SVOLGIMENTO DEL COMPITO DI ALGEBRA 2 DEL 21/01/2014 (SECONDO COMPITINO).

1 Esercizio 1

Siano α e β algebrici su un campo F. Si provi che anche $\alpha+\beta$ è algebrico su F.

Risoluzione. Siccome α, β sono algebrici, i gradi $|F(\alpha) : F|$ e $|F(\beta) : F|$ sono finiti. In particolare β è zero di un polinomio di grado $|F(\beta) : F|$ a coefficienti in F, quindi è zero di un polinomio di grado $|F(\beta) : F|$ a coefficienti in $F(\alpha)$ (lo stesso), per cui $|F(\alpha)(\beta) : F(\alpha)| \leq |F(\beta) : F|$. Per la formula dei gradi

$$|F(\alpha, \beta) : F| = |F(\alpha)(\beta) : F(\alpha)| \cdot |F(\alpha) : F| \leq |F(\beta) : F| \cdot |F(\alpha) : F|$$

è finito, essendo $|F(\alpha) : F|$ e $|F(\beta) : F|$ finiti, in altre parole $F(\alpha, \beta)$ ha dimensione finita su F. Siccome $F(\alpha+\beta)$ è un F-sottospazio vettoriale di $F(\alpha, \beta)$ (essendo $\alpha+\beta \in F(\alpha, \beta)$), anche lui ha dimensione finita su F, in altre parole il grado $|F(\alpha+\beta) : F|$ è finito, cioè $\alpha+\beta$ è algebrico su F.

2 Esercizio 2

Sia $F = \mathbb{Z}/p\mathbb{Z}$ con p primo e sia $f(x) \in F[x]$ un polinomio irriducibile di grado n. Si provi che $f(x)$ divide $x^{p^n} - x$.

Risoluzione. Sia a uno zero di $f(x)$ in un'opportuna estensione di F. Osserviamo che siccome $f(x)$ è irriducibile di grado n, $F[a] \cong F[x]/(f(x))$ è un campo (essendo $(f(x))$ ideale massimale, essendo $f(x)$ irriducibile in $F[x]$, che in quanto anello dei polinomi su un campo è un dominio a ideali principali) ha dimensione n su F, quindi $F[a]$ è un campo con $q = p^n$ elementi. Segue che ogni elemento $t \in F[a]$ verifica $t^q = t$ (infatti questo è ovvio se $t = 0$ e se $t \neq 0$ allora è $t^{q-1} = 1$ essendo $F[a] - \{0\}$ un gruppo di ordine $q-1$, quindi moltiplicando per t troviamo $t^q = t$), cioè è zero del polinomio $x^q - x$. In particolare anche a è zero di $x^q - x$, quindi $x^q - x$ appartiene al nucleo della valutazione in a, $F[x] \to F$, $P(x) \mapsto P(a)$. Tale nucleo è l'ideale di $F[x]$ generato dal polinomio minimo di a su F, che è $(f(x))$. Quindi $x^q - x \in (f(x))$, in altre parole $f(x)$ divide $x^q - x$ in $F[x]$.

3 Esercizio 3

Sia G un gruppo non banale con la proprietà che ogni sottogruppo è finitamente generato.

1. Sia $\{H_\lambda\}_{\lambda \in \Lambda}$ una catena di sottogruppi propri. Provare che $K = \cup_{\lambda \in \Lambda} H_\lambda$ è un sottogruppo di G. Usare il fatto che K è finitamente generato per provare che $K = H_\lambda$ per un opportuno $\lambda \in \Lambda$.

2. Dedurre che G contiene almeno un sottogruppo massimale.

Risoluzione. L'idea è applicare il Lemma di Zorn. Sia $\mathfrak{X}$ la famiglia dei sottogruppi propri di G. $\mathfrak{X}$ è non vuota essendo $\{1\} \in \mathfrak{X}$ (infatti G è non banale, cioè $G \neq \{1\}$). Per mostrare che $\mathfrak{X}$ ha elementi massimali rispetto all'inclusione (cioè quello che vogliamo) per il Lemma di Zorn basta mostrare che data una catena $C = \{H_\lambda\}_{\lambda\in\Lambda}$ in $\mathfrak{X}$ (cioè un sottoinsieme di $\mathfrak{X}$ totalmente ordinato rispetto all'inclusione) esiste un maggiorante di C in $\mathfrak{X}$. Sia $H := \bigcup_{\lambda\in\Lambda} H_\lambda$. Mostriamo che H è un sottogruppo di G.

- L'elemento neutro 1 di G appartiene ad H essendo $1 \in H_\lambda$ per ogni $\lambda \in \Lambda$ e quindi anche $1 \in H$.
- Sia $x \in H$ e mostriamo che $x^{-1} \in H$. Siccome $x \in H = \bigcup_{\lambda\in\Lambda} H_\lambda$ per definizione di unione esiste $\lambda \in \Lambda$ con $x \in H_\lambda$ per cui anche $x^{-1} \in H_\lambda$ (essendo H_λ un sottogruppo) quindi $x^{-1} \in H$ (per definizione di unione).
- Siano $x, y \in H$ e mostriamo che $xy \in H$. Siccome $H = \bigcup_{\lambda\in\Lambda} H_\lambda$ per definizione di unione esistono $\lambda, \mu \in \Lambda$ tali che $x \in H_\lambda$ e $y \in H_\mu$. Siccome l'inclusione induce in C un ordine totale (perché C è una catena) si ha $H_\lambda \subseteq H_\mu$ oppure $H_\mu \subseteq H_\lambda$. Nel primo caso $x \in H_\lambda \subseteq H_\mu \ni y$ quindi siccome H_μ è un sottogruppo di G, $xy \in H_\mu \subseteq H$ e quindi $xy \in H$. Nel secondo caso $y \in H_\mu \subseteq H_\lambda \ni x$ quindi siccome H_λ è un sottogruppo di G, $xy \in H_\lambda \subseteq H$ quindi $xy \in H$.

Resta da mostrare che $H \in \mathfrak{X}$, cioè che $H \neq G$. Siccome ogni sottogruppo di G è finitamente generato e H è un sottogruppo di G, H è finitamente generato, quindi esistono $a_1, \ldots, a_k \in H$ tali che $H = \langle a_1, \ldots, a_k\rangle$. Sia $i \in \{1, \ldots, k\}$. Siccome $a_i \in H = \bigcup_{\lambda\in\Lambda} H_\lambda$, per definizione di unione esiste $\lambda_i \in \Lambda$ tale che $a_i \in H_{\lambda_i}$. Siccome l'ordine di inclusione in C è totale, i suoi sottoinsiemi finiti ammettono massimo, quindi esiste $j \in \{1, \ldots, k\}$ tale che $H_{\lambda_i} \subseteq H_{\lambda_j}$ per ogni $i = 1, \ldots, k$. Ne segue che $a_i \in H_{\lambda_j}$ per ogni $i = 1, \ldots, k$ quindi, poiché H_{λ_j} è un sottogruppo di G, $H = \langle a_1, \ldots, a_k\rangle \subseteq H_{\lambda_j}$ quindi, essendo $H_{\lambda_j} \subseteq \bigcup_{\lambda\in\Lambda} H_\lambda = H$, segue che $H = H_{\lambda_j} \in \mathfrak{X}$.

4 Esercizio 4

Nell'anello degli interi di Gauss $\mathbb{Z}[i]$ si consideri il sottoinsieme

$$J = \{(x - 2y) + i(2x + y) \in x, y \in \mathbb{Z}\}.$$

1. Si provi che J è un ideale di $\mathbb{Z}[i]$.
2. Si provi che J è l'ideale principale generato da $1 + 2i$.
3. Si dica se J è un ideale massimale di $\mathbb{Z}[i]$.

4. Si consideri l'ideale I generato da $5+5i$. Determinare $I+J$ e $I \cap J$.

Risoluzione.

1. Mostriamo che J è un ideale di $\mathbb{Z}[i]$. Scegliendo $x = y = 0$ troviamo $0 \in J$, e se $(x-2y)+i(2x+y) \in J$ allora $-((x-2y)+i(2x+y)) = (-x-2(-y))+i(2(-x)+(-y)) \in J$. Prendiamo ora $(x-2y)+i(2x+y)$, $(z-2w)+i(2z+w) \in J$ e mostriamo che la loro somma sta in J. Si ha

$$(x-2y)+i(2x+y)+(z-2w)+i(2z+w) =$$

$$= (x+z-2(y+w))+i(2(x+z)+(y+w)) \in J.$$

Resta da mostrare che se $x-2y+i(2x+y) \in J$ e $a+ib \in \mathbb{Z}[i]$ allora il loro prodotto sta in J. Si ha

$$(x-2y+i(2x+y))(a+ib) = a(x-2y)-b(2x+y)+i(a(2x+y)+b(x-2y)) =$$

$$= ax-by-2(ay+bx)+i(2(ax-by)+(ay+bx)) \in J.$$

2. Mostriamo che $J = (1+2i)$. Dati $x, y \in \mathbb{Z}$ si ha

$$(x-2y)+i(2x+y) = x(1+2i)+y(-2+i) =$$

$$= x(1+2i)+yi(1+2i) = (1+2i)(x+iy).$$

Questo prova che $J \subseteq (1+2i)$. L'inclusione $(1+2i) \subseteq J$ segue da $1+2i \in J$ che si vede subito scegliendo $x = 1$ e $y = 0$.

3. J è un ideale massimale di $\mathbb{Z}[i]$ perché $\mathbb{Z}[i]$ è un dominio a ideali principali e $J = (1+2i)$ è generato da un elemento irriducibile, infatti $1+2i$ ha norma $N(1+2i) = (1+2i)(1-2i) = 5$ che è un numero primo, quindi $1+2i$ è irriducibile.

4. Si ha $5+5i = 5(1+i) = (1+2i)(1-2i)(1+i)$ quindi $1+2i$ divide $5+5i$, cioè $5+5i \in (1+2i) = J$. Segue che $I \subseteq J$, quindi $I+J = J$ e $I \cap J = I$.

5 Esercizio 5

Sia $F = \mathbb{Z}/5\mathbb{Z}$ e si consideri il polinomio $f(x) = x^3+2x+1 \in F[x]$.

1. Si provi che $f(x)$ è irriducibile.

2. Sia u una radice di $f(x)$ in una opportuna estensione e sia $K = F[u]$. Determinare $|K|$.

3. Si provi che per ogni $b \in K \setminus \mathbb{Z}/5\mathbb{Z}$, si ha $F[b] = K$.

4. Si provi che K contiene E un campo di spezzamento su $\mathbb{Z}/5\mathbb{Z}$ del polinomio $x^{31}-1$.

Risoluzione.

1. $f(x)$ è irriducibile perché se fosse riducibile avrebbe un fattore di grado minore di 3, quindi avrebbe almeno un fattore di grado 1 (infatti avrebbe tre fattori irriducibili di grado 1 oppure uno di grado 1 e uno di grado 2), del tipo $a(x-\alpha)$ con $a, \alpha \in F$, quindi sarebbe $f(\alpha) = 0$, e questo è falso in quanto $f(\alpha) \neq 0$ per ogni $\alpha \in F$, infatti $f(0) = 1$, $f(1) = 4$, $f(2) = 3$, $f(3) = 4$ e $f(4) = 3$.

2. $K = F[u]$ è uno spazio vettoriale su F di dimensione $|F[u] : F|$, uguale al grado del polinomio minimo di u su F, che è $f(x)$ in quanto $f(x)$ è un polinomio monico irriducibile di $F[x]$ che ha u come zero. Segue che $|F[u] : F| = 3$ quindi K come spazio vettoriale su F è isomorfo a F^3, quindi $|K| = |F^3| = |F|^3 = 5^3$.

3. Sia $b \in K \setminus F$. Allora per la formula dei gradi $3 = |F[u] : F| = |F[u] : F[b]| \cdot |F[b] : F|$ e $|F[b] : F| \neq 1$ essendo $b \notin F$. Siccome 3 è primo segue che $|F[b] : F| = 3$ e $|F[u] : F[b]| = 1$, e quest'ultima uguaglianza è equivalente a $F[b] = F[u] = K$.

4. $K - \{0\}$ è un gruppo moltiplicativo finito di ordine $125 - 1 = 124 = 4 \cdot 31$. Inoltre tale gruppo è ciclico essendo il gruppo moltiplicativo di un campo finito. Sia t un suo generatore. Allora t ha ordine $4 \cdot 31$ quindi t^4 ha ordine $o(t^4) = o(t)/(4, o(t)) = 124/4 = 31$. Ne segue che i 31 elementi $1, t, t^2, \ldots, t^{30}$ sono a due a due distinti e $(t^i)^{31} = 1$ per ogni $i = 0, 1, \ldots, 30$. Siccome $x^{31} - 1$ ha grado 31, tanto quante sono le potenze di t, segue che le potenze di t sono tutti e soli gli zeri di $x^{31} - 1$. Quindi il campo $F[t]$ è un campo di spezzamento per $x^{31} - 1$.

6 Esercizio 6

Sia $f(X) := X^4 - X^2 - 3 \in \mathbb{Q}[X]$.

1. Provare che $f(x)$ è irriducibile in $\mathbb{Q}[X]$.

2. Sia u uno zero reale di $f(x)$ (mostrare che esiste). Esprimere l'inverso di u e di u^2 come polinomi in u.

3. Da $u^2(1 - u^2) = -3$ dedurre che $1 - u^2$ non è un quadrato in $\mathbb{Q}(u)$.

4. Mostrare che $\mathbb{Q}(u)$ non è un campo di spezzamento per $f(x)$ su $\mathbb{Q}$.

5. Mostrare che un campo di spezzamento per $f(x)$ su $\mathbb{Q}$ ha grado 8.

Risoluzione.

1. Mostriamo che $f(X)$ è irriducibile in $\mathbb{Q}[X]$. Per il lemma di Gauss, siccome $f(X)$ ha coefficienti interi, è irriducibile in $\mathbb{Q}[X]$ se e solo se lo è in $\mathbb{Z}[X]$. Mostriamo che $f(X)$ non ha zeri in $\mathbb{Z}$. Se $a \in \mathbb{Z}$ è tale che $f(a) = 0$ allora

$a^4 - a^2 - 3 = 0$ da cui $a(a^3 - a) = 3$ quindi a divide 3 in $\mathbb{Z}$, e questo implica che $a \in \{1, -1, 3, -3\}$. Ma $f(1) = f(-1) = -3 \neq 0$, $f(3) = f(-3) = 69 \neq 0$. Per il teorema di Ruffini segue allora che $f(X)$ non ha fattori di grado 1. Per mostrare che $f(X)$ è irriducibile in $\mathbb{Z}[X]$ ci resta da verificare che non ammette decomposizioni in due fattori irriducibili di grado 2. Osserviamo che siccome $f(X)$ è monico, se esistono tali fattori di grado 2 allora ne esistono di monici (i loro coefficienti di grado massimo devono avere 1 come prodotto, quindi sono entrambi 1 oppure entrambi -1, e nel secondo caso basta cambiare segno a entrambi). Supponiamo quindi per assurdo che esistano $a, b, c, d \in \mathbb{Z}$ tali che

$$\begin{aligned} f(X) &= X^4 - X^2 - 3 = (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a + c)X^3 + (d + ac + b)X^2 + (ad + bc)X + bd. \end{aligned}$$

Per definizione di polinomio, da questa uguaglianza segue che i rispettivi coefficienti coincidono, cioè

$$a + c = 0,\ d + ac + b = -1,\ ad + bc = 0,\ bd = -3.$$

Dall'ultima segue che $b \in \{1, -1, 3, -3\}$ e $d = -3/b$.

- Se $b = 1$ o $b = -3$ allora da $d = -3/b$ segue $b + d = -2$ e quindi $-1 = d + ac + b = ac - 2$ da cui $ac = 1$, ed essendo $a + c = 0$ otteniamo $-a^2 = 1$, cioè $a^2 = -1$ assurdo essendo $a \in \mathbb{Z}$.
- Se $b = -1$ o $b = 3$ allora da $d = -3/b$ segue $b + d = 2$ e quindi $-1 = d + ac + b = ac + 2$ da cui $ac = -3$, ed essendo $a + c = 0$ otteniamo $a^2 = 3$, assurdo essendo $a \in \mathbb{Z}$.

2. Risolvendo l'equazione biquadratica $X^4 - X^2 - 3 = 0$ troviamo $X^2 = \frac{1}{2}(1 \pm \sqrt{13})$, quindi $u := \sqrt{\frac{1}{2}(1 + \sqrt{13})}$ è uno zero di $f(X)$, e $u \in \mathbb{R}$ essendo $\frac{1}{2}(1 + \sqrt{13}) \geq 0$. Si ha $f(u) = 0$, cioè $u^4 - u^2 - 3 = 0$, cioè $u(u^3 - u) = 3$ per cui $u^{-1} = \frac{1}{3}(u^3 - u)$. Inoltre da $u^4 - u^2 = 3$ segue anche $u^2(u^2 - 1) = 3$ cioè $(u^2)^{-1} = \frac{1}{3}(u^2 - 1)$.

3. Come abbiamo osservato si ha $u^2(u^2 - 1) = 3$, cioè $u^2(1 - u^2) = -3$, quindi $1 - u^2$ non è un quadrato in $\mathbb{Q}(u)$, infatti se esistesse $\alpha \in \mathbb{Q}(u)$ tale che $\alpha^2 = 1 - u^2$ allora sarebbe $-3 = u^2(1 - u^2) = u^2\alpha^2 = (u\alpha)^2$, quindi -3 sarebbe un quadrato in $\mathbb{Q}(u)$, ma questo è assurdo perché $\mathbb{Q}(u) \subseteq \mathbb{R}$ essendo u reale, e -3 non è un quadrato in $\mathbb{R}$.

4. Sappiamo che $f(u) = 0$ e siccome $f(X)$ è biquadratico anche $f(-u) = 0$, quindi per il teorema di Ruffini $(X - u)(X + u) = X^2 - u^2$ divide $f(X)$. Effettuando la divisione con resto di $f(X)$ per $X^2 - u^2$, oppure applicando il teorema di Ruffini prima a u e poi a $-u$ troviamo

$$f(X) = (X^2 - u^2)(X^2 - (1 - u^2)).$$

Quindi uno zero di $f(X)$ diverso da u e da $-u$ è una radice quadrata di $1-u^2$. Per il punto precedente $\mathbb{Q}(u)$ non contiene radici quadrate di $1-u^2$, quindi $\mathbb{Q}(u)$ non è un campo di spezzamento per $f(X)$ su $\mathbb{Q}$.

5. Sappiamo che u ha grado 4 su $\mathbb{Q}$ e per il punto precedente un campo di spezzamento per $f(X)$ su $\mathbb{Q}$ è $\mathbb{Q}(u,\alpha)$ dove α è una radice quadrata di $1-u^2$, e non appartiene a $\mathbb{Q}(u)$. Siccome α è zero di $X^2-(1-u^2)$ segue allora che $|\mathbb{Q}(u)(\alpha):\mathbb{Q}(u)|=2$. Quindi

$$|\mathbb{Q}(u,\alpha):\mathbb{Q}| = |\mathbb{Q}(u)(\alpha):\mathbb{Q}(u)| \cdot |\mathbb{Q}(u):\mathbb{Q}| = 2\cdot 4 = 8.$$