COMPITINO DI ALGEBRA 1

16 dicembre 2020

Esercizio 1.
Sia

$$A = \frac{\mathbb{Z}[i][x]}{(7, (x^2+1)(x-1)(x+6))}.$$

Determinare la cardinalità di A, il numero degli elementi invertibili di A, e il numero dei nilpotenti in A.

Soluzione.
Ricordiamo che dati I, J ideali di un anello R con $I \subset J$ si ha $R/J \cong (R/I)/(J/I)$. Applichiamo ora questo isomorfismo all'anello $\mathbb{Z}[i][x]$ e ai suoi ideali $I = 7\,\mathbb{Z}[i][x]$ e $J = (7, f(x))$, dove $f(x) = (x^2+1)(x-1)(x+6)$: ricordando che

$$\frac{\mathbb{Z}[i][x]}{7\,\mathbb{Z}[i][x]} \cong \frac{\mathbb{Z}[i]}{(7)}[x] \cong \mathbb{F}_{7^2}[x],$$

otteniamo

$$A = \frac{\mathbb{Z}[i][x]}{(7, f(x))} \cong \frac{\mathbb{F}_{7^2}[x]}{(\bar{f}(x))}$$

dove $\bar{f}(x)$ denota la classe di $f(x)$ modulo 7. Ne segue in particolare che A è un $\mathbb{F}_{7^2}$-spazio vettoriale di dimensione $4 = \deg \bar{f}(x)$, e dunque $|A| = 49^4 = 7^8$.
Osserviamo ora che $\bar{f}(x) = (x-\alpha)(x+\alpha)(x-\bar{1})^2$ dove $\alpha \in \mathbb{F}_{7^2}$ è tale che $\alpha^2 = -1$. Dal teorema cinese abbiamo

$$\frac{\mathbb{F}_{7^2}[x]}{(\bar{f}(x))} \cong \frac{\mathbb{F}_{7^2}[x]}{(x-\alpha)} \times \frac{\mathbb{F}_{7^2}[x]}{(x+\alpha)} \times \frac{\mathbb{F}_{7^2}[x]}{((x-\bar{1})^2)} \cong \mathbb{F}_{7^2} \times \mathbb{F}_{7^2} \times \frac{\mathbb{F}_{7^2}[x]}{((x-\bar{1})^2)}.$$

A questo punto è semplice contare gli elementi invertibili e i nilpotenti: infatti una terna (a, b, c) è invertibile se e solo se a, b, c sono invertibili ed è nilpotente se e solo se lo sono a, b, c. Nel nostro caso gli elementi invertibili sono quindi quelli con $a, b \in \mathbb{F}_{7^2}^*$ e $c = c(x) = c_0 + c_1 x$ coprimo con $x-1$, cioè $c(1) = c_0 + c_1 \neq 0$. Gli elementi invertibili di A sono quindi $48 \times 48 \times 49 \times 48$.
Le terne (a, b, c) nilpotenti sono quelle con $a = b = 0$ e $c = k(x-1)$ per un certo $k \in \mathbb{F}_{7^2}$. I nilpotenti dell'anello A sono quindi 49.

Esercizio 2.
Sia K il campo di spezzamento di $x^6 - 2$ su $\mathbb{Q}$ e sia $L = \mathbb{Q}(\zeta_{16})$.

1. Elencare le sotto-estensioni quadratiche di K.

2. Calcolare il grado $[K \cap L : \mathbb{Q}]$.

SOLUZIONE. Il polinomio $x^6 - 2$ è irriducibile in $\mathbb{Q}[x]$ per i lemmi di Eisenstein e Gauss, quindi $\mathbb{Q}(\sqrt[6]{2})$ ha grado 6 su $\mathbb{Q}$. Il campo di spezzamento di $x^6 - 2$ è $K = \mathbb{Q}(\sqrt[6]{2} \cdot \zeta_6^i : i = 0, \dots, 5) = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$. Inoltre si ha $\zeta_6 = \frac{1+\sqrt{-3}}{2}$, da cui $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$. Siccome $\sqrt{-3}$ non sta in $\mathbb{Q}(\sqrt[6]{2})$ (che è contenuto in $\mathbb{R}$) ed ha grado al più 2 su questo campo, otteniamo $[\mathbb{Q}(\sqrt[6]{2}, \zeta_6) : \mathbb{Q}(\sqrt[6]{2})] = [K : \mathbb{Q}(\sqrt[6]{2})] = 2$, e quindi $[K : \mathbb{Q}] = 12$.

1. Il campo K contiene sia $\sqrt{2} = \sqrt[6]{2}^3$, sia $\sqrt{-3}$, e quindi contiene le 3 estensioni quadratiche $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-6})$. Sia $F = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Il campo F è il composto di $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{-3})$, che sono due estensioni normali di $\mathbb{Q}$ (in quanto hanno grado 2) con intersezione $\mathbb{Q}$. Ne segue che $F/\mathbb{Q}$ è Galois con gruppo $(\mathbb{Z}/2\mathbb{Z})^2$ e quindi, per corrispondenza di Galois, che F ammette esattamente tre sotto-estensioni quadratiche (tante quante i sottogruppi di indice 2 in $(\mathbb{Z}/2\mathbb{Z})^2$), ovvero quelle già trovate. Se K contenesse un'ulteriore sotto-estensione quadratica $\mathbb{Q}(\sqrt{d})$ non contenuta in F, allora si avrebbe $F \cap \mathbb{Q}(\sqrt{d}) = \mathbb{Q}$, e quindi $F(\sqrt{d})/\mathbb{Q}$ sarebbe di Galois con gruppo $\mathrm{Gal}(F/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$, e quindi avrebbe grado 8. Questo è assurdo, perché $F(\sqrt{d})$ è contenuto in K (siccome F e $\sqrt{d}$ lo sono), e $8 = [F(\sqrt{d}) : \mathbb{Q}]$ non divide $12 = [K : \mathbb{Q}]$.

2. Dimostreremo che $K \cap L = \mathbb{Q}(\sqrt{2})$. Da un lato, $\sqrt{2} = \zeta_{16}^2 + \zeta_{16}^{-2} = \sqrt[6]{2}^3$ è sia in L che in K. Dall'altro, osserviamo innanzitutto che $K \cap L$ è contenuto sia in L che in K, e quindi per moltiplicatività nella torri il grado $[K \cap L : \mathbb{Q}]$ divide sia $[K : \mathbb{Q}] = 12$ che $[L : \mathbb{Q}] = \varphi(16) = 8$, ovvero divide 4. Vogliamo escludere che si abbia $[K \cap L : \mathbb{Q}] = 4$. Osserviamo che F è l'*unica* sotto-estensione di K di grado 4: infatti essa corisponde, per teoria di Galois, a un sottogruppo di $\mathrm{Gal}(K/\mathbb{Q})$ di cardinalità $3 = [K : \mathbb{Q}]/[F : \mathbb{Q}]$, e cioè ad un 3-Sylow di $\mathrm{Gal}(K/\mathbb{Q})$. Siccome $F/\mathbb{Q}$ è normale, come già osservato, questo 3-Sylow è un sottogruppo normale, e quindi (per i teoremi di Sylow) è l'unico sottogruppo di $\mathrm{Gal}(K/\mathbb{Q})$ di cardinalità 3. Per corrispondenza di Galois, questo implica che F sia l'unica sotto-estensione di grado 4 di K. Pertanto, se per assurdo si avesse $[K \cap L : \mathbb{Q}] = 4$, allora dovrebbe valere $K \cap L = F$. Per trovare la contraddizione mostriamo ora che $\sqrt{-3}$ appartiene ad F (come già visto) ma non ad L. In effetti, L contiene esattamente tre sotto-estensioni quadratiche, ovvero $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})$: che queste siano contenute in L è chiaro ($i = \zeta_{16}^4$, e come già osservato $\sqrt{2} \in L$). Inoltre, le sotto-estensioni quadratiche corrispondono ai sottogruppi di indice 2 di $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/16\mathbb{Z})^\times$, che sono in bigezione con i sottogruppi di indice 2 del quoziente di $(\mathbb{Z}/16\mathbb{Z})^\times$ modulo il sottogruppo $Q = \langle 9 \rangle$ dei quadrati. Il quoziente $(\mathbb{Z}/16\mathbb{Z})^\times/Q$ ha 4 elementi, e quindi al massimo 3 sottogruppi

di indice 2. Ci sono perciò al massimo 3 sotto-estensioni quadratiche, che sono quelle già trovate. Siccome $\mathbb{Q}(\sqrt{-3})$ non è fra queste, abbiamo raggiunto l'assurdo voluto.

Seconda soluzione. Cominciamo osservando che il polinomio $x^6 - 2$ è irriducibile in $\mathbb{Q}[x]$ (per i lemmi di Eisenstein e Gauss). L'estensione $\mathbb{Q}(\sqrt[6]{2})$ ha quindi grado 6 su $\mathbb{Q}$. Il campo di spezzamento di questo polinomio è $K = \mathbb{Q}(\sqrt[6]{2} \cdot \zeta_6^i : i = 0, \dots, 5) = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$. Inoltre si ha $\zeta_6 = \frac{1+\sqrt{-3}}{2}$, da cui $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$. Il campo K è il composto di $\mathbb{Q}(\sqrt[6]{2})$ e di $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$. Siccome $\sqrt{-3}$ non sta in $\mathbb{Q}(\sqrt[6]{2}) \subset \mathbb{R}$ ed ha grado al più 2 su questo campo, otteniamo $[K : \mathbb{Q}(\sqrt[6]{2})] = 2$, e quindi $[K : \mathbb{Q}] = 12$. Sappiamo inoltre che $K/\mathbb{Q}$ è di Galois, in quanto K è un campo di spezzamento.
Il gruppo di Galois G di K su $\mathbb{Q}$ ha quindi ordine $12 = [K : \mathbb{Q}]$. Ogni elemento σ di G è determinato da $\sigma(\sqrt[6]{2})$, che deve essere una radice del polinomio $x^6 - 2$ e quindi della forma $\sqrt[6]{2} \cdot \zeta_6^i$ per un certo $i \in \{0, \dots, 5\}$, e da $\sigma(\zeta_6)$, che dev'essere una radice del polinomio minimo di ζ_6 su $\mathbb{Q}$ (che come noto è $x^2 - x + 1$), ovvero $\sigma(\zeta_6) = \zeta_6^{\pm 1}$. Il gruppo di Galois ha quindi al più 12 elementi (sei scelte per i, due scelte per il segno $\pm$), e siccome sappiamo che in effetti ne ha esattamente 12, tutti gli automorfismi così descritti sono elementi del gruppo di Galois. Ne segue in particolare che G contiene

$$r : \begin{cases} \sqrt[6]{2} \mapsto \sqrt[6]{2} \cdot \zeta_6 \\ \zeta_6 \mapsto \zeta_6 \end{cases} \qquad \text{e} \qquad s : \begin{cases} \sqrt[6]{2} \mapsto \sqrt[6]{2} \\ \zeta_6 \mapsto \zeta_6^{-1} \end{cases}$$

Controllando l'azione sui generatori è immediato verificare che si ha $r^6 = s^2 = \mathrm{Id}$ e $rs = sr^{-1}$. Otteniamo allora che il sottogruppo di G generato da r ed s è isomorfo al gruppo diedrale su 6 elementi, che ha ordine 12: si ha dunque $G = \langle r, s \rangle \cong D_6$.

1. Per teoria di Galois, le sotto-estensioni quadratiche di K corrispondono ai sotto-gruppi di $G \cong D_6$ di indice 2. Ogni tale sottogruppo contiene il sottogruppo Q di D_6 generato dai quadrati: dato che $(sr^i)^2 = \mathrm{Id}$ per ogni i, mentre $(r^i)^2 = r^{2i}$, abbiamo $Q = \langle r^2 \rangle$, che ha ordine $3 = \mathrm{ord}_G(r^2)$. Il quoziente D_6/Q è quindi un gruppo con 4 elementi, che non può essere $\mathbb{Z}/4\mathbb{Z}$ perché D_6 non contiene elementi di ordine 4 (e quindi lo stesso vale per i suoi quozienti). I sottogruppi di indice 2 in D_6 sono quindi in corrispondenza con i sottogruppi di indice 2 in $(\mathbb{Z}/2\mathbb{Z})^2$, che sono 3. È poi immediato trovare tre sotto-estensioni quadratiche di K: in effetti $\sqrt{2} = \sqrt[6]{2}^3$ è in K, e abbiamo già osservato che $\sqrt{-3}$ è in K. Ne segue che anche $\sqrt{-6}$ è in K, e abbiamo così identificato tre sotto-estensioni quadratiche, ovvero $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-6})$, che per quanto già dimostrato sono tutte. Si noti in particolare che il campo fissato da $\langle r^2 \rangle$ in K è $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$: infatti il campo $K^{\langle r^2 \rangle}$ ha grado $12/3 = 4$ su $\mathbb{Q}$, e per definizione r^2 fissa sia $\sqrt{2}$ che $\sqrt{-3}$, dunque $K^{\langle r^2 \rangle}$ contiene $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$, che ha a sua volta grado 4 su $\mathbb{Q}$.

2. Il grado $[L \cap K : \mathbb{Q}]$ è un divisore sia di $[K : \mathbb{Q}] = 12$ che di $[L : \mathbb{Q}] = \varphi(16) = 8$, quindi è un divisore di 4. Dato che $\sqrt{2} = \zeta_{16}^2 + \zeta_{16}^{-2}$ è in L, l'intersezione $L \cap K$ contiene $\mathbb{Q}(\sqrt{2})$, e quindi ha grado almeno 2 su $\mathbb{Q}$. Dimostriamo che in effetti $[L \cap K : \mathbb{Q}] = 2$. Supponiamo per assurdo $[L \cap K : \mathbb{Q}] = 4$, e sia H il sottogruppo di $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/16\mathbb{Z})^\times$ corrispondente a $L \cap K$. Siccome $\mathrm{Gal}(L/\mathbb{Q})$ è abeliano, H è un sottogruppo normale, e quindi per teoria di Galois l'estensione $K \cap L$ di $\mathbb{Q}$ è normale, con gruppo di Galois isomorfo a $(\mathbb{Z}/16\mathbb{Z})^\times/H$ e quindi abeliano. Sia N il sottogruppo di G corrispondente a $K \cap L$ (vista come sotto-estensione di K): allora $|N| = [K : L \cap K] = \frac{[K:\mathbb{Q}]}{[K \cap L:\mathbb{Q}]} = 3$, e quindi $N = \langle r^2 \rangle$ (perché questo è l'unico sottogruppo di ordine 3 di D_6). Ne segue che $K \cap L$ dovrebbe essere $K^{\langle r^2 \rangle} = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$, e questa dovrebbe essere una sotto-estensione di $\mathbb{Q}(\zeta_{16})$. Questo è assurdo: le sotto-estensioni quadratiche di $\mathbb{Q}(\zeta_{16})$ sono in bigezione con i sottogruppi di $(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ di indice 2, a loro volta in bigezione con i sottogruppi di indice 2 del quoziente $\frac{\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}{2\mathbb{Z}/4\mathbb{Z} \times 2\mathbb{Z}/2\mathbb{Z}} \cong (\mathbb{Z}/2\mathbb{Z})^2$, e quindi sono esattamente 3. Se avessimo $\mathbb{Q}(\sqrt{2}, \sqrt{-3}) \subseteq \mathbb{Q}(\zeta_{16})$, quest'ultimo campo conterrebbe almeno 4 sotto-estensioni quadratiche $(\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-3}))$, contraddizione.

Esercizio 3.
Sia L/K un'estensione normale finita, sia $f(x) \in K[x]$ un polinomio irriducibile di grado $n \geq 2$ e siano $\alpha_1, \ldots, \alpha_n$ le sue radici (tutte distinte) in una chiusura algebrica di L.

1. Mostrare con un esempio che $L(\alpha_i)$ e $L(\alpha_j)$ non sono necessariamente isomorfi su L.

2. Mostrare che per ogni i e j i campi $L(\alpha_i)$ e $L(\alpha_j)$ sono isomorfi su K.

3. Dimostrare che in $L[x]$ il polinomio $f(x)$ si spezza in d fattori di grado n/d per un certo $d \geq 1$.

Soluzione.

1. Siano $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ e $f(x) = x^4 - 2$. Chiaramente L/K è normale in quanto campo di spezzamento di $x^2 - 2$. Il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein, mentre in $L[x]$ si ha $f(x) = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$. I due fattori di secondo grado sono irriducibili in $L[x]$ in quanto le radici α_i $(i = 1, 2, 3, 4)$ di $f(x)$ hanno grado 4 su $\mathbb{Q}$ e quindi su L hanno grado almeno 2 dato che

$$4 = [\mathbb{Q}(\alpha_i) : \mathbb{Q}] \leq [L(\alpha_i) : \mathbb{Q}] = [L(\alpha_i) : L][L : \mathbb{Q}] = [L(\alpha_1) : L] \cdot 2.$$

Questo mostra che $[L(\alpha_i) : L] = 2$ per ogni i, di conseguenza ci sono esattamente due immersioni di $L(\alpha_1)$ in $\bar{L}$ che sono l'identità su L, e queste necessariamente

permutano le radici del polinomio minimo di α_1 su L. Più precisamente, se α_1 e α_2 sono le radici di $x^2 - \sqrt{2}$ e α_3, α_4 quelle di di $x^2 + \sqrt{2}$, le immersioni di $L(\alpha_1)$ su L sono definite da $\alpha_1 \to \alpha_1$ e $\alpha_1 \to \alpha_2$. Ne segue che $L(\alpha_1)$ e $L(\alpha_3)$ non sono isomorfi su L.

2. $[K(\alpha_1) : K] = n$, quindi ci sono esattamente n immersioni

$$\varphi_i \colon K(\alpha_1) \to \bar{L},\ \varphi_{i|K} = \mathrm{id},$$

e sono definite da $\alpha_1 \to \alpha_i$ per $i = 1, \ldots, n$. Si ha quindi $\varphi_i(K(\alpha_1)) = K(\alpha_i)$.

Per ogni i indichiamo con $\tilde{\varphi}_i$ un'estensione di φ_i a $L(\alpha_1)$ (dalla teoria sappiamo che ne esistono esattamente $[L(\alpha_1) : K(\alpha_1)]$). Poiché L è un'estensione normale di K, per ogni i vale $\tilde{\varphi}_i(L) = L$, e

$$\tilde{\varphi}_i(L(\alpha_1)) = \tilde{\varphi}_i(L)(\varphi(\alpha_1)) = L(\alpha_i).$$

Infine, per la transitività della relazione di isomorfismo si ha che per ogni i e j i campi $L(\alpha_i)$ e $L(\alpha_j)$ sono isomorfi su K.

3. Sia $f(x) = \mu_1(x) \ldots \mu_d(x)$ la fattorizzazione di $f(x)$ in $L[x]$ (notiamo che i fattori irriducibili $\mu_i(x)$ sono e due a due distinti dato che $f(x)$ ha radici distinte in $\bar{L}$). Per dimostrare la tesi basta far vedere che i polinomi $\mu_i(x)$ hanno tutti lo stesso grado, che sarà necessariamente n/d.

Siano α_i una radice di μ_i e α_j una radice di μ_j. Usando la formula del grado nelle torri di estensioni e quella per il grado di un'estensione semplice otteniamo

$$[L(\alpha_i) : K] = [L(\alpha_i) : L][L : K] = \deg(\mu_i)[L : K]$$

e analogamente

$$[L(\alpha_j) : K] = [L(\alpha_j) : L][L : K] = \deg(\mu_j)[L : K.]$$

D'altra parte dal punto (2) sappiamo che $L(\alpha_i)$ e $L(\alpha_j)$ sono isomorfi su K, quindi $[L(\alpha_i) : K] = [L(\alpha_j) : K]$, per cui dalle formule precedenti otteniamo $\deg(\mu_i) = \deg(\mu_j)$ come volevamo.