Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Prova scritta dell'11 novembre 2019

Si risolvano i seguenti esercizi.

1) Si considerino l'elemento $x^2+1 \in \mathbb{Z}[x]$ e l'anello $A = \mathbb{Z}[x]/(x^2+1)$.

i) Dire se in $\mathbb{Z}[x]$ l'ideale generato da x^2+1 sia primo e se sia massimale; nel caso non sia massimale, determinare un ideale intermedio tra (x^2+1) e (1).

ii) Dire se l'anello A sia un dominio di integrità, se sia un dominio a fattorizzazione unica, se sia un domino a ideali principali, se sia un dominio euclideo, se sia un campo.

iii) Dire se in A gli elementi 2, x, $2x$ e $2+x$ siano fattorizzabili in irriducibili; in caso affermativo se ne determini una fattorizzazione in irriducibili.

2) Si considerino i gruppi G_1, G_2, G_3, G_4, G_5 definiti nel modo seguente:

$$G_1 = C_6 \times C_{15} \times C_{20}, \quad G_2 = C_{30} \times C_{60}, \quad G_3 = C_{1800}, \quad G_4 = D_{900}, \quad G_5 = \mathcal{S}_6 \times C_{15}$$

dove per ogni $n > 0$ C_n denota il gruppo cicico di ordine n, D_n il gruppo diedrale delle simmetrie del poligono regolare di n lati, $\mathcal{S}_n$ il gruppo simmetrico delle permutazioni di un insieme di n elementi.

i) Per ogni $i \in \{1,2,3,4,5\}$ dire se G_i sia abeliano e se sia risolubile.

ii) Determinare gli $i, j \in \{1,2,3,4,5\}$ tali che $G_i \cong G_j$.

iii) Per ogni $i \in \{1,2,3,4,5\}$ determinare il centro $Z(G_i)$ di G_i.

iv) Per ogni $i \in \{1,2,3,4,5\}$ determinare il sottogruppo derivato G_i' di G_i.

3) Si consideri il polinomio $p(x) = x^3 - 7 \in \mathbb{Q}[x]$ e siano K il campo di spezzamento di $p(x)$, G il gruppo di Galois di K su $\mathbb{Q}$.

i) $p(x)$ è irriducibile? è risolubile per radicali?

ii) Calcolare $[K : \mathbb{Q}]$ e determinare K; trovare un elemento $\alpha \in K$ tale che $K = \mathbb{Q}(\alpha)$.

iii) Descrivere G; dato un elemento $\beta \in K$ tale che $p(\beta) = 0$ determinare il sottogruppo H di G corrispondente alla sottoestensione $\mathbb{Q}(\beta) \subseteq K$.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Soluzioni della prova scritta dell'11 novembre 2019

1)
i) e ii) $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica perché $\mathbb{Z}$ lo è, e x^2+1 è irriducibile in $\mathbb{Z}[x]$ per il lemma di Gauss perché è irriducibile in $\mathbb{Q}[x]$ e primitivo; quindi x^2+1 è un elemento primo, $(x^2+1) \subseteq \mathbb{Z}[x]$ è un ideale primo e $A = \mathbb{Z}[x]/(x^2+1)$ è un dominio di integrità.
Più precisamente l'immagine di x in A è una radice quadrata di -1 (che possiamo quindi indicare con i) e, poiché x^2+1 è monico, $\{a+bx|a,b \in \mathbb{Z}\}$ è un insieme di rappresentanti per A, cioè $A = \{a+ib|a,b \in \mathbb{Z}\}$ con $i^2 = -1$.
Quindi $A = \mathbb{Z}[i] \subseteq \mathbb{C}$ è l'anello degli interi di Gauss: è dunque un dominio euclideo (con valutazione $v(a+ib) = a^2+b^2$; in particolare A è a ideali principali e a fattorizzazione unica) e non è un campo (ad esempio 2 non è invertibile).
Ne segue che (x^2+1) non è massimale.
In particolare l'ideale di A generato da 2 è non banale (diverso da (0) e da A), cioè $(x^2+1) \subsetneq (2, x^2+1) \subsetneq \mathbb{Z}[x]$.
iii) A è a fattorizzazione unica quindi ogni elemento di A ha una (unica a meno di invertibili) fattorizzazione.
i è invertibile in A con inverso $i^{-1} = -i$, quindi: i ha fattorizzazione banale; 2 e $2i$ hanno la stessa fattorizzazione a meno di invertibili (i).
Ora: $v(2) = 4 \neq v(1) \neq 5 = v(2+i)$ quindi 2, $2i$ e $2+i$ non sono invertibili e $2+i$ è irriducibile, mentre $2 = pq$ con $v(p) = v(q) = 2$ (perché v è moltiplicativa, 5 è un numero primo e $4 = 2 \cdot 2$ è la fattorizzazione di 4 in $\mathbb{Z}$).
In particolare $p = \pm 1 \pm i$; poiché $1+i$ e $1-i$ sono associati $(1+i = i(1-i))$ si ha che $1+i|2$; d'altra parte $(1+i)^2 = 2i$, che è quindi la fattorizzazione in irriducibili di $2i$.

2)
i) G_1, G_2, G_3 sono abeliani perché prodotti diretti di gruppi ciclici (abeliani); sono quindi anche risolubili.
$G_4 = D_{900} =< r, s|r^{900} = id, s^2 = id, srs^{-1} = r^{-1} >$ non è abeliano perché r ed s non commutano $(r^{-1} \neq r)$; è risolubile perché il sottogruppo generato da r è normale di indice 2 e abeliano.
G_5 non è né abeliano né risolubile perché contiene un sottogruppo isomorfo a $\mathcal{S}_6$, che non è né abeliano né risolubile.
ii) Ovviamente $G_i \cong G_i \ \forall i$.
D'altra parte $G_5 \ncong G_i$ per $i \neq 5$ perché G_5 non è risolubile mentre gli altri gruppi sono tutti risolubili.
Analogamente $G_4 \ncong G_i$ per $i \neq 4$ perché inoltre G_4 non è abeliano mentre G_1, G_2 e G_3 lo sono.
$G_3 \ncong G_2$ e $G_3 \ncong G_1$ perché in G_3 esiste un elemento di ordine 1800 mentre in G_2 l'ordine di ogni elemento divide $MCD(30,60) = 60$ e in G_1 l'ordine di ogni elemento divide $MCD(6,15,20) = 60$.
Resta da capire se G_1 e G_2 siano isomorfi: da quanto appena visto, in G_1 esiste un elemento di ordine 60, quindi $G_1 \cong C_{60} \times H$ con H gruppo abeliano di $\frac{6 \cdot 15 \cdot 20}{60} = 30$ elementi; ma un tale gruppo è necessariamente isomorfo a C_{30} perché 30 è prodotto di primi distinti, quindi $G_1 \cong C_{60} \times C_{30} \cong G_2$.
iii) $Z(G_i) = G_i$ per $i = 1,2,3$ perché in questi casi G_i è abeliano.

In G_4 le riflessioni non sono centrali perché non commutano con r, mentre una rotazione r^m commuta con s se e solo se $r^{-m} = r^m$; quindi $Z(G_4) =< r^{450} > \cong C_2$.
Infine $Z(G_5) = Z(\mathcal{S}_6) \times Z(C_{15}) = \{id\} \times C_{15} \cong C_{15}$.
iv) $G_i' = \{id\}$ per $i = 1, 2, 3$ perché in questi casi G_i è abeliano.
In G_4 $r^m s r^n (r^m s)^{-1} r^{-n} = r^{-2n}$ ed $r^m s r^n s (r^m s)^{-1} (r^n s)^{-1} = r^{2m-2n}$, quindi $G_4' =< r^2 > \cong C_{450}$.
Infine $G_5' = \mathcal{S}_6' \times C_{15}' = \mathcal{A}_6 \times \{id\} \cong \mathcal{A}_6$.

3)
i) $p(x)$ è irriducibile per il criterio di Eisenstein ed è risolubile per radicali perché ha grado $3 < 5$.
ii) $[K : \mathbb{Q}]|3! = 6$ perché $deg(p(x)) = 3$.
Sia β una radice di $p(x)$; da i) segue che $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, quindi $3|[K : \mathbb{Q}]$ perché $[K : \mathbb{Q}] = [K : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$.
D'altra parte K contiene una radice primitiva 3^a di 1 ($\omega =$ rapporto tra due radici distinte di $p(x)$) che ha grado 2 su $\mathbb{Q}$, quindi non appartiene a $\mathbb{Q}(\beta)$ e ha grado 2 anche su $\mathbb{Q}(\beta)$.
Dunque $\mathbb{Q} \subsetneq \mathbb{Q}(\beta) \subsetneq \mathbb{Q}(\beta, \omega) \subseteq K$ e $[\mathbb{Q}(\beta, \omega) : \mathbb{Q}(\beta)] = 2$, quindi $[\mathbb{Q}(\beta, \omega) : \mathbb{Q}] = 6$ e $K = \mathbb{Q}(\beta, \omega)$. In particolare $\{1, \beta, \beta^2, \omega, \beta\omega, \beta^2\omega\}$ è una base di K su $\mathbb{Q}$.
Poiché G è un sottogruppo di $\mathcal{S}_{\{radici\ di\ p(x)\}}$ (che è isomorfo a $\mathcal{S}_3$) di cardinalità $\#G = [K : \mathbb{Q}] = 6$, abbiamo $G \cong \mathcal{S}_3$; G ha un sottogruppo di indice 2 e tre sottogruppi di indice 3, a cui corrispondono rispettivamente una sottoestensione di K di grado 2 ($\mathbb{Q}(\omega)$) e tre sottoestensioni di grado 3 ($\mathbb{Q}(\beta)$, $\mathbb{Q}(\beta\omega)$, $\mathbb{Q}(\beta\omega^2)$).
Qualsiasi elemento che non appartiene all'unione di queste sottoestensioni è un elemento primitivo, cioè genera K.

Prima di esibire esplicitamente un elemento primitivo α discutiamo il punto iii).
iii) Il sottogruppo H di G corrispondente alla sottoestensione $\mathbb{Q}(\beta)$ di K è il sottogruppo degli automorfismi di K che fissano β, cioè $H = \{g \in G | g(\beta) = \beta\}$; poiché $[K : \mathbb{Q}(\beta)] = 2$, $H =< \sigma >$ con $o(\sigma) = 2$; σ permuta tra loro le altre due radici di $p(x)$ e permuta tra loro le due radici primite 3^e di 1: $\sigma(\beta\omega) = \beta\omega^2$ e $\sigma(\omega) = \omega^2$.

Proviamo ora che se poniamo $\alpha = \beta + \omega$ abbiamo $K = \mathbb{Q}(\alpha)$. Ovviamente $\alpha \notin \mathbb{Q}(\beta)$ e $\alpha \notin \mathbb{Q}(\omega)$.
Sia $\sigma \in G$ tale che $\sigma \neq id$ e $\sigma(\beta\omega) = \beta\omega$; allora $\sigma(\beta) = \beta\omega^2$ e $\sigma(\omega) = \omega^2$, quindi $\sigma(\alpha) = \beta\omega^2 + \omega^2 = -\beta\omega - \beta - \omega - 1 \neq \alpha$ quindi $\alpha \notin \mathbb{Q}(\beta\omega)$.
Analogamente se $\sigma \neq id$ è tale che $\sigma(\beta\omega^2) = \beta\omega^2$ allora $\sigma(\beta) = \beta\omega$ e $\sigma(\omega) = \omega^2$, quindi $\sigma(\alpha) = \beta\omega + \omega^2 = \beta\omega - \omega - 1 \neq \alpha$ quindi $\alpha \notin \mathbb{Q}(\beta\omega)$.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Prova scritta del 20 settembre 2019

Si risolvano i seguenti esercizi.

1) Siano $A = \mathbb{Q}[x,y]/(x^2 - y)$ e $f = xy - 1 \in A$.

i) Dimostrare che A è un dominio a fattorizzazione unica; A è un dominio euclideo? è un dominio a ideali principali?

ii) Fattorizzare f in irriducibili.

iii) Determinare tutti gli A-moduli M tali che $dim_{\mathbb{Q}} M = 2$: sono tutti ciclici?

2) Siano G un gruppo, $Aut(G)$ il gruppo degli automorfismi di G, $H \leq G$ un sottogruppo. H si dice sottogruppo *caratteristico* di G se per ogni $\varphi \in Aut(G)$ si ha $\varphi(H) \subseteq H$.

i) Dimostrare che se H è un sottogruppo caratteristico di G allora per ogni $\varphi \in Aut(G)$ si ha $\varphi(H) = H$.

ii) Dimostrare che se H è un sottogruppo caratteristico di G allora $H \trianglelefteq G$ (H è normale in G) e che il viceversa è falso.

iii) Sia G' il sottogruppo derivato di G; G' è un sottogruppo caratteristico di G?

iv) Siano G finito e H un sottogruppo di Sylow di G; è vero che se $H \trianglelefteq G$ allora H è un sottogruppo caratteristico di G?

3) Si consideri il polinomio $p(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ e siano K il campo di spezzamento di $p(x)$, G il gruppo di Galois di K su $\mathbb{Q}$.

i) $p(x)$ è irriducibile? è risolubile per radicali?

ii) Calcolare $[K : \mathbb{Q}]$ e determinare K; in particolare se α è una radice di $p(x)$ è vero che $K = \mathbb{Q}(\alpha)$?

iii) Descrivere G e illustrare la corrispondenza di Galois per l'estensione $\mathbb{Q} \subseteq K$. Esiste un campo $E \subseteq K$ tale che $[E : \mathbb{Q}] = 3$?

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Soluzioni della prova scritta del 20 settembre 2019

1)
i) Se R è un anello commutativo unitario e $a \in R$ si ha $R[T]/(T-a) \cong R$, quindi ponendo $R = \mathbb{Q}[x]$, $a = x^2$, $T = y$ si ha $A \cong \mathbb{Q}[x]$

Dunque A è un dominio euclideo, quindi un dominio a ideali principali e a fattorizzazione unica.
ii) Fattorizzare $f = xy - 1 = x^3 - 1$ in A significa fattorizzare $x^3 - 1$ in $\mathbb{Q}[x]$.
Ora 1 è una radice di $x^3 - 1$, quindi $(x-1)|x^3 - 1 = (x-1)(x^2 + x + 1)$; $x^2 + x + 1$ non ha radici razionali ed è di grado 2, quindi è irriducibile (basta anche osservare che $x^2 + x + 1$ è un polinomio ciclotomico).

Quindi $f = (x-1)(x^2 + x + 1)$ è la fattorizzazione di f in irriducibili.
iii) $\mathbb{Q}[x]$ è un $\mathbb{Q}[x]$-modulo di dimensione infinita su $\mathbb{Q}$.
Sia $p \in \mathbb{Q}[x]$ di grado d; il $\mathbb{Q}[x]$-modulo $\mathbb{Q}[x]/(p)$ ha dimensione d su $\mathbb{Q}$ (ed è ciclico).
D'altra parte ogni $\mathbb{Q}[x]$-modulo M di dimensione finita su $\mathbb{Q}$ è finitamente generato come $\mathbb{Q}[x]$-modulo, quindi è della forma $\mathbb{Q}[x]/(p_1) \oplus ... \oplus \mathbb{Q}[x]/(p_r)$ con $p_1|...|p_r$ e $\sum_{i=1}^{r} deg(p_i) = dim_{\mathbb{Q}} M$; M è ciclico se e solo se $r = 1$.

Dunque i $\mathbb{Q}[x]$-moduli di dimensione 2 sono:

$$\mathbb{Q}[x]/(x^2 + ax + b) \quad (a, b \in \mathbb{Q}) \quad - \text{ ciclico}$$

$$\mathbb{Q}[x]/(x-a) \oplus \mathbb{Q}[x]/(x-a) \quad (a \in \mathbb{Q}) \quad - \text{ non ciclico.}$$

2)
i) $\varphi \in Aut(G) \Rightarrow \varphi$ invertibile e $\varphi^{-1} \in Aut(G)$, quindi se $H \leq G$ è caratteristico si ha $\varphi^{-1}H \subseteq H$, da cui $H = \varphi\varphi^{-1}(H) \subseteq \varphi(H)$, che insieme alla condizione $\varphi(H) \subseteq H$ implica $\varphi(H) = H$.
ii) Per ogni $g \in G$ $gHg^{-1} = c_g(H)$ dove il coniugio $c_g : G \to G$ è definito da $c_g(x) = gxg^{-1}$ per ogni $x \in G$ ed è un automorfismo di G. Quindi se H è un sottogruppo caratteristico di G si ha in particolare $gHg^{-1} = H$ per ogni $g \in G$, cioè $H \trianglelefteq G$.
Siano ora $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ e $H = \mathbb{Z}_2 \times \{id\} \leq G$.
G è abeliano, quindi $H \trianglelefteq G$.
D'altra parte la mappa $\sigma : G \to G$ definita da $\sigma(a, b) = (b, a)$ è un automorfismo di G ma $\sigma(H) \not\subseteq H$.
Quindi H non è caratteristico.
iii) Siano $\varphi \in Aut(G)$ e $\pi : G \to G/G'$ la proiezione sul quoziente.
La composizione $\pi \circ \varphi : G \to G/G'$ è un omomorfismo di gruppi da G ad un gruppo abeliano, quindi fattorizza tramite G'. Questo significa che $G' \subseteq ker(\pi \circ \varphi)$, cioè che $\varphi(G') \subseteq G'$.

Dunque G' è caratteristico.
Altra dimostrazione.
G' è il sottogruppo di G generato da $\{xyx^{-1}y^{-1} | x, y \in G\}$, quindi per ogni automorfismo φ di G si ha che $\varphi(G')$ è generato da

$$\{\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} | x, y \in G\} \subseteq \{xyx^{-1}y^{-1} | x, y \in G\}.$$

Dunque $\varphi(G') \subseteq G'$ e G' è caratteristico.

iv) Siano G finito, p un primo, $H \subseteq G$ un p-sottogruppo di Sylow, $\varphi \in Aut(G)$. $\#\varphi(H) = \#H$ quindi $\varphi(H)$ è un p-Sylow di G; ma tutti i p-Sylow di G sono coniugati, quindi esiste $x \in G$ tale che $\varphi(H) = xHx^{-1}$.

Ne segue che un p-Sylow è caratteristico se e solo se è normale.

3)

i) $p(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$, quindi $p(x)$ non è irriducibile.
D'altra parte $p(x)$ è risolubile per radicali perché ha grado 4 (e anche perché le sue radici sono $\pm\sqrt{2}$ e $\pm\sqrt{3}$).
ii) Da i) segue che $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ e $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ perché $x^2 - 2$ e $x^2 - 3$ sono irriducibili di grado 2. Sia $\sigma \in G$; allora $\sigma\big|_{\mathbb{Q}(\sqrt{2})}$ ha autovalori 1 e -1, con autospazi rispettivamente $\mathbb{Q}$ e $\mathbb{Q}\sqrt{2}$; ma $\sigma(\sqrt{3}) = \pm\sqrt{3}$, quindi $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ perché $\sqrt{3} \notin \mathbb{Q}\sqrt{2}$ (e ovviamente $\sqrt{3} \notin \mathbb{Q}$).
Ne segue che $\sqrt{3}$ ha grado 2 su $\mathbb{Q}(\sqrt{2})$.

Quindi $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$ e $K \neq \mathbb{Q}(\sqrt{2})$, $K \neq \mathbb{Q}(\sqrt{3})$.
iii) Poiché $[K : \mathbb{Q}] = 4$ non esistono sottoestensioni di K di grado 3 su $\mathbb{Q}$; inoltre $\#G = 4$.
Poiché $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ sono sottoestensioni distinte e non banali di K, G ha almeno due sottogruppi non banali, quindi $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$; poiché inoltre per ogni $\sigma \in G$ si ha $\sigma(\sqrt{2}) = \pm\sqrt{2}$ e $\sigma(\sqrt{3}) = \pm\sqrt{3}$, ad ogni scelta del segno corrisponde un elemento di G.
Più precisamente: $G = \{id, \sigma, \tau, \sigma\tau\}$ con

$$\sigma(\sqrt{2}) = \sqrt{2}, \quad \sigma(\sqrt{3}) = -\sqrt{3}, \quad \tau(\sqrt{2}) = -\sqrt{2}, \quad \tau(\sqrt{3}) = \sqrt{3}$$

e si ha

$$Fix(\{id\}) = K, \quad Fix(G) = \mathbb{Q},$$

$$Fix(< \sigma >) = \mathbb{Q}(\sqrt{2}), \quad Fix(< \tau >) = \mathbb{Q}(\sqrt{3}), \quad Fix(< \sigma\tau >) = \mathbb{Q}(\sqrt{6}).$$

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Prova scritta del 15 luglio 2019

Si risolvano i seguenti esercizi.

1) Siano $\mathbb{Z}$ l'anello degli interi e $\mathbb{Z}[i]$ l'anello degli interi di Gauss. Osservare che ogni $Z[i]$-modulo ha una struttura naturale di $\mathbb{Z}$-modulo, cioè di gruppo abeliano.

i) Dire se $\mathbb{Z}[i]/(2+i)$ e $\mathbb{Z}[i]/(2-i)$ siano isomorfi come $\mathbb{Z}[i]$-moduli; studiarne e confrontarne la struttura come $\mathbb{Z}$-moduli; studiarne la struttura come anelli.

ii) Dimostrare che il gruppo abeliano $\mathbb{Z}/(25)$ può essere dotato di una struttura di $Z[i]$-modulo (in modo unico?) e determinarne i divisori elementari.

iii) Per quali $p \in \mathbb{Z}$ primi ($p > 0$) l'anello $\mathbb{Z}[i]/(p)$ è un campo? Descrivere tale campo.

2) Si consideri il gruppo $G = \mathcal{S}_3 \rtimes_c \mathcal{S}_3$ dove $c : \mathcal{S}_3 \to Aut(\mathcal{S}_3)$ è il coniugio.

i) Determinare i fattori di composizione di G con la loro molteplicità.

ii) Determinare il sottogruppo derivato G' di G e il quoziente G/G'.

iii) Siano H_2 e H_3 rispettivamente un 2-Sylow e un 3-Sylow di G: dire se H_2 e H_3 siano abeliani e se siano normali in G.

3) Si consideri il polinomio $p(x) = x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2 \in \mathbb{Q}[x]$ e siano K il campo di spezzamento di $p(x)$, G il gruppo di Galois di K su $\mathbb{Q}$.

i) $p(x)$ è irriducibile? è risolubile per radicali?

ii) Calcolare $[K : \mathbb{Q}]$, esibire una base di K su $\mathbb{Q}$ e determinare tutte le sottoestensioni di K.

iii) Scegliere un elemento primitivo $\alpha \in K$, calcolarne il polinomio minimo e determinarne tutti i coniugati, cioè tutti gli elementi $\sigma(\alpha)$ al variare di $\sigma \in G$.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Soluzioni della prova scritta del 15 luglio 2019

1)
i) $2+i$ e $2-i$ sono irriducibili non associati tra loro in $\mathbb{Z}[i]$, quindi i due $\mathbb{Z}[i]$-moduli $\mathbb{Z}[i]/(2+i)$ e $\mathbb{Z}[i]/(2-i)$ non sono isomorfi.
Il coniugio $\mathbb{Z}[i] \ni a+ib \mapsto a-ib \in \mathbb{Z}[i]$ è un omomorfismo di $\mathbb{Z}$-moduli (cioè di gruppi abeliani) e di anelli unitari e trasforma $(2 \pm i)$ in $(2 \mp i)$, quindi induce $\bar{f} : \mathbb{Z}[i]/(2+i) \to \mathbb{Z}[i]/(2-i)$ omomorfismo invertibile (isomorfismo) di $\mathbb{Z}$-moduli e di anelli. Quindi è sufficiente studiare la struttura (di gruppo abeliano e di anello) di $\mathbb{Z}[i]/(2+i)$.
Si consideri la composizione $f : \mathbb{Z} \to \mathbb{Z}[i]/(2+i)$ tra l'omomorfismo naturale di anelli unitari $\mathbb{Z} \to \mathbb{Z}[i]$ e la proiezione sul quoziente $\pi : \mathbb{Z}[i] \to \mathbb{Z}[i]/(2+i)$; f è un omomorfismo sia di gruppi sia di anelli. Inoltre f è suriettiva perché $\pi(i) = f(-2)$. Quindi $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}/ker(f)$. D'altra parte $5 = (2+i)(2-i) \in ker(f)$ quindi $(5) \subseteq ker(f)$, ma (5) è massimale in $\mathbb{Z}$ quindi $ker(f) = (5)$.
Ne segue che $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}_5$ (gruppo ciclico di ordine 5 e anello - campo - di cardinalità 5).
ii) *argomento 1*: Sia $\mathbb{Z}/(25)$ dotato di una struttura di $\mathbb{Z}[i]$-modulo; poiché $\mathbb{Z}/(25)$ è uno $\mathbb{Z}$-modulo ciclico, esso sarà ciclico a maggior ragione come $\mathbb{Z}[i]$-modulo, quindi sarà della forma $\mathbb{Z}[i]/(a+ib)$ con $a, b \in \mathbb{Z}$ tali che $a+ib|25 = (2+i)^2(2-i)^2$. Si osservi che come $\mathbb{Z}$-moduli si ha:

$$\mathbb{Z}[i]/(5) \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5 \ncong \mathbb{Z}_{25},$$

$$\mathbb{Z}[i]/((2+i)^2) \cong \mathbb{Z}[i]/((2-i)^2) \quad \text{(isomorfismo indotto dal coniugio)},$$

$$argomento\ 1a: \qquad \mathbb{Z}[i]/((2+i)^2) \oplus \mathbb{Z}[i]/((2-i)^2) \cong \mathbb{Z}[i]/(25) \cong \mathbb{Z}_{25} \oplus \mathbb{Z}_{25}.$$

Quindi $\mathbb{Z}[i]/((2+i)^2)$ e $\mathbb{Z}[i]/((2-i)^2)$ (che sono $\mathbb{Z}[i]$-moduli non isomorfi tra loro) hanno cardinalità 25 e non possono essere isomorfi (come $\mathbb{Z}$-moduli) a $\mathbb{Z}_5 \oplus \mathbb{Z}_5$, quindi sono entrambi isomorfi a $\mathbb{Z}_{25}$.
argomento 1b: $(2+i)^2 \not| 5$ e $(2+i)^2|25$, quindi $\mathbb{Z}_{25} \hookrightarrow \mathbb{Z}[i]/((2+i)^2) = \mathbb{Z}[i]/(3+4i)$; inoltre $i = (3+4i)(1-i)-7$, quindi la mappa $\mathbb{Z}_{25} \to \mathbb{Z}[i]/(3+4i)$ è anche suriettiva.
argomento 2: dotare $\mathbb{Z}_{25}$ di una struttura di $\mathbb{Z}[i]$-modulo significa descrivere l'azione di i su 1 cioè trovare un elemento $i \in \mathbb{Z}_{25}$ tale che $i^2 = -1$. $\mathbb{Z}_{25}^*$ è un gruppo ciciico di cardinalità 20 quindi esistono esattamente due valori di i con la proprietà cercata: $i = \pm 7$.
Per determinare i divisori elementari d_+ e d_- di questi due $\mathbb{Z}[i]$-moduli (ciclici) si osservi che abbiamo:

$$d_+|(25, i-7) = ((2+i)^2(2-i)^2, -(1+i)(2-i)^2) = (2-i)^2 = 3-4i,$$

$$d_-|(25, i+7) = ((2+i)^2(2-i)^2, -(1-i)(2+i)^2) = (2+i)^2 = 3+4i.$$

e che per il punto i) d_+ e d_- non possono essere $2 \pm i$.

Quindi esistono esattamente due strutture di $\mathbb{Z}[i]$-modulo su $\mathbb{Z}_{25}$:

$$\mathbb{Z}[i]/(3+4i) \cong \mathbb{Z}[i]/((2+i)^2) \quad \text{e} \quad \mathbb{Z}[i]/(3-4i) \cong \mathbb{Z}[i]/((2-i)^2),$$

con divisori elementari rispettivamente $3+4i$ e $3-4i$.
iii) $\mathbb{Z}[i]/(p)$ è un campo se e solo se p è irriducibile in $\mathbb{Z}_[i]$ e questo avviene se e solo se $p \equiv 3 \pmod 4$. Come gruppo additivo abbiamo $\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, quindi abbiamo che:

$\mathbb{Z}[i]/(p)$ è un campo se e solo se $p \equiv 3 \pmod 4$ e in tal caso $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$.

2)
i) I fattori si composizione di $\mathcal{S}_3$ sono $\mathbb{Z}_2$ e $\mathbb{Z}_3$, ciascuno con molteplicità 1.
Si considerino i sottogruppi $G_1 = \mathcal{S}_3 \times \{id\} \trianglelefteq G$, $G_2 = \{id\} \times \mathcal{S}_3 \leq G$: per definizione di G abbiamo $G_1 \cong \mathcal{S}_3$ e $G/G_1 \cong G_2 \cong \mathcal{S}_3$, quindi i fattori di composizione di G sono i fattori di composizione di $\mathcal{S}_3$ contati due volte: $\mathbb{Z}_2$ e $\mathbb{Z}_3$, ciascuno con molteplicità 2.
ii) Abbiamo ovviamente $G' \geq G'_1, G'_2 \cong \mathcal{S}'_3 = \mathcal{A}_3$; d'altra parte G'_1 e G'_2 commutano tra loro perché $\mathcal{A}_3$ è un gruppo commutativo (per ogni $\sigma \in \mathcal{A}_3$ $c(\sigma)\big|_{\mathcal{A}_3} = id$), quindi $K =< G'_1, G'_2 >= G'_1 G'_2 = \{(\sigma_1, \sigma_2) \in G | \sigma_1, \sigma_2 \in \mathcal{A}_3\} (\cong \mathbb{Z}_3 \times \mathbb{Z}_3)$, che è un sottogruppo normale di G tale che G/K ha ordine 4 (quindi è abeliano). Ne segue che $G' \leq K$, quindi $G' = K$.
Per studiare più precisamente G/G' osserviamo che se $\tau \in \mathcal{S}_3$ è una trasposizione si ha che (τ, id) e (id, τ) commutano in G (e hanno ordine 2), quindi generano un sottogruppo H di G isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, la cui intersezione con G' è ovviamente banale. Quindi $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
iii) H_2 e H_3 hanno cardinalità rispettivamente 2^2 e 3^2, quindi sono abeliani. D'altra parte già sono stati esibiti in ii) due sottogruppi di G con queste cardinalità: G' è un 3-Sylow di G (normale in G, quindi è l'unico 3-Sylow di G); H è un 2-Sylow di G, che dipende dalla trasposizione scelta, quindi non è unico e in particolare non è normale.

3)
i) $(x^2+2x+2)(x^3-1) = (x^2+2x+2)(x^2+x+1)(x-1)$, quindi $p(x)$ non è irriducibile ed è risolubile per radicali (in quanto è prodotto di polinomi di grado minore o uguale a 2, che sono tutti risolubili per radicali).
ii) Il campo di spezzamento di (x^2+2x+2) è $\mathbb{Q}(-1+i) = \mathbb{Q}(i)$ e il campo di spezzamento di (x^2+x+1) è $\mathbb{Q}(\omega) = \mathbb{Q}(i\sqrt{3})$ dove ω è una radice primitiva terza di 1. Quindi:
$K = \mathbb{Q}(i, \sqrt{3})$, che ha grado 4 su $\mathbb{Q}$;
$\{1, i, \sqrt{3}, i\sqrt{3}\}$ è una base di K su $\mathbb{Q}$;
$G =< \sigma, \tau > \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ è il gruppo di Galois di K su $\mathbb{Q}$, dove $\sigma(i) = -i$, $\sigma(\sqrt{3}) = \sqrt{3}$, $\tau(i) = i$, $\tau(\sqrt{3}) = -\sqrt{3}$.
I sottogruppi di G sono quindi G, $< \sigma >$, $< \tau >$, $< \sigma\tau >$ e $\{id\}$, a cui corrispondono le sottoestensioni $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{3})$, K.
iii) Per quanto visto in ii) qualsiasi elemento della forma $a + ib + \sqrt{3}c + i\sqrt{3}d$ con almeno due tra b, c, d diversi da zero è un elemento primitivo di K su $\mathbb{Q}$.
Ad esempio $\alpha = i + \sqrt{3} \in K$ è un elemento primitivo. I suoi coniugati sono $\pm i \pm \sqrt{3}$ e il suo polinomio minimo è

$$\prod_{\sigma \in G} x - \sigma(\alpha) = (x - i - \sqrt{3})(x + i - \sqrt{3})(x - i + \sqrt{3})(x + i + \sqrt{3}) =$$

$$= ((x - \sqrt{3})^2 + 1)((x + \sqrt{3})^2 + 1) = (x^2 + 4 - 2\sqrt{3}x)(x^2 + 4 + 2\sqrt{3}x) =$$

$$= x^4 - 4x^2 + 16.$$

Un altro modo per calcolare il polinomio minimo di α è il seguente:
$\alpha = i + \sqrt{3} \Rightarrow (\alpha - i)^2 = 3$, cioè $\alpha^2 - 4 = 2i\alpha$, da cui $-4\alpha^2 = \alpha^4 - 8\alpha^2 + 16$, dunque α annulla il polinomio $x^4 - 4x^2 + 16$; ma poiché α è un elemento primitivo il suo polinomio minimo ha grado 4, quindi è il polinomio trovato.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Prova scritta del 21 giugno 2019

Si risolvano i seguenti esercizi.

1) Siano A un dominio di integrità, Q il campo dei quozienti di A, $\alpha \in A \setminus \{0\}$, $B = A[T]/(\alpha T - 1)$.

i) Dimostrare che B è un dominio di integrità e che $A \subseteq B \subseteq Q$.

ii) Per quali α si ha $B = A$? (*)Esibire un dominio di integrità A e un elemento $\alpha \in A \setminus \{0\}$ tali che si abbia $A \neq B = Q$.

iii) Scegliere un dominio a fattorizzazione unica A e un elemento $\alpha \in A \setminus \{0\}$ e dimostrare che B è a fattorizzazione unica.

iv) Siano $A = K[x]$ e $\alpha = x$. Determinare un A-modulo (V, f) di dimensione 1 su K (o di qualsiasi altra dimensione) la cui struttura di A-modulo si estende ad una struttura di B-modulo e un A-modulo (W, g) di dimensione 1 su K (o di qualsiasi altra dimensione) la cui struttura di A-modulo non si estende ad una struttura di B-modulo.

2) Siano $G = \mathcal{S}_4$ il gruppo delle permutazioni di $\{1, 2, 3, 4\}$, $H = \{\sigma \in G | \sigma(4) = 4\}$, $K =< (1, 2)(3, 4), (1, 3)(2, 4) >$, $C =< (1, 2, 3, 4) >$.

i) Determinare cardinalità e struttura dei gruppi H, K e C.

ii) Dimostrare che $HK = KH$ e $HC = CH$.

iii) G è prodotto diretto o semidiretto di H e K? è prodotto diretto o semidiretto di H e C?

iv) Determinare i fattori di composizione di G.

3) Siano $f(x) = x^5 - 5x^3 + 5 \in \mathbb{Q}[x]$, K il campo di spezzamento di f su $\mathbb{Q}$, $G = Gal(K/\mathbb{Q})$ il gruppo di Galois di K su $\mathbb{Q}$.

i) Dire se f sia irriducibile.

ii) Determinare G e calcolare $[K : \mathbb{Q}]$.

iii) f è risolubile per radicali su $\mathbb{Q}$?

iv) Dimostrare che esiste un campo $E \subseteq K$ tale che $[E : \mathbb{Q}] = 2$ e dire se f sia risolubile per radicali su E.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Soluzioni della prova scritta del 21 giugno 2019

1)
i) Si considerino l'inclusione $i : A \hookrightarrow Q$ e la composizione $f = j \circ \pi$ degli omomorfismi naturali $j : A \hookrightarrow A[T]$ e $\pi : A[T] \to A[T]/(\alpha T - 1)$:

$$f : A \hookrightarrow A[T] \to A[T]/(\alpha T - 1) = B.$$

f è iniettiva perché $A \cap (\alpha T - 1) = \{0\}$: infatti se $p(T) \neq 0$ si ha che $(\alpha T - 1)p(T)$ è diverso da 0 e ha grado maggiore del grado di $p(T)$, quindi non è una costante e non appartiene ad A.

Quindi $A \subseteq B$.
i si estende (in modo unico) ad un omomorfismo $\bar{i} : B = A[T]/(\alpha T - 1) \to Q$: infatti l'ipotesi che α sia diverso da zero implica che α è invertibile in Q, quindi l'omomorfismo $\tilde{i} : A[T] \to Q$ definito da

$$\tilde{i}\big|_A = i, \quad \tilde{i}(T) = \alpha^{-1}$$

mappa $\alpha T - 1$ in zero (cioè si ha $(\alpha T - 1) \subseteq ker(\tilde{i})$) dunque passa al quoziente e induce un omomorfismo $\bar{i} : A[T]/(\alpha T - 1) \to Q$.
$\bar{i}$ è iniettiva perché $ker(\tilde{i}) = (\alpha T - 1)$. Infatti si supponga per assurdo che

$$ker(\tilde{i}) \not\subseteq (\alpha T - 1)$$

e sia

$$p(T) = \sum_{r=0}^{d} a_r T^r \in ker(\tilde{i}) \setminus (\alpha T - 1)$$

di grado minimo d; ovviamente $d > 0$ perché $\bar{i}\big|_A = i$ è iniettiva.
Abbiamo che $0 = \tilde{i}(P(T)) = P(\alpha^{-1}) = \alpha^{-d} \sum_{r=0}^{d} a_r \alpha^{d-r}$ in Q, quindi

$$\sum_{r=0}^{d} a_r \alpha^{d-r} = 0 \ \text{ in } \ A,$$

da cui segue l'esistenza di un elemento $b \in A$ tale che $a_d = \alpha b$.
Ne segue che $P(T) - b(\alpha T - 1)T^{d-1}$ ha grado minore di d e

$$P(T) - b(\alpha T - 1)T^{d-1} \in ker(\tilde{i}) \setminus (\alpha T - 1),$$

cosa che contraddice l'ipotesi di minimalità di d.

Dunque $ker f \subseteq (\alpha T - 1)$ e $B = A[\alpha^{-1}] \subseteq Q$.

In particolare B è un dominio di integrità.
ii) Poiché $B = A[\alpha^{-1}]$ si ha $A = B$ se e solo se $\alpha^{-1} \in A$ cioè se e solo se $\alpha \in A^*$.
ii)(*) $\alpha \notin A^*$ (altrimenti si avrebbe $A = B$), quindi in particolare A non è un campo ($A \neq Q$), ma è un dominio di integrità tale che $A[\alpha^{-1}] = Q$.
Ad esempio:

$$A = K[[x]], \quad \alpha = x;$$

$$A = \left\{ \frac{m}{n} | m, n \in \mathbb{Z}, n \text{ dispari} \right\}, \quad \alpha = 2;$$

$$A = \left\{ \frac{p(x)}{q(x)} \in K(x) | p(x), q(x) \in K[x],\ q(0) \neq 0 \right\}, \quad \alpha = x.$$

iii) Dimostrazione generale.
Se $\alpha \in A^*$ non c'è nulla da dimostrare perché $B = A$.
Sia $\alpha \notin A^*$.
$A[T]$ è un dominio a fattorizzazione unica e $\alpha T - 1 \in A[T]$ è un polinomio primitivo di primo grado, dunque irriducibile (e primo), quindi $(\alpha T - 1) \subseteq A[T]$ è un ideale primo e $B = A[T]/(\alpha T - 1)$ è un dominio di integrità (in particolare questo argomento è un'altra dimostrazione del fatto che B è un dominio di integrità, quando si aggiunga l'ipotesi che A sia a fattorizzazione unica).
Poiché α è invertibile in B, tutti i divisori di α e tutti i fattori irriducibili di α in A sono invertibili in B e $B = \cup_{n \in \mathbb{N}} \alpha^{-n} A$.
Ne segue che ogni elemento non nullo di B è, a meno di invertibili, prodotto di elementi irriducibili di A che non dividono α; inoltre se $a \in A$, $b \in B$ e $n \in \mathbb{N}$ sono tali che $(a, \alpha) = 1$ e $\alpha^n b \in A$, la condizione $a|b$ in B equivale alla condizione $a|\alpha^n b$ in A.
Proviamo adesso che ogni irriducibile (quindi primo) $p \in A$ che non divide α è primo in B: se $p|b_1 b_2$ in B esistono $n_1, n_2 \geq 0$ tali che $\alpha^{n_1} b_1, \alpha^{n_2} b_2, \in A$ e $p|\alpha^{n_1+n_2} b_1 b_2$ in A, quindi $p|\alpha^{n_1} b_1$ in A oppure $p|\alpha^{n_2} b_2$ in A quindi $p|b_1$ oppure $p|b_2$ in B. Dunque p è primo in B.
Da quanto visto ogni elemento non nullo di B è prodotto di primi.

Quindi B è un dominio a fattorizzazione unica.

iv) Un $K[x]$-modulo M è un $K[x, x^{-1}]$-modulo se e solo se x è un endomorfismo invertibile di M. In particolare $(V, f) = (K, 1)$ e $(W, g) = (K, 0)$ sono $K[x]$-moduli che soddisfano le condizioni richieste.

2)
i) $H \cong \mathcal{S}_3$ e ha cardinalità 6; K è generato da due elementi (distinti) di ordine due che commutano tra loro, quindi $K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ e ha ordine 4; H è un gruppo ciclico generato da un elemento di ordine 4 quindi ha cardinalità 4 ed è isomorfo a $\mathbb{Z}_4$.
ii) Tra gli elementi di K e gli elementi di C l'unico che fissa 4 è l'identità, cioè

$$H \cap K = \{id\} = H \cap C;$$

ne segue che

$$\#(HK) = \#(KH) = \#(H)\#(K) = 24 = \#G$$

e

$$\#(HC) = \#(CH) = \#(H)\#(C) = 24 = \#G,$$

quindi

$$HK = KH = HC = CH = G.$$

iii) H non è normale in G, quindi non è fattore diretto di G. K è normale in G quindi dalle proprietà viste nel punto ii) ($H \cap K = \{id\}$ e $HK = G$) segue che $G = K \ltimes H$.
Invece C non è normale in G quindi G non è prodotto semidiretto di H e C.
iv) $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong K \triangleleft G$ e $G/K \cong H \cong \mathcal{S}_3 \cong \mathbb{Z}_3 \ltimes \mathbb{Z}_2$. Dunque i fattori di composizione di G sono $\mathbb{Z}_2$ con molteplicità 3 e $\mathbb{Z}_3$ con molteplicità 1.

3)
i) f è irriducibile per il criterio di Eisenstein con $p = 5$.
ii) f ha esattamente tre radici reali e due complesse coniugate, quindi $G \cong \mathcal{S}_5$ e $[K : \mathbb{Q}] = 5! = 120$: infatti $f'(x) = 5x^4 - 15x^2$ ha uno zero doppio in 0 e due zeri semplici in $\pm\sqrt{3}$: quindi f è crescente fuori dall'intervallo $[-\sqrt{3}, \sqrt{3}]$ e decrescente dentro tale intervallo; d'altra parte $f(-\sqrt{3}) = 6\sqrt{3}+5 > 0$ e $f(\sqrt{3}) = -6\sqrt{3}+5 < 0$, quindi f ha esattamente 3 zeri reali.
iii) $Gal(K/\mathbb{Q}) \cong \mathcal{S}_5$ non è risolubile, quindi f non è risolubile per radicali su $\mathbb{Q}$.
iv) $\mathcal{S}_5$ ha un (unico) sottogruppo di indice 2: il gruppo $\mathcal{A}_5$; a questo corrisponde la sottoestensione $E = Fix(\mathcal{A}_5)$ di K, che ha grado 2 su $\mathbb{Q}$. Poiché $Gal(K/E) \cong \mathcal{A}_5$ che non è risolubile, f non è risolubile per radicali neanche su E.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Prova scritta del 20 febbraio 2019

Si risolvano i seguenti esercizi.

1) Si consideri l'anello $A = \mathbb{Z}[X,Y]/(2XY-1)$ e siano $\pi : \mathbb{Z}[X,Y] \to A$ la proiezione sul quoziente, $x = \pi(X)$, $y = \pi(Y)$.

i) Dimostrare che A è un dominio di integrità.

ii) A è un dominio a fattorizzazione unica? In caso affermativo trovare la fattorizzazione in irriducibili di $2x^2 - xy$.

iii) Dire se l'ideale $(3) \subseteq A$ sia primo e se sia massimale; A è un dominio a ideali principali?

iv) A è un dominio euclideo?

2) Si consideri il dominio a ideali principali $A = \mathbb{Z}\left[\frac{1}{6}\right] \subseteq \mathbb{Q}$.

i) Quali dei seguenti gruppi abeliani hanno una struttura di A-modulo?

$$\mathbb{Z}, \quad \mathbb{Z}_4, \quad \mathbb{Z}_5, \quad \mathbb{Z}_n \ (n \in \mathbb{Z}_+).$$

ii) Sia $d \in A \setminus \{0\}$; descrivere la struttura di gruppo abeliano dell'A-modulo $A/(d)$.

iii) Dire se i seguenti A-moduli siano tra loro isomorfi:

$$M_1 = A/(2) \oplus A/(50), \ M_2 = A/(100), \ M_3 = A/(25).$$

3) Per ogni gruppo Γ si denoti con $Z(\Gamma)$ il centro di Γ.
Sia G un gruppo. Tra le seguenti affermazioni si dimostrino quelle vere e si trovi un controesempio per quelle false:

i) $H \trianglelefteq K \trianglelefteq G \Rightarrow H \trianglelefteq G$.

ii) $K \trianglelefteq G, \varphi \in Aut(G) \Rightarrow \varphi(K) = K$.

iii) $\varphi \in Aut(G) \Rightarrow \varphi(Z(G)) = Z(G)$.

iv) $K \trianglelefteq G \Rightarrow Z(K) \trianglelefteq G$.

4) Siano $f(x) = x^5 - 20x + 10 \in \mathbb{Q}[x]$, K il campo di spezzamento di f su $\mathbb{Q}$, $G = Gal(K/\mathbb{Q})$ il gruppo di Galois di K su $\mathbb{Q}$.

i) Dire se f sia irriducibile.

ii) Determinare G e calcolare $[K : \mathbb{Q}]$.

iii) Sia $\alpha \in K$ tale che $f(\alpha) = 0$; determinare $Gal(K/\mathbb{Q}(\alpha))$.

iv) Dire se f sia risolubile per radicali su $\mathbb{Q}$ e/o su $\mathbb{Q}(\alpha)$.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Soluzioni della prova scritta del 20 febbraio 2019

1)
i) $\mathbb{Z}[X,Y] = \mathbb{Z}[X][Y]$ è un dominio a fattorizzazione unica (perché è un anello di polinomi a coefficienti in $\mathbb{Z}$, che è a fattorizzazione unica) e $2XY-1$ è irriducibile (quindi primo), perché è di grado 1 in Y e primitivo ($MCD(2X,1)=1$). Quindi l'ideale generato da $2XY-1$ è primo e il quoziente A è un dominio di integrità.
ii) $A \cong \mathbb{Z}\left[\frac{1}{2}\right][T,T^{-1}]$; infatti:
$2XY-1$ è nel nucleo dell'omomorfismo di anelli definito da

$$X \mapsto T,\ Y \mapsto \frac{T^{-1}}{2},$$

quindi è ben definito l'omomorfismo di anelli $F : A \to \mathbb{Z}\left[\frac{1}{2}\right][T,T^{-1}]$ tale che

$$x \mapsto T,\ y \mapsto \frac{T^{-1}}{2};$$

viceversa:
2 è invertibile in A ($2^{-1} = xy$), quindi esiste (unico) omomorfismo $\mathbb{Z}\left[\frac{1}{2}\right] \to A$;
x è invertibile in A ($x^{-1} = 2y$), quindi è ben definito l'omomorfismo

$$G : \mathbb{Z}\left[\frac{1}{2}\right][T,T^{-1}] \ni T \mapsto x \in A$$

(e si ha $\frac{1}{2} \mapsto xy$, $T^{-1} \mapsto 2y$);
d'altra parte F e G sono uno l'inverso dell'altro, quindi

$$A \cong \mathbb{Z}\left[\frac{1}{2}\right][T,T^{-1}].$$

$\mathbb{Z}\left[\frac{1}{2}\right]$ è a fattorizzazione unica (è euclideo), quindi $\mathbb{Z}\left[\frac{1}{2}\right][T]$ è a fattorizzazione unica.
T è invertibile in A e per ogni $f \in A$ esiste $n \in \mathbb{Z}$ tale che $T^n f \in \mathbb{Z}\left[\frac{1}{2}\right][T]$; in particolare per ogni $g \in \mathbb{Z}\left[\frac{1}{2}\right][T] \subseteq A$ la condizione $g|f$ in A equivale alla condizione $g|T^n f$ in $\mathbb{Z}\left[\frac{1}{2}\right][T]$.
Ne segue che:
tutti gli irriducibili (primi) di $\mathbb{Z}\left[\frac{1}{2}\right][T]$ tranne T sono primi in A;
e che:
in A ogni elemento non nullo si fattorizza come prodotto di primi (per una potenza di T, che è invertibile).
Dunque A è un dominio a fattorizzazione unica.
$2x^2 - xy = \frac{1}{2}(4T^2-1) = \frac{1}{2}(2T-1)(2T+1)$, dove $\frac{1}{2}$ è invertibile e $2T \pm 1$ è irriducibile.
iii) (3) è primo/massimale se e solo se $A/(3)$ è un dominio di integrità/campo. Ora

$$A/(3) \cong \mathbb{Z}[X,Y]/(3,2XY-1) \cong \mathbb{Z}_3[X,Y]/(XY+1) \cong \mathbb{Z}_3[X,X^{-1}]$$

che è un dominio di integrità e non è un campo.

Quindi (3) è primo e non è massimale. Si osservi che $(3) \neq (0)$ perché $A \ncong A/(3)$. In un dominio a ideali principali ogni ideale primo non nullo è massimale; quindi A non è un dominio a ideali principali.
iv) A non è euclideo perché non è a ideali principali.

2)
Un A-modulo è il dato di $(M, f : Z\left[\frac{1}{6}\right] \to End(M))$ dove M è un gruppo abeliano e f è un omomorfismo di anelli unitari, cioè M è un gruppo abeliano in cui il prodotto per 6 è invertibile.
Poiché in A gli elementi 2 e 3 sono invertibili, le classi di equivalenza a meno di invertibili (e quindi i divisori elementari di un A-modulo finitamente generato) sono definite a meno di prodotto per potenze di 2 e di 3.
i) Il prodotto per 6 è invertibile in $\mathbb{Z}_n$ se e solo se $(n, 6) = 1$.
Quindi $\mathbb{Z}_n$ ha una struttura di A-modulo se e solo se $(n, 6) = 1$; in particolare $\mathbb{Z}$ e $\mathbb{Z}_4$ non hanno una struttura di A-modulo, mentre $\mathbb{Z}_5$ è un A-modulo con $\frac{1}{6}. = id$.
ii) Esistono $n, m \in \mathbb{Z}_+$ tali che $\tilde{d} = 2^n 3^m d \in \mathbb{Z}$ è primo con 2 e con 3.
Si ha $A/(d) = A/(\tilde{d})$ perché $(d) = (\tilde{d})$.
Inoltre $A/(\tilde{d}) \cong \mathbb{Z}_{\tilde{d}}$: infatti banalmente l'omomorfismo $\mathbb{Z} \to A$ induce un omomorfismo $\mathbb{Z}_{\tilde{d}} \to A/(\tilde{d})$; viceversa la proiezione $\mathbb{Z} \to \mathbb{Z}_{\tilde{d}}$ si estende ad un omomorfismo $A \to \mathbb{Z}_{\tilde{d}}$ perché 6 è invertibile in $\mathbb{Z}_{\tilde{d}}$ (in quanto $(\tilde{d}, 6) = 1$). I due omomorfismi così costruiti sono l'uno l'inverso dell'altro.
Quindi $A/(d) \cong \mathbb{Z}_{\tilde{d}}$.
iii) $A/(2) \cong (0)$, $A/(50) \cong \mathbb{Z}_{25}$, $A/(100) \cong \mathbb{Z}_{25}$, $A/(25) \cong \mathbb{Z}_{25}$. Quindi

$$M_1 \cong M_2 \cong M_3 \cong \mathbb{Z}_{25}.$$

3)
i) è falsa: ad esempio se si scelgono

$$G = \mathcal{S}_4,\ K =< (12)(34), (13)(24) >,\ H =< (12)(34) >$$

si ha $H \trianglelefteq K \trianglelefteq G$ e $H \not\trianglelefteq G$ ($(13)(12)(34)(13)^{-1} = (14)(23) \notin H$).
ii) è falsa: ad esempio se si scelgono

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2,\ K =< (1, 0) >,\ \varphi(a, b) = (b, a)$$

si ha $K \trianglelefteq G$, $\varphi \in Aut(G)$ e $\varphi(K) =< (0, 1) > \neq K$.
iii) è vera.
Siano $z \in Z(G)$, $g \in G$; allora $g\varphi(z) = \varphi(\varphi^{-1}(g)z) = \varphi(z\varphi^{-1}(g)) = \varphi(z)g$, quindi $\varphi(z) \in Z(G)$ e $\varphi(Z(G)) \subseteq Z(G)$, $Z(G) \subseteq \varphi^{-1}(Z(G))$; poiché $\varphi^{-1} \in Aut(G)$ si ha anche $Z(G) \subseteq \varphi(Z(G))$.
Ne segue che $\varphi(Z(G)) = Z(G)$.
iv) è vera.
Per ogni $g \in G$ il coniugio c_g è un automorfismo di K, quindi $c_g(Z(K)) = Z(K)$, cioè $Z(K) \trianglelefteq G$.

4)
i) f è irriducibile per il criterio di Eisenstein con $p = 2$ (oppure con $p = 5$).
In particolare se α è una radice di f abbiamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$.

Ne segue che $G \leq \mathcal{S}_5$ contiene un 5-ciclo.
ii) f ha esattamente 3 radici reali; ciò segue dalle due seguenti osservazioni:
$f : \mathbb{R} \to \mathbb{R}$ è crescente su $(-\infty, -\sqrt{2}) \cup (\sqrt{2}, \infty)$ e decrescente su $(-\sqrt{2}, \sqrt{2})$;
inoltre $f(-3) < 0$, $f(-\sqrt{2}) > 0$, $f(\sqrt{2}) < 0$, $f(2) > 0$.
La coniugazione $\mathbb{C} \ni a + ib \mapsto a - ib \in \mathbb{C}$ (che fissa f quindi permuta le radici di f; si osservi che $K \subseteq \mathbb{C}$) fissa le tre radici reali e scambia le due radici non reali di f.
Ne segue che $G \leq \mathcal{S}_5$ contiene una trasposizione (un 2-ciclo).
Ora un sottogruppo di $\mathcal{S}_5$ che contiene una trasposizione e un 5-ciclo è tutto $\mathcal{S}_5$.
Quindi $G \cong \mathcal{S}_5$ e $[K : \mathbb{Q}] = \#G = 120$.
iii) $Gal(K/\mathbb{Q}(\alpha)) = \{\sigma \in G | \sigma(\alpha) = \alpha\} \cong \{\sigma \in \mathcal{S}_{\{\text{radici di } f\}} | \sigma(\alpha) = \alpha\}$, quindi $Gal(K/\mathbb{Q}(\alpha)) \cong \mathcal{S}_4$.
iv) $Gal(K/\mathbb{Q}) \cong \mathcal{S}_5$ non è risolubile, quindi f non è risolubile per radicali su $\mathbb{Q}$.
$Gal(K/\mathbb{Q}(\alpha)) \cong \mathcal{S}_4$ è risolubile, quindi f è risolubile per radicali su $\mathbb{Q}(\alpha)$; o anche, senza usare la struttura di $Gal(K/\mathbb{Q}(\alpha))$: K è il campo di spezzamento di $\frac{f(x)}{x-\alpha}$ (che ha grado 4) su $\mathbb{Q}(\alpha)$, quindi è un'estensione risolubile per radicali su $\mathbb{Q}(\alpha)$.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Prova scritta del 30 gennaio 2019

Si risolvano i seguenti esercizi.

1) Sia $v : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ la funzione definita nel modo seguente:

$$v(m) = n \Leftrightarrow 2^n \leq |m| < 2^{n+1}$$

e siano $a, b, q, r \in \mathbb{Z}$ elementi tali che

$$(*) \qquad a = bq + r.$$

i) Dimostrare che v è una valutazione euclidea.
ii) Se $a = 2$ e $b = 3$ determinare q, r tali che $(*)$ sia una divisione euclidea in $(\mathbb{Z}, v)$.
iii) Dimostrare che se $(*)$ è una divisione euclidea in $(\mathbb{Z}, v)$ allora $(*)$ è una divisione euclidea anche in $(\mathbb{Z}, |\cdot|)$ e mostrare con un esempio che il viceversa è falso.

2) Sia A un dominio di integrità.
Per ogni A-modulo M si denoti con $T(M)$ l'insieme degli elementi di torsione di M e con $\pi_M : M \to M/T(M)$ la proiezione sul quoziente.
Sia $f : M \to N$ un omomorfismo di A-moduli. Dimostrare che:
i) esiste un unico omomorfismo $\tilde{f} : M/T(M) \to N/T(N)$ tale che $\tilde{f} \circ \pi_M = \pi_N \circ f$;
ii) se f è iniettivo allora $\tilde{f}$ è iniettivo;
iii) l'implicazione "$\tilde{f}$ iniettivo $\Rightarrow$ f iniettivo" è falsa.

3) Siano p un numero primo, G un gruppo <u>non abeliano</u> di ordine p^3, $Z = Z(G)$ il centro di G, G' il sottogruppo dei commutatori di G.
i) Calcolare la cardinalità e descrivere la struttura di Z e G/Z; determinare G'.
ii) Dimostrare che se $K \leq G$ è tale che $\#K = p^2$ allora $Z \leq K \trianglelefteq G$.
iii) Dimostrare che per ogni $x \in G \setminus Z$ il sottogruppo $< Z, x > \leq G$ è abeliano e ha ordine p^2.
iv) Dimostrare che G è prodotto semidiretto di due suoi sottogruppi non banali se e solo se esiste $x \in G \setminus Z$ tale che $x^p = e$.

4) Siano $f(x) = x^4 + 10x^2 + 20 \in \mathbb{Q}[x]$, K il campo di spezzamento di f su $\mathbb{Q}$, $G = Gal(K/\mathbb{Q})$ il gruppo di Galois di K su $\mathbb{Q}$.
i) Dire se f sia irriducibile.
ii) Risolvere f per radicali.
iii) Calcolare $[K : \mathbb{Q}]$ e determinare G.
iv) Trovare tutte le sottoestensioni di K.

Algebra 2 - a.a. 2018/2019 (Ilaria Damiani)
Soluzioni della prova scritta del 30 gennaio 2019

1)
i) Siano $a, b \in \mathbb{Z} \setminus \{0\}$. Si ha

$$v(a) = n \Rightarrow |a| \geq 2^n \Rightarrow |ab| \geq |a| \geq 2^n \Rightarrow v(ab) \geq n = v(a).$$

Siano $a, b \in \mathbb{Z}$ con $b \neq 0$ e siano $q, r \in \mathbb{Z}$ tali che $a = bq + r$ e $|r| \leq \frac{|b|}{2}$. Allora

$$v(b) = n \Rightarrow |b| < 2^{n+1} \Rightarrow |r| \leq \frac{|b|}{2} < \frac{2^{n+1}}{2} = 2^n \Rightarrow v(r) < n = v(b).$$

ii) $2 = 3 \cdot 1 - 1$: infatti $2^0 \leq 1 < 2^1 \leq 3 < 2^2$ quindi $v(-1) = 1 < 2 = v(3)$.
iii) Abbiamo che $b \neq 0$ e $r = 0$ oppure $v(r) < v(b)$; se $v(r) < v(b)$ abbiamo

$$|r| < 2^{v(r)+1} \leq 2^{v(b)} \leq |b|.$$

Controesempio per il viceversa: $2 = 3 \cdot 0 + 2$, $|2| < |3|$ ma $v(2) = 1 = v(3)$.

2)
i) sia $m \in T(M)$; se $a \in A \setminus \{0\}$ è tale che $am = 0$ si ha

$$af(m) = f(am) = 0 \text{ quindi } f(m) \in T(N),$$

cioè $f(T(M)) \subseteq T(N)$ e $(\pi_N \circ f)(T(M)) = \{0\}$.
La tesi segue dal teorema di omomorfismo/proprietà universale del quoziente.
ii) Sia $m \in M$ tale che $\pi_M(m) \in ker(\tilde{f})$. Allora

$$\pi_N \circ f(m) = \tilde{f} \circ \pi_M(m) = 0$$

quindi $f(m) \in T(N)$ e $\exists a \in A \setminus \{0\}$ tale che $f(am) = af(m) = 0$; ne segue che

$$am \in ker(f) = \{0\},$$

da cui

$$m \in T(M)$$

cioè

$$\pi_M(m) = 0.$$

Dunque $ker(\tilde{f}) = \{0\}$ e $\tilde{f}$ è iniettiva.
iii) Esempio: $A = \mathbb{Z}$, $M = \mathbb{Z}_m$ con $m > 1$, $N = \{0\}$, $f : M \to N$ omomorfismo nullo. f non è iniettivo perché $M \neq \{0\}$; $T(M) = M$ quindi $M/T(M) = \{0\}$ e $\tilde{f} : \{0\} \to \{0\}$ è iniettiva.

3)
i) G p-gruppo $\Rightarrow p|\#Z$ quindi $\#(G/Z)|p^2$; G non abeliano $\Rightarrow G/Z$ non ciclico, quindi $\#(G/Z) \not| p$.
Dunque $\#(G/Z) = p^2$, $\#Z = p$ e $Z \cong \mathbb{Z}_p$.
I gruppi di ordine p^2 sono abeliani e G/Z non è ciclico, quindi $G/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

G/Z abeliano $\Rightarrow G' \leq Z$; ma $G' \neq \{e\}$ perché G è risolubile (ogni p-gruppo lo è, e comunque $\{e\} \trianglelefteq Z \trianglelefteq G$ è una successione di sottogruppi normali con quozienti abeliani) quindi $G' = Z$.
ii) Z e K sono abeliani e Z è centrale, quindi $< Z, K >$ è abeliano;
$\#K = p^2$ e $\#G = p^3$, quindi l'unico sottogruppo di G che contiene strettamente K è G;
poiché G non è abeliano si deve avere $< Z, K >= K$, cioè $Z \leq K$.
G/Z è abeliano, quindi tutti i sottogruppi di G/Z sono normali in G/Z, quindi tutti i sottogruppi di G che contengono Z sono normali in G; ne segue che $K \trianglelefteq G$.
iii) Z è il centro di G, quindi commuta con x, quindi $< Z, x >$ è abeliano, quindi non è tutto G, quindi $\# < Z, x > | p^2$.
$x \notin Z$ quindi $< Z, x >$ contiene strettamente Z, quindi $p^2 | \# < Z, x >$.
Ne segue che $\# < Z, x >= p^2$.
iv) Se G è prodotto semidiretto di due suoi sottogruppi non banali in particolare esistono $H, K \leq G$ tali che $H \cap K = \{e\}$, $\#H = p$, $\#K = p^2$; quindi $Z \leq K$ e H contiene un elemento di ordine p che non appartiene a Z.
Viceversa sia $x \in G \setminus Z$ tale che $x^p = e$ e sia $y \in G \setminus < Z, x >$ (y esiste perché $\# < Z, x >= p^2$, e si ha anche $\# < Z, y >= p^2$). Abbiamo:
$< Z, y > \trianglelefteq G$ per il punto ii);
$G =< Z, x, y >$ perché $< Z, x, y >$ contiene strettamente $< Z, x >$, che ha cardinalità p^2;
$x \notin < Z, y >$ perché $< Z, y > \neq G =< Z, x, y >$, quindi $< Z, y > \cap < x >= \{e\}$.
Dunque G è prodotto semidiretto di $< Z, y >$ e $< x >$.

4)
i) f è irriducibile per il criterio di Eisenstein con $p = 5$.
In particolare se α è una radice di f abbiamo $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
ii) se α è una radice di f abbiamo che α^2 è radice di $x^2+10x+20$, cioè $\alpha^2 = -5 \pm \sqrt{5}$.
In particolare $\mathbb{Q} \subseteq \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\alpha)$ e $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 2$.
Quindi le quattro radici di f sono $\pm\alpha$ e $\pm\beta$ con $\alpha^2 = -5 + \sqrt{5}$ e $\beta^2 = -5 - \sqrt{5}$:

$$\pm\alpha = \sqrt{-5 + \sqrt{5}}, \quad \pm\beta = \sqrt{-5 - \sqrt{5}}.$$

In particolare $K = \mathbb{Q}(\alpha, \beta)$.
iii) $\alpha^2\beta^2 = 20$, quindi $\alpha\beta = \pm 2\sqrt{5} \in \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$. In particolare $\beta = \frac{\alpha\beta}{\alpha} \in \mathbb{Q}(\alpha)$ e $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.
Ne segue che $K = \mathbb{Q}(\alpha)$ e $[K : \mathbb{Q}] = 4 = \#G$.
Sia $\sigma \in G$ tale che $\sigma(\alpha) = \beta$; allora $\sigma(\alpha^2) = \beta^2$, quindi $\sigma(\sqrt{5}) = -\sqrt{5}$, da cui

$$\alpha\beta = -\sigma(\alpha\beta) = -\sigma(\alpha)\sigma(\beta) = -\beta\sigma^2(\alpha);$$

dunque $\sigma^2(\alpha) = -\alpha \neq \alpha$ e $\sigma^2 \neq id$.
Ne segue che $G =< \sigma > \cong \mathbb{Z}_4$.
iv) $\mathbb{Z}_4$, quindi G, ha un unico sottogruppo non banale, quindi K ha un'unica sottoestensione non banale. Le sottoestensioni di K sono quindi quelle già trovate:

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\alpha) = K.$$