Svolgimento del secondo compitino di Algebra 2 (a.a 2014-2015).

1. Enunciare e dimostrare il lemma di Gauss.

   Svolgimento. *Lemma di Gauss*: Sia D un dominio a fattorizzazione unica e siano $f(X), g(X) \in D[X]$ primitivi, cioè il massimo comun divisore dei loro coefficienti sia uguale a 1. Allora $f(X)g(X)$ è primitivo.

   Dimostrazione. Supponiamo per assurdo che $f(X)g(X)$ non sia primitivo. Allora esiste $p \in D$ irriducibile tale che p divide tutti i coefficienti di $f(X)g(X)$. Osserviamo che $\overline{D} := D/(p)$ è un dominio di integrità, infatti se $a, b \in D$ e $ab \in (p)$ allora p divide ab quindi, per l'unicità della fattorizzazione, deduciamo che p divide a oppure p divide b, e quindi abbiamo che se $(a + (p))(b + (p)) = 0$ in $\overline{D}$ allora uno tra $a + (p)$ e $b + (p)$ è zero. Consideriamo l'omomorfismo di riduzione $\varphi : D[X] \to \overline{D}[X]$. Siccome $f(X)$ è primitivo ha un coefficiente non divisibile per p, di conseguenza per il polinomio ridotto $\overline{f}(X) = \varphi(f(X))$ vale $\overline{f}(X) \neq 0$. Analogamente $\overline{g}(X) \neq 0$. D'altra parte $\overline{f}(X)\overline{g}(X) = \overline{f(X)g(X)} = 0$ essendo p un divisore di tutti i coefficienti di $f(X)g(X)$. Ne segue che $\overline{f}, \overline{g} \neq 0$ ma $\overline{f}\,\overline{g} = 0$, e questo è assurdo perché $\overline{D}[X]$ è un dominio di integrità, essendo $\overline{D}$ un dominio di integrità.

2. Sia F un campo. Provare che u è algebrico su F se e solo se $F[u]$ ha dimensione finita come spazio vettoriale su F.

   Svolgimento. ($\Rightarrow$) Supponiamo che u sia algebrico su F, in altre parole u è zero di un polinomio non nullo di $F[X]$. Sia $f(X) \in F[X]$ il suo polinomio minimo, e sia n il suo grado. Siano $v_i := u^i$ per $i = 0, \ldots, n-1$. Mostriamo che $\{v_0, \ldots, v_{n-1}\}$ è un insieme di generatori per $F[u]$ su F. Un generico elemento di $F[u]$ ha la forma $P(u)$ dove $P(X) \in F[X]$. Sia $P(u) \in F[u]$. Effettuiamo la divisione con resto di $P(X)$ per $f(X)$ ottenendo $P(X) = f(X)Q(X)+R(X)$ con $R(X)$ di grado minore di n oppure $R(X) = 0$. Valutando in u abbiamo $P(u) = f(u)Q(u) + R(u) = R(u)$ essendo $f(u) = 0$, quindi $P(u)$ ha la forma $R(u)$ con $R(X)$ di grado minore di n. Ne segue che $R(u)$ è combinazione lineare di $v_0, \ldots, v_{n-1}$.

   ($\Leftarrow$) Supponiamo che $F[u]$ abbia dimensione finita come spazio vettoriale su F. Sia n la sua dimensione. Allora l'insieme $\{1, u, u^2, \ldots, u^n\}$ ha cardinalità $n+1$, maggiore della dimensione di $F[u]$ su F, quindi è linearmente dipendente su F, in altre parole esistono $a_0, \ldots, a_n \in F$ non tutti nulli tali che $a_0 + a_1u + a_2u^2 + \ldots + a_nu^n = 0$. Ne segue che u è zero del polinomio non nullo $a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ quindi è algebrico su F.

3. Utilizzare il lemma di Zorn per dimostrare che ogni gruppo G non abeliano contiene un sottogruppo proprio massimale rispetto alla proprietà di essere abeliano.

   Svolgimento. Sia G un gruppo non abeliano (con elemento neutro 1, e useremo la notazione moltiplicativa) e sia $\mathfrak{X}$ la famiglia dei sottogruppi abeliani di G. Si ha $\mathfrak{X} \neq \emptyset$ in quanto $\{1\} \in \mathfrak{X}$. Dobbiamo trovare un

elemento massimale in $\mathfrak{X}$. Per farlo usiamo il lemma di Zorn. Dobbiamo quindi mostrare che se C è una catena in $\mathfrak{X}$, cioè un sottoinsieme di $\mathfrak{X}$ tale che la relazione di inclusione induce su C un ordine totale, allora esiste un maggiorante di C in $\mathfrak{X}$. Scriviamo $C = \{H_\lambda \ : \ \lambda \in \Lambda\}$. Certamente $H := \bigcup_{\lambda\in\Lambda} H_\lambda$ è un maggiorante per C. Ci resta da mostrare che $H \in \mathfrak{X}$, cioè che H è un sottogruppo abeliano di G.

- $1 \in H$. Questo segue dal fatto che per un $\lambda \in \Lambda$ si ha $H_\lambda \leq G$ quindi $1 \in H_\lambda \subseteq H$ (per definizione di unione) quindi $1 \in H$.
- Se $x, y \in H$ allora $xy^{-1} \in H$. Infatti siccome $x, y \in H$ allora per definizione di unione esistono $\lambda, \mu \in \Lambda$ con $x \in H_\lambda$ e $y \in H_\mu$. Ora siccome C è una catena si ha $H_\lambda \subseteq H_\mu$ oppure $H_\mu \subseteq H_\lambda$. Supponiamo senza perdita in generalità che sia $H_\lambda \subseteq H_\mu$. Allora $x \in H_\lambda \subseteq H_\mu$ quindi $x, y \in H_\mu$. Siccome H_μ è un sottogruppo di G si ha $xy^{-1} \in H_\mu \subseteq H$ quindi $xy^{-1} \in H$.
- Se $x, y \in H$ allora $xy = yx$. Come sopra, siccome C è una catena esiste $\mu \in \Lambda$ con $x, y \in H_\mu$ per cui siccome H_μ è abeliano e contiene x, y si ha $xy = yx$.

Abbiamo dimostrato che ogni catena ammette un maggiorante in $\mathfrak{X}$. Per il lemma di Zorn $\mathfrak{X}$ ha elementi massimali.

4. Sia $f(x) \in \mathbb{Q}[x]$ un polinomio di grado $n \geq 1$ e si definisca

$$f^*(x) = x^n f\left(\frac{1}{x}\right).$$

   (a) Provare che se $f(0) \neq 0$ e $f^*(x)$ è irriducibile in $\mathbb{Q}[x]$, allora anche $f(x)$ lo è.

   (b) Usare il punto precedente e il lemma di Eisenstein per provare che $f(x) = 2x^4 + 6x^3 - 8x + 9$ è irriducibile in $\mathbb{Q}[x]$.

   (c) Sia u uno zero di $f(x)$ in un opportuno campo di spezzamento. Scrivere u^{-1} nella forma $a_3u^3 + a_2u^2 + a_1u + a_0$ con $a_0, a_1, a_2, a_3 \in \mathbb{Q}$.

   (d) Sia u uno zero di $f(x)$ in un opportuno campo di spezzamento e sia $v = 4u^5 + 12u^4 + 18u - 4$. Scrivere v nella forma $a_3u^3 + a_2u^2 + a_1u + a_0$ con $a_0, a_1, a_2, a_3 \in \mathbb{Q}$.

   (e) Provare che $\mathbb{Q}[v] = \mathbb{Q}[u]$.

   Svolgimento.

   (a) In altre parole dobbiamo mostrare che se $f(x)$ è riducibile allora $f^*(x)$ è riducibile. Per farlo mostriamo che per ogni $f, g \in \mathbb{Q}[x]$ si ha $(fg)^* = f^*g^*$. Siano r il grado di f e s il grado di g, $n = r + s$ il grado di fg. Si ha $(fg)^*(x) = x^n(fg)(1/x) = x^{r+s}f(1/x)g(1/x) = (x^r f(1/x))(x^s g(1/x)) = f^*(x)g^*(x)$. Supponiamo ora $f(0) \neq 0$ e $f(x)$ riducibile, e scriviamo $f(x) = g(x)h(x)$ con g, h di grado r, s

rispettivamente, e $r, s > 0$, $r + s = n$ con n il grado di f. Allora poiché $g(0)h(0) = f(0) \neq 0$, si ha $g(0) \neq 0$, $h(0) \neq 0$, quindi g^* ha grado r, h^* ha grado s e $f^* = g^*h^*$ per quanto visto, quindi f^*, che ha grado $n = r + s$ essendo $f(0) \neq 0$, è riducibile.

(b) Si ha $f^*(x) = 9x^4 - 8x^3 + 6x + 2$ è irriducibile per il criterio di Eisenstein applicato al primo 2. Quindi per il punto (1) anche $f(x)$ è irriducibile.

(c) Si ha $f(u) = 0$, cioè $2u^4 + 6u^3 - 8u + 9 = 0$, da cui $u(2u^3 + 6u^2 - 8) = -9$. Dividendo per -9 abbiamo $u \cdot (-\frac{2}{9}u^3 - \frac{2}{3}u^2 + \frac{8}{9}) = 1$ per cui, per definizione di inverso, $u^{-1} = -\frac{2}{9}u^3 - \frac{2}{3}u^2 + \frac{8}{9}$.

(d) Abbiamo $v = 4u^5 + 12u^4 + 18u - 4$. Per scriverlo nella forma richiesta scriviamo prima u^4, u^5 come polinomi in u di grado al più 3. Abbiamo $u^4 = -3u^3 + 4u - 9/2$ da cui

$$\begin{aligned} u^5 &= u \cdot u^4 = u(-3u^3 + 4u - \frac{9}{2}) = -3u^4 + 4u^2 - \frac{9}{2}u \\ &= -3(-3u^3 + 4u - \frac{9}{2}) + 4u^2 - \frac{9}{2}u \\ &= 9u^3 + 4u^2 - \frac{33}{2}u + \frac{27}{2}, \end{aligned}$$

Ne segue che

$$\begin{aligned} v &= 4u^5 + 12u^4 + 18u - 4 \\ &= 4(9u^3 + 4u^2 - \frac{33}{2}u + \frac{27}{2}) + 12(-3u^3 + 4u - \frac{9}{2}) + 18u - 4 \\ &= 16u^2 - 4. \end{aligned}$$

(e) Dobbiamo mostrare che $\mathbb{Q}[u] = \mathbb{Q}[v]$. Ricordiamo che essendo u, v algebrici su $\mathbb{Q}$, $\mathbb{Q}[u] = \mathbb{Q}(u)$ e $\mathbb{Q}[v] = \mathbb{Q}(v)$. Siccome $v \in \mathbb{Q}(u)$ si ha $\mathbb{Q}(v) \subseteq \mathbb{Q}(u)$ quindi basta mostrare che $\mathbb{Q}(u)$ e $\mathbb{Q}(v)$ hanno la stessa dimensione su $\mathbb{Q}$, in altre parole basta mostrare che v ha grado 4 su $\mathbb{Q}$. Ora $\mathbb{Q}(v) = \mathbb{Q}(16u^2 - 4) = \mathbb{Q}(u^2)$ quindi basta mostrare che u^2 ha grado 4 su $\mathbb{Q}$. Si ha

$$4 = |\mathbb{Q}(u) : \mathbb{Q}| = |\mathbb{Q}(u) : \mathbb{Q}(u^2)| \cdot |\mathbb{Q}(u^2) : \mathbb{Q}|$$

quindi il grado di u^2 divide 4, cioè è 1, 2 o 4. Rimane da escludere che u^2 abbia grado 1 o 2. Sia $w := u^2$. Se w avesse grado 1 o 2 allora esisterebbero $a, b \in \mathbb{Q}$ con $aw + b = w^2$, da cui

$$au^2 + b = aw + b = w^2 = u^4 = -3u^3 + 4u - 9/2,$$

quindi $3u^3 + au^2 - 4u + b + 9/2 = 0$, assurdo perché u ha grado 4 su $\mathbb{Q}$ (quindi non può essere zero di un polinomio non nullo di grado minore di 4).

5. Sia $u = \sqrt{\sqrt[3]{4} - 1}$.

   (a) Determinare il polinomio minimo di u su $\mathbb{Q}$.

   (b) Provare che $\mathbb{Q}[u]$ contiene $\sqrt[3]{4}$ e calcolare $|\mathbb{Q}[u] : \mathbb{Q}[\sqrt[3]{4}]|$.

   (c) Determinare il polinomio minimo $h(x)$ di u^2 su $\mathbb{Q}$.

   (d) Sia E il campo di spezzamento di $h(x)$ su $\mathbb{Q}$. Provare che E contiene una radice primitiva terza di 1.

   (e) Determinare $|E : \mathbb{Q}|$.

   Svolgimento.

   (a) Si ha $(u^2 + 1)^3 = 4$ cioè $u^6 + 3u^4 + 3u^2 + 1 = 4$, quindi u è zero di $f(X) = X^6 + 3X^4 + 3X^2 - 3$ che è irriducibile per il criterio di Eisenstein, quindi essendo monico è il polinomio minimo di u su $\mathbb{Q}$. Quindi u ha grado 6 su $\mathbb{Q}$.

   (b) $\mathbb{Q}[u] = \mathbb{Q}(u)$ contiene $u^2 + 1 = \sqrt[3]{4}$. Ora $\sqrt[3]{4}$ è zero di $X^3 - 4$, che è irriducibile in $\mathbb{Q}$ per il lemma di Gauss poiché ha grado 3 e non ha zeri in $\mathbb{Z}$. Ne segue che $\sqrt[3]{4}$ ha grado 3 su $\mathbb{Q}$ quindi per la formula dei gradi

   $$6 = |\mathbb{Q}(u) : \mathbb{Q}| = |\mathbb{Q}(u) : \mathbb{Q}(\sqrt[3]{4})| \cdot |\mathbb{Q}(\sqrt[3]{4}) : \mathbb{Q}| = |\mathbb{Q}(u) : \mathbb{Q}(\sqrt[3]{4})| \cdot 3,$$

   e ne deduciamo che $|\mathbb{Q}(u) : \mathbb{Q}(\sqrt[3]{4})| = 6/3 = 2$.

   (c) Siccome $(u^2 + 1)^3 = 4$, u^2 è zero di $h(X) = (X + 1)^3 - 4 = X^3 + 3X^2 + 3X - 3$ che è irriducibile per il criterio di Eisenstein quindi essendo monico è il polinomio minimo di u^2 su $\mathbb{Q}$.

   (d) Si ha $h(X) = (X+1)^3-4$ quindi le tre radici complesse di $h(X)$ sono u^2, ζu^2 e $\zeta^2 u^2$ dove ζ è una radice primitiva terza di 1. Ne segue che il campo di spezzamento $E = \mathbb{Q}(u^2, \zeta u^2, \zeta^2 u^2)$ certamente contiene $(\zeta u^2)/u^2 = \zeta$, essendo un campo.

   (e) Dal punto precedente deduciamo che $E = \mathbb{Q}(u^2, \zeta)$. Ora u^2 ha grado 3 su $\mathbb{Q}$ ed è reale, mentre ζ ha grado 2 su $\mathbb{Q}$ ed è non reale. Ne segue che ζ ha grado al più 2 su $\mathbb{Q}(u^2)$ (essendo zero di $X^2 + X + 1 \in \mathbb{Q}(u^2)[X]$) e non ha grado 1 su $\mathbb{Q}(u^2)$ essendo altrimenti $\zeta \in \mathbb{Q}(u^2) \subseteq \mathbb{R}$, assurdo dato che $\zeta \notin \mathbb{R}$. Quindi $|\mathbb{Q}(u^2)(\zeta) : \mathbb{Q}(u^2)| = 2$ per cui, per la formula dei gradi,

   $$\begin{aligned} |E : \mathbb{Q}| &= |\mathbb{Q}(u^2, \zeta) : \mathbb{Q}| = |\mathbb{Q}(u^2)(\zeta) : \mathbb{Q}| \\ &= |\mathbb{Q}(u^2)(\zeta) : \mathbb{Q}(u^2)| \cdot |\mathbb{Q}(u^2) : \mathbb{Q}| = 2 \cdot 3 = 6. \end{aligned}$$

6. Sia F un campo finito e sia $f(x) = x^5 + 4x^3 + x^2 + 2x + 4$.

   (a) Provare che 1 è uno zero multiplo di $f(x)$ se e solo se F ha caratteristica 3.

   (b) Fattorizzare $f(x)$ nel caso $F = \mathbb{Z}/3\mathbb{Z}$.

(c) Determinare l'ordine di un campo di spezzamento di $f(x)$ su $F = \mathbb{Z}/3\mathbb{Z}$.

Svolgimento.

(a) Uno zero multiplo di $f(x)$ è uno zero comune di $f(x)$ e di $f'(x)$. Quindi 1 è uno zero multiplo di $f(x)$ se e solo se $f(1) = 0$ e $f'(1) = 0$. Si ha $f'(x) = 5x^4 + 12x^2 + 2x + 2$, quindi le condizioni $f(1) = 0$, $f'(1) = 0$ sono le seguenti:

$$0 = f(1) = 1+4+1+2+4 = 12, \qquad 0 = f'(1) = 5+12+2+2 = 21.$$

Abbiamo cioè $12 = 0$ e $21 = 0$, equivalentemente $MCD(12, 21) = 0$ cioè $3 = 0$, in altre parole F ha caratteristica 3.

(b) Applicando Ruffini a $f(x)$ con la radice 1 due volte otteniamo $f(x) = (x-1)^2(x^3 + 2x^2 + x + 1)$. Questa è la fattorizzazione di $f(x)$ in irriducibili in quanto $g(x) = x^3 + 2x^2 + x + 1$ è irriducibile in $F[X]$ perché non ha zeri in $F = \mathbb{F}_3 = \{0, 1, 2\}$.

(c) Sia u uno zero di $g(x)$ in un'opportuna estensione di F. Siccome u ha grado 3 su F (il suo polinomio minimo è $g(x)$), $F[u]$ ha dimensione 3 su F quindi è un campo finito di $|F|^3 = 3^3 = 27$ elementi. Siccome $g(x)$ è irriducibile e ha uno zero nel campo finito $F[u]$, si spezza completamente su $F[u]$ quindi $F[u]$ è un campo di spezzamento per $g(x)$ su F. Se ora indichiamo con E un campo di spezzamento di $f(x)$ su F abbiamo $E = F(1, u) = F(u) = F[u]$ quindi $|E| = |F[u]| = 27$.