterio di Eisenstein applicato al primo 5 tale polinomio è irriducibile su $\mathbb{Q}$ quindi $f_2(x) = x^6 - 5$.

Punto 3. Siccome $f_1(x) = x^2 - x + 1$ non ha radici reali è irriducibile su $\mathbb{Q}$ con ϵ come radice, dal teorema di Ruffini si ricava che l'altra radice è $1 - \epsilon$ e quindi $E_1 = \mathbb{Q}(\epsilon)$ ha grado 2 su $\mathbb{Q}$. Gli zeri di $f_2(x) = x^6 - 5$ sono $u\epsilon^i$ per $i = 0, 1, 2, 3, 4, 5$. Ne segue che $E_2 = \mathbb{Q}(u, u\epsilon, u\epsilon^2, u\epsilon^3, u\epsilon^4, u\epsilon^5)$ contiene u e $u\epsilon/u = \epsilon$ e d'altra parte è generato da essi, quindi $E_2 = \mathbb{Q}(u, \epsilon)$. Ora $|\mathbb{Q}(u) : \mathbb{Q}| = 6$ perché $f_2(x)$ ha grado 6, d'altra parte $\mathbb{Q}(u) \subseteq \mathbb{R}$ e $\epsilon \notin \mathbb{R}$ quindi ϵ ha grado 2 non solo su $\mathbb{Q}$ ma anche su $\mathbb{Q}(u)$. Segue allora dalla formula dei gradi che

$$|E_2 : \mathbb{Q}| = |\mathbb{Q}(u, \epsilon) : \mathbb{Q}| = |\mathbb{Q}(u)(\epsilon) : \mathbb{Q}| = |\mathbb{Q}(u)(\epsilon) : \mathbb{Q}(u)| \cdot |\mathbb{Q}(u) : \mathbb{Q}| = 2 \cdot 6 = 12.$$

Siccome $\epsilon \in E_2$ si ha $E_1 = \mathbb{Q}(\epsilon) \subseteq E_2$ quindi $E_1 \cap E_2 = E_1$ e quindi $|E_1 \cap E_2 : \mathbb{Q}| = |E_1 : \mathbb{Q}| = 2$.

6 Esercizio 6

Si consideri l'ideale $I = (29)$ dell'anello $\mathbb{Z}[i]$ degli interi di Gauss.

1. È vero che I è un ideale massimale?
2. Qual è l'ordine dell'anello $\mathbb{Z}[i]/I$?
3. Quali sono gli elementi invertibili dell'anello $\mathbb{Z}[i]/I$?

Svolgimento. **Punto 1**. Si ha $29 = 5^2+2^2 = (5+2i)(5-2i)$ da cui I è contenuto in $J = (5+2i)$. D'altra parte $I \neq J$ infatti essendo $\mathbb{Z}[i]$ un PID, se fosse $I = J$ allora 29 dividerebbe $5+2i$ ma questo contraddice il fatto che $N(29) = 29^2$ non divide $N(5+2i) = (5+2i)(5-2i) = 29$ (qui N indica la funzione norma, $N(a+ib) = (a+ib)(a-ib) = a^2+b^2$). Quindi I è contenuto propriamente in J quindi non è massimale.

Punto 2. Un generico elemento di $A = \mathbb{Z}[i]/(29)$ è del tipo $a + ib + (29)$, dove $a, b \in \mathbb{Z}$. Effettuando la divisione con resto di a e b per 29 troviamo che $a + ib + (29) = r + is + (29)$ con $r, s \in \{0, 1, 2, \ldots, 28\}$. Tale scrittura di un elemento di A è unica, infatti se $r, s, t, u \in \{0, 1, 2, \ldots, 28\}$ sono tali che $r + is + (29) = t + iu + (29)$ allora esistono $\alpha, \beta \in \mathbb{Z}$ con $r - t + i(s - u) = 29(\alpha + i\beta)$, quindi 29 divide le differenze $r-t$ e $s-u$ in $\mathbb{Z}$, da cui, essendo $r, s, t, u \in \{0, 1, 2, \ldots, 28\}$, segue $r = t$ e $s = u$. Quindi un generico elemento $a + ib + (29)$ è determinato da ventinove possibili scelte per a e altrettante per b. In conclusione $|A| = 29^2$.

Punto 3. $I = (29) = ((5 + 2i)(5 - 2i))$ e $5 + 2i$ e $5 - 2i$ sono coprimi (essendo irriducibili non associati ed essendo $\mathbb{Z}[i]$ un dominio euclideo), quindi dal teorema cinese del resto $\mathbb{Z}[i]/I \cong \mathbb{Z}[i]/(5 + 2i) \times \mathbb{Z}[i]/(5 - 2i)$. Il coniugio induce un isomorfismo $\mathbb{Z}[i]/(5 + 2i) \cong \mathbb{Z}[i]/(5 - 2i)$ da cui $|\mathbb{Z}[i]/(5 + 2i)| = |\mathbb{Z}[i]/(5 - 2i)| = 29$. Ne segue che $\mathbb{Z}[i]/(29)$ ha 28^2 elementi invertibili, sono quelli che tramite l'isomorfismo dato dal teorema cinese del resto hanno come immagine una coppia di elementi non nulli. Si tratta degli elementi $a + ib + (29)$ con la proprietà che $5 + 2i$ e $5 - 2i$ non dividono $a + ib$.