SOLUZIONI DEL 2^o COMPITINO DI ALGEBRA 1

8 gennaio 2018

Esercizio 1. Consideriamo l'anello degli interi di Gauss $A = \mathbb{Z}[i]$ e indichiamo con N la usuale norma definita da $N(a + ib) = a^2 + b^2$.

1. Dimostrare che dato l'ideale $I = (a + ib)$ si ha $|A/I| = N(a + ib)$.

2. Dire quanti sono gli ideali I di A di indice 100.

Soluzione:

1. Sia $n = N(a + ib) = a^2 + b^2$.

   Supponiamo inizialmente che a, b siano coprimi su $\mathbb{Z}$. Vogliamo esibire un omomorfismo tra A/I e $\mathbb{Z}/n\mathbb{Z}$. Poiché a, b sono coprimi, sono entrambi invertibili in $\mathbb{Z}/n\mathbb{Z}$. In particolare sia c un intero tale che $bc \equiv 1 \mod n$, definiamo $\phi : A \to \mathbb{Z}/n\mathbb{Z}$ come

   $$\phi : x + iy \mapsto x - acy.$$

   Poiché $a^2 + b^2 \equiv 0 \mod n$ si ha che $(-ac)^2 \equiv -1 \mod n$ è dunque ϕ è un omomorfismo. Ovviamente ϕ è suriettivo. Inoltre $\phi(a + ib) = 0$. Affermiamo che $\ker \phi = I$ e dunque $A/I \simeq \mathbb{Z}/n\mathbb{Z}$. Infatti se $\phi(x + iy) = 0$ allora si ha che $x - acy = hn$ per un qualche intero h e dunque

   $$\begin{aligned} x + iy &= iy + acy + hn = \\ &= icby + acy + h'n = \\ &= (cy + h' + a - ib)(a + ib) \end{aligned}$$

   per un altro intero h' e quindi $x + iy \in I$.

   Se invece a e b non fossero coprimi su $\mathbb{Z}$, detto m il loro MCD, abbiamo che $a = a'm, b = b'm$ con a' e b' coprimi. L'indice di I in $I' = (a' + ib')$ è $m^2 = N(m)$ e vale $[A : I] = [A : I'][I' : I] = N(a' + ib')m^2 = N(a + ib)$.

2. L'anello A è principale, quindi ogni ideale I di A è della forma $I = (a + ib)$ per opportuni interi a e b. Cerchiamo dunque gli ideali generati da $a+ib$, con $N(a+ib) = 100 = 2^2 5^2$. La norma di un intero di Gauss è il prodotto delle norme dei suoi fattori primi. Un primo q degli interi di Gauss può avere norma 2 (se $q = 1 + i$, a meno di invertibili) o norma p, con p un primo di $\mathbb{Z}$ dispari e congruo a 1 modulo 4, oppure norma p^2, con p un primo di $\mathbb{Z}$ dispari, congruo a 3 modulo 4. In particolare a meno di invertibili $1 + i$ è l'unico primo con norma 2 e $2 \pm i$ sono gli unici due primi con norma 5. Ne segue che i possibili ideali che hanno indice 100 in A sono: $((1 + i)^2(2 + i)^2), ((1 + i)^2(2 - i)^2), ((1 + i)^2 5)$. Questi tre ideali sono distinti perché sono generati da prodotti distinti di primi e A è un UFD.

Esercizio 2. Consideriamo il sottoanello A di $\mathbb{Q}(x)$ definito da

$$A = \{f(x)/g(x) \mid f, g \in \mathbb{Q}[x],\ g(x) \text{ non ha radici in } \mathbb{Q}\}.$$

1. Determinare A^*;
2. mostrare che A è PID;
3. mostrare che A ha infiniti ideali primi.

Soluzione:

1. Gli invertibili di A sono i rapporti $f(x)/g(x)$ dove $f(x)$ e $g(x)$ non hanno radici in $\mathbb{Q}$. Infatti è chiaro che gli elementi di questo tipo hanno un'inverso. D'altra parte fissato un polinomio $g(x)$ che non si annulla su $\mathbb{Q}$ e fissato un altro polinomio $f(x)$, se $f(x)$ si annulla per un certo $q \in \mathbb{Q}$ allora tutti i numeratori dei rapporti $f'(x)/g'(x) \in (f(x)/g(x))$ si annullano in q e quindi $f(x)/g(x)$ non è invertibile.

2. Ovviamente A è un dominio essendo un sottoanello del campo $\mathbb{Q}(x)$. Sia I un ideale di A e sia $\{f_j(x)/g_j(x)\}_{j \in J}$ un insieme (eventualmente anche infinito) di generatori di I. I polinomi $\{f_j(x)\}_{j \in J}$ generano un ideale $\overline{I}$ di $\mathbb{Q}[x]$ e poiché $\mathbb{Q}[x]$ è principale abbiamo che esiste un polinomio $\overline{f}(x) \in \mathbb{Q}[x]$ tale che $\overline{I} = (\overline{f}(x))$. Quindi per ogni $j \in J$ esiste un polinomio $h_j(x) \in \mathbb{Q}[x]$ tale che $f_j(x) = \overline{f}(x)h_j(x)$. Inoltre $\overline{f}(x) = \sum_{j \in J} k_j(x)f_j(x)$ per opportuni $k_j(x) \in \mathbb{Q}[x]$ tutti nulli tranne un numero finito. Dato che per ogni j si ha che $f_j(x)/1 \in I$, ne segue che anche $\overline{f}(x)/1 \in I$. Inoltre $f_j(x)/g_j(x) = \overline{f}(x)h_j(x)/g_j(x)$ e dunque $I = (\overline{f}(x)/1)$ e perció I è un ideale principale.

3. Per quanto detto al punto **??**, per ogni $q \in \mathbb{Q}$ il rapporto $f(x)/1 = (x-q)/1$ genera un ideale proprio I_q.

   Tale ideale è primo. Infatti se $f(x)/g(x) \cdot h(x)/k(x) \in I_q$ allora $f(x)h(x)$ si annulla in q e dunque uno dei due fattori si annulla in q, ovvero uno tra $f(x)/g(x)$ e $h(x)/k(x)$ appartiene a I_q.

   Inoltre due tali ideali $I_q, I_{q'}$ per $q \neq q'$ sono distinti. Infatti $I_q + I_{q'} \ni ((x-q)/1 - (x-q')/1) = ((q-q')/1) = A$, cioè la somma non è un ideale proprio. Vi sono quindi infiniti ideli primi distinti.

Esercizio 3. Sia K il campo di spezzamento di $x^3 - 5$ su $\mathbb{Q}$ e sia F il campo di spezzamento di $x^{11} - 1$ su $\mathbb{Q}$.

1. Determinare il gruppo di Galois di $K/\mathbb{Q}$ e un elemento primitivo per tale estensione.
2. Calcolare il grado e il gruppo di Galois di $KF/\mathbb{Q}$.
3. Contare le sottoestensioni L di KF, tali che $\sqrt[3]{5} \in L$ e $L/\mathbb{Q}$ è di Galois.

Soluzione:

1. Indichiamo con ζ_n una radice n-esima primitiva dell'unità contenuta in $\mathbb{C}$, allora le radici del polinomio $x^3 - 5$ sono gli elementi $\zeta_3^i \sqrt[3]{5}$ per $i = 0, 1, 2$ e il suo campo di spezzamento è $K = \mathbb{Q}(\{\zeta^i \sqrt[3]{5}\}_{i=0,1,2}) = \mathbb{Q}(\sqrt[3]{5}, \zeta_3)$.

   La formula delle torri ci dà $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$. Ora $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ perchè $x^3 - 5$ è irriducibile; inoltre $[K : \mathbb{Q}(\sqrt[3]{5})] = 2$ perchè ζ_3 ha grado 2 su $\mathbb{Q}$ e non appartiene a $\mathbb{Q}(\sqrt[3]{5})$ che è un campo reale. Si ottiene quindi che $[K : \mathbb{Q}] = 6$ e di conseguenza il suo gruppo di Galois è isomorfo a S_3.

   Ci sono molti modi per verificare che un elemento α di K genera $K/\mathbb{Q}$: in questo caso possiamo mostrare che $\alpha = \zeta_3 + \sqrt[3]{5}$ genera l'estensione, facendo vedere che l'orbita di α sotto l'azione del gruppo di Galois ha 6 elementi, questo ci permetterà di concludere che il suo grado è 6 e quindi genera l'estensione.

   Gli elementi del gruppo di Galois di $K/\mathbb{Q}$ permutano le radici di $x^3 - 5$ e possono essere descritti come $\{\sigma_{i,j}\}_{i=0,1,2}^{j=1,2}$ dove $\sigma_{ij}(\sqrt[3]{5}) = \zeta_3^i \sqrt[3]{5}$, e $\sigma_{ij}(\zeta_3) = \zeta_3^j$. Si ha quindi

   $$\sigma_{ij}(\alpha) = \sigma_{hk}(\alpha) \iff \zeta_3^i \sqrt[3]{5} + \zeta_3^j = \zeta_3^h \sqrt[3]{5} + \zeta_3^k \iff (\zeta_3^i - \zeta_3^h)\sqrt[3]{5} = (\zeta_3^k - \zeta_3^j).$$

   Necessariamente si ottiene $i = h$ perché altrimenti si avrebbe $\sqrt[3]{5} \in \mathbb{Q}(\zeta_3)$ (che è chiaramente impossibile) e da questo segue anche $j = k$: l'orbita di α ha quindi 6 elementi come volevamo.

2. $F = \mathbb{Q}(\zeta_{11})$. Osserviamo che $\mathbb{Q}(\zeta_{11}, \zeta_3) = \mathbb{Q}(\zeta_{33})$ dato che 11 e 3 sono coprimi: infatti il contenimento $\subseteq$ è evidente, inoltre se $a, b \in \mathbb{Z}$ sono tali che $11a + 3b = 1$ allora $\zeta_{33} = \zeta_{11}^b \zeta_3^a$. Da questo segue che $KF = \mathbb{Q}(\zeta_{11}, \zeta_3, \sqrt[3]{5}) = \mathbb{Q}(\zeta_{33}, \sqrt[3]{5})$.

   Ora $[\mathbb{Q}(\zeta_{33}) : \mathbb{Q}] = \phi(33) = 20$ e $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ sono coprimi, quindi $[KF : \mathbb{Q}] = 60$.

   Dalla teoria sappiamo che $\mathrm{Gal}(KF/\mathbb{Q})$ si immerge in $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(F/\mathbb{Q})$ ma i due gruppi hanno la stessa cardinalità, quindi

   $$\mathrm{Gal}(KF/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(F/\mathbb{Q}) \cong S_3 \times (\mathbb{Z}/11\mathbb{Z})^*.$$

3. Una estensione normale L di $\mathbb{Q}$ che contiene $\sqrt[3]{5}$, necessariamente contiene il campo di spezzamento K di $x^3 - 5$. Il campo K è fissato da un sottogruppo del gruppo di Galois isomorfo a $(\mathbb{Z}/11\mathbb{Z})^*$, quindi, per il teorema di corrispondenza di Galois, le estensioni L che stiamo cercando sono tante quanti i sottogruppi di $(\mathbb{Z}/11\mathbb{Z})^*$; tale gruppo è ciclico di ordine 10, quindi ha esattamente 4 sottogruppi e le estensioni cercate sono 4. Osserviamo che tali sottogruppi sono tutti normali nel gruppo di Galois G di $KF/\mathbb{Q}$ in quanto $(\mathbb{Z}/11\mathbb{Z})^*$ è abeliano e $\{id\} \times (\mathbb{Z}/11\mathbb{Z})^*$ è caratteristico in G.