Lezione 23

Prerequisiti: Lezione 22.

Norme di elementi ed ideali.

Sia F un campo, sia K una sua estensione di grado finito n. Sia $\alpha \in K$. Consideriamo l'applicazione

$$\begin{aligned} \mu_\alpha : K &\to K \\ x &\mapsto \alpha x \end{aligned}$$

Questa è un omomorfismo di F-spazi vettoriali. Sia M_α la matrice (scritta per righe) associata a μ_α rispetto ad una base di K su F fissata. Allora, come noto, $\det M_\alpha$ non dipende dalla scelta della base. Lo denoteremo $\det \mu_\alpha$.

Definizione 23.1 Si dice *norma* di α (in K, su F) il seguente elemento di F:

$$N_{K/F}(\alpha) = \det \mu_\alpha .$$

Scriveremo semplicemente $N(\alpha)$ quando il riferimento ai campi F e K è sottinteso.

Osservazione 23.2 Per ogni $\alpha \in F$, la matrice associata a μ_α rispetto ad una qualsiasi base di K è αI_n, essendo I_n la matrice identità di ordine n. Quindi $N(\alpha) = \alpha^n$. Ciò prova che, in generale, la norma dipende non solo dal campo F, ma anche dalla scelta dell'estensione K.

Esempio 23.3
a) Sia $F = \mathbf{R}$, $K = \mathbf{C}$. Una base di $\mathbf{C}$ su $\mathbf{R}$ è formata da $1, i$. Sia $\alpha = a + bi$, con $a, b \in \mathbf{R}$. Allora si ha

$$\mu_\alpha(1) = a + bi, \qquad \mu_\alpha(i) = -b + ai,$$

quindi la matrice associata a μ_α rispetto alla base scelta (scritta per righe) è

$$M_\alpha = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Segue che $N(a+bi) = \det M_\alpha = a^2 + b^2$, che è l'usuale norma del numero complesso $a + ib$, intesa come quadrato del modulo, che nasce come lunghezza nel piano di Gauss.

b) Sia $F = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{m})$, ove m è un intero diverso da 0, 1 e privo di quadrati. Una base di $\mathbf{Q}(\sqrt{m})$ su $\mathbf{Q}$ è formata da $1, \sqrt{m}$. Sia $\alpha = a + b\sqrt{m}$, con $a, b \in \mathbf{Q}$. Allora si ha

$$\mu_\alpha(1) = a + b\sqrt{m}, \qquad \mu_\alpha(\sqrt{m}) = bm + a\sqrt{m},$$

quindi la matrice associata a μ_α rispetto alla base scelta (scritta per righe) è

$$M_\alpha = \begin{pmatrix} a & b \\ bm & a \end{pmatrix}.$$

Segue che $N(a+b\sqrt{m}) = \det M_\alpha = a^2 - b^2 m$. Si osservi che si ottiene la stessa norma per $F = \mathbf{R}$, $K = \mathbf{R}(\sqrt{m})$, quando m è un intero negativo: essa generalizza quella dell'Esempio a), che corrisponde a $m = -1$.

c) Sia $F = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt[3]{2})$. Una base di $\mathbf{Q}(\sqrt[3]{2})$ su $\mathbf{Q}$ è formata da $1, \sqrt[3]{2}, \sqrt[3]{4}$. Sia $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, con $a, b, c \in \mathbf{Q}$. Allora si ha

$$\mu_\alpha(1) = a + b\sqrt[3]{2} + c\sqrt[3]{4}, \qquad \mu_\alpha(\sqrt[3]{2}) = 2c + a\sqrt[3]{2} + b\sqrt[3]{4}, \qquad \mu_\alpha(\sqrt[3]{4}) = 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4},$$

quindi la matrice associata a μ_α rispetto alla base scelta (scritta per righe) è

$$M_\alpha = \begin{pmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{pmatrix}.$$

Segue che $N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$.

La nozione generalizzata di norma che abbiamo appena introdotto gode anch'essa della proprietà moltiplicativa:

Proposizione 23.4 Per ogni $\alpha, \beta \in K$, $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha) N_{K/F}(\beta)$.

<u>Dimostrazione:</u> Si ha che $\mu_{\alpha\beta} = \mu_\alpha \circ \mu_\beta$, per cui $\det \mu_{\alpha\beta} = \det(\mu_\alpha \circ \mu_\beta) = \det \mu_\alpha \det \mu_\beta$. □

Introduciamo ora due nuove nozioni, legate alla norma da criteri di algebra lineare. Ricordiamo che non dipendono dalla scelta della base di K su F la traccia di M_α (ossia la somma degli elementi sulla diagonale principale), e il polinomio caratteristico di M_α. Li potremo quindi indicare rispettivamente con $\mathrm{tr}\mu_\alpha$, $\mathrm{char}\mu_\alpha$.

Definizione 23.5 Si dice *traccia* di α (in K, su F) il seguente elemento di F:

$$T_{K/F}(\alpha) = \mathrm{tr}\mu_\alpha,$$

e si dice *caratteristica* di α (in K, su F) il seguente elemento di $F[x]$:

$$\mathrm{char}_{K/F}(\alpha) = \mathrm{char}\mu_\alpha.$$

Ometteremo l'indice K/F quando ciò non crei ambiguità.

Osservazione 23.6 Per ogni $\alpha \in F$ si ha che $T(\alpha) = n\alpha$, $\mathrm{char}(\alpha) = (x-\alpha)^n$.

Con facili argomenti di algebra lineare si dimostra:

Proposizione 23.7 Per ogni $\alpha \in K$

$$\mathrm{char}_{K/F}(\alpha) = x^n - T_{K/F}(\alpha)x^{n-1} + \cdots + (-1)^n N_{K/F}(\alpha).$$

Mostriamo ora come norma, traccia e caratteristica si possano determinare sulla base del polinomio minimo.

Proposizione 23.8 Sia $f(x)$ il polinomio minimo di α su F, sia $m = [K : F(\alpha)]$. Allora

$$\mathrm{char}_{K/F}(\alpha) = f(x)^m.$$

<u>Dimostrazione:</u> Supponiamo dapprima che $m = 1$. Allora $K = F(\alpha)$. Per il Teorema di Cayley-Hamilton, μ_α annulla $\mathrm{char}_{K/F}(\alpha)$, da cui segue facilmente che α è radice di $\mathrm{char}_{K/F}(\alpha)$. Quindi $f(x)$ divide $\mathrm{char}_{K/F}(\alpha)$. Poiché entrambi i polinomi sono monici di grado *n*, segue che $f(x) = \mathrm{char}_{K/F}(\alpha)$, come volevasi.
Consideriamo ora il caso generale, in cui *m* è un qualunque intero positivo. Allora, in base a quello che abbiamo appena provato, $f(x)$ è il polinomio caratteristico della restrizione di μ_α a $F(\alpha)$. Sia *p* il grado di $f(x)$. Sia $\beta_1,....,\beta_p$ una base di $F(\alpha)$ su *F*, e sia $\gamma_1,....,\gamma_m$ una base di *K* su $F(\alpha)$. Allora gli elementi $\beta_1\gamma_1,...,\beta_p\gamma_1,\beta_1\gamma_2,....,\beta_p\gamma_2,....,\beta_1\gamma_m,...,\beta_p\gamma_m$ formano una base di *K* su *F*. Sia $B = (b_{ij})$ la matrice associata a $\mu_{\alpha|F(\alpha)}$ rispetto alla base $\beta_1,....,\beta_p$.
Allora, per ogni $i = 1,..., p$,

$$\alpha\beta_i = \sum_{k=1}^{p} b_{ik}\beta_k ,$$

così che, per ogni $j = 1,...,m$

$$\alpha\beta_i\gamma_j = \sum_{k=1}^{p} b_{ik}\beta_k\gamma_j .$$

Quindi, rispetto alla base scelta in *K*, la matrice associata a μ_α è la seguente matrice "a blocchi":

$$M_\alpha = \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B \end{pmatrix}.$$

Pertanto $\mathrm{char}_{K/F}(\alpha) = \det(xI_p - B)^m = f(x)^m$. □

Dalle Proposizioni 23.7 e 23.8 segue subito

Corollario 23.9 Sia $[F(\alpha):F]=p$, e sia $f(x)$ il polinomio minimo di α su *F*. Siano $\alpha_1,...,\alpha_p$ le radici di $f(x)$ in un suo campo di spezzamento su *F*. Allora

$$N_{K/F}(\alpha)=\left(\prod_{i=1}^{p}\alpha_i\right)^{\frac{n}{p}},\qquad T_{K/F}(\alpha)=\frac{n}{p}\left(\sum_{i=1}^{p}\alpha_i\right),\qquad \mathrm{char}_{K/F}(\alpha)=\left(\prod_{i=1}^{p}(x-\alpha_i)\right)^{\frac{n}{p}},$$

ossia, in base alle formule di Viète (Proposizione 7.11) la norma di α su *F* è pari a $(-1)^p$ per il termine noto di $f(x)$ elevato alla $\frac{n}{p}$, la traccia di α su *F* è pari a $-\frac{n}{p}$ per il termine di x^{p-1} in $f(x)$, la caratteristica di α su *F* è $f(x)^{\frac{n}{p}}$.
(Ricordiamo che p divide n come conseguenza del Teorema di moltiplicazione dei gradi per le estensioni successive, il quoziente $\frac{n}{p}$ è pari al grado di *K* su $F(\alpha)$).

Osservazione 23.10 Se $f(x)$ è un polinomio separabile, allora possiamo sostituire ad $\alpha=\alpha_1,...,\alpha_p$ gli elementi $\sigma_1(\alpha),...,\sigma_p(\alpha)$, essendo $\sigma_1,...,\sigma_p$ le immersioni di $F(\alpha)$ in un'estensione algebricamente chiusa di *F* (vedi Proposizione 6.4). Quindi $N_{F(\alpha)/F}(\alpha)=\prod_{i=1}^{p}\sigma_i(\alpha)$. In altri termini, la norma di α è il prodotto delle sue radici coniugate. Ciò generalizza una ben nota proprietà della norma dei numeri complessi. In realtà, l'identità resta valida se a $F(\alpha)$ si sostituisce *K* e si considerano le immersioni $\sigma_1,...,\sigma_n$ di *K* in un'estensione algebricamente chiusa di *F*. Per una dimostrazione si veda [A2], Proposition 7.3.6.

Esempio 23.11 Sia m un intero diverso da 0,1 e avente un fattore primo di molteplicità 1. Calcoliamo la norma di $\sqrt[n]{m}$ in $\mathbf{Q}(\sqrt[n]{m})$ su $\mathbf{Q}$. Il polinomio minimo di $\sqrt[n]{m}$ su $\mathbf{Q}$ è $f(x)=x^n-m$ (irriducibile per Eisenstein). Quindi, in base al Corollario 23.9, (applicato per $p = n$), $N(\sqrt[n]{m})=(-1)^{n+1}m$. In particolare, $N(\sqrt{2})=-2$, in pieno accordo con l'Esempio 23.3 b).

Estendiamo ora la nozione di norma agli ideali dell'anello degli interi D_K di un campo numerico *K*. Secondo il Corollario 20.13, ogni ideale di D_K (ivi compreso D_K stesso) è un gruppo abeliano libero di rango *n*, essendo $n=[K:\mathbf{Q}]$. Quindi dal Teorema 17.19 segue che $(D_K:I)$ è finito.

Definizione 23.12 Si dice *norma* dell'ideale non nullo I di D_K il numero naturale

$$N(I)=(D_K:I).$$

Si pone, inoltre, per convenzione, $N((0))=0$.

Proviamo ora che questa definizione è una naturale estensione di quella data per gli elementi.

Proposizione 23.13 Sia $\alpha\in D_K, \alpha\neq 0$. Allora

$$N((\alpha))=\left|N_{K/\mathbf{Q}}(\alpha)\right|.$$

In particolare, $N_{K/\mathbf{Q}}(\alpha)$ è un numero intero.

Dimostrazione: Siano $\omega_1,...,\omega_n$ gli elementi di una base di D_K su **Z**. Poiché questi elementi sono linearmente indipendenti su **Z**, sono tali anche su **Q**; quindi essi formano una base di K su **Q**. Inoltre $\alpha\omega_1,...,\alpha\omega_n$ è una base di (α) su **Z**. Ora, in base al Teorema 17.19, esiste una matrice T a coefficienti interi tale che

$$\begin{pmatrix} \alpha\omega_1 \\ \vdots \\ \alpha\omega_n \end{pmatrix} = T \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix},$$

e $N((\alpha)) = |\det T|$. Ma, evidentemente, T è la matrice (scritta per righe) associata a μ_α rispetto alla base $\omega_1,...,\omega_n$ di K. Ciò basta per concludere. □

Dalle Proposizioni 23.4 e 23.13 si deduce

Corollario 23.14 La norma di ideali principali gode della proprietà moltiplicativa.

Gli elementi invertibili di D_K possono essere caratterizzati in termini di norma:

Corollario 23.15 Siano $\alpha, \beta \in D_K$. Se α divide β, allora $N(\alpha)$ divide $N(\beta)$. Inoltre α è invertibile se e solo se $|N(\alpha)| = 1$.

Dimostrazione: La prima parte dell'enunciato segue dalla Proposizione 23.4. In particolare, se α è invertibile, cioè è un divisore di 1, allora $|N(\alpha)| = 1$. Viceversa, se $|N(\alpha)| = 1$, allora, in base alla Proposizione 23.13 e alla Definizione 23.12, $(\alpha) = D_K$, e quindi α è invertibile. □

Esempio 23.16

a) Sia $a + bi \in \mathbf{Z}[i]$, con $a, b \in \mathbf{Z}$. Allora, in base all'Esempio 23.3 b), $N(a+bi) = a^2 + b^2$. Quindi, in base al Corollario 23.15, gli elementi invertibili in $\mathbf{Z}[i]$ sono $1, -1, i, -i$. Ciò era già stato stabilito, per altra via, nell'Esempio 16.11 c) di Algebra 2. Allora la proprietà era stata derivata dal Corollario 16.10, valido (solo) per i domini euclidei. Il Corollario 23.15 può essere considerato una generalizzazione di quest'ultimo.
b) In maniera analoga si prova che gli unici elementi invertibili di $\mathbf{Z}[i\sqrt{5}]$ sono 1 e -1.

La moltiplicatività della norma, in realtà, vale per tutti gli ideali di D_K. La dimostrazione del relativo teorema, che qui omettiamo, utilizza esplicitamente la fattorizzazione di ideali e la nozione di ideali coprimi.

Teorema 23.17 Siano I,J ideali di D_K. Allora $N(IJ) = N(I)N(J)$.

Dimostrazione: [A], Theorem 4.2.7.

Se ne deduce un criterio sufficiente di primalità per ideali:

Corollario 23.18 Sia I un ideale non nullo di D_K. Allora, se $N(I)$ è primo, anche I è primo.

Corollario 23.19 Siano I,J ideali non nulli di D_K tali che $I \subset J$. Allora $N(J)$ divide $N(I)$ e si ha $I = J$ se e solo se $N(I) = N(J)$.

Dimostrazione: Per ipotesi J divide I, (vedi Osservazione 22.19), ossia esiste un ideale L tale che $LJ = I$ e quindi la prima parte dell'enunciato segue dal Teorema 23.17, in base al quale $N(I) = N(L)N(J)$. Se $N(I) = N(J)$, allora $N(L) = 1$, quindi $L = D_K$, per cui $I = J$. □

Dal Corollario 23.19 e dalla Proposizione 23.13 segue

Corollario 23.20 Se $\alpha \in I$, ove I è un ideale non nullo di D_K, allora $N(I)$ divide $N(\alpha)$.

Quest'ultima proprietà è utile per calcolare la norma di un ideale.

Esempio 23.21 Calcoliamo le norme degli ideali primi $P_1 = (2, 1 + i\sqrt{5})$, $P_3 = (3, 1 + i\sqrt{5})$, $P_4 = (3, 1 - i\sqrt{5})$ di $D_{\mathbf{Q}(i\sqrt{5})} = \mathbf{Z}[i\sqrt{5}]$. In base a quanto stabilito nell'Esempio 22.7, si ha $P_1^2 = (2)$. Quindi, per il Teorema 23.17,

$$N(P_1)^2 = N(P_1^2) = N((2)) = \left|N_{\mathbf{Q}(i\sqrt{5})/\mathbf{Q}}(2)\right| = 2^2 = 4,$$

dove la penultima uguaglianza segue dall'Esempio 23.3 b), o anche dall'Osservazione 23.2. Dunque $N(P_1) = 2$.
Per calcolare $N(P_3)$, consideriamo che $3 \in P_3$, quindi, in virtù del Corollario 23.20, $N(P_3)$ divide $N(3) = 9$. Ma $N(P_3) \neq 1$ (perché $P_3 \neq \mathbf{Z}[i\sqrt{5}]$) e $N(P_3) \neq 9$, (perché $P_3 \neq (3)$). Quindi $N(P_3) = 3$.
Allo stesso modo si prova che $N(P_4) = 3$.

Dal fatto che $N(P_1) = 2$ segue che P_1 non è un ideale principale. Infatti, se fosse $P_1 = (\alpha)$ per qualche $\alpha \in D_K$, allora si avrebbe $N(P_1) = N((\alpha)) = |N(\alpha)|$, quindi $N(\alpha) = 2$ oppure $N(\alpha) = -2$. Ma, se $\alpha = a + i\sqrt{5}b$, con $a, b \in \mathbf{Z}$, allora, in base all'Esempio 23.3 b), $N(\alpha) = a^2 + 5b^2$, che è un intero positivo diverso da 2. Contraddizione.

Il nostro prossimo obiettivo è la determinazione delle norme degli ideali primi di D_K.

Lemma 23.22 Sia I un ideale di D_K. Allora $N(I) \in I$.

Dimostrazione: Sia $r = N(I) = (D_K : I) = |D_K / I|$. Allora, per ogni $\alpha \in D_K$, si ha $r(\alpha + I) = r\alpha + I = I$, lo zero di D_K / I, ossia $r\alpha \in I$. Ciò vale in particolare per $\alpha = 1$. □

Proposizione 23.23 Sia I un ideale primo non nullo di D_K. Allora esiste un unico numero primo p tale che $p \in I$.

Dimostrazione: Sia $N(I) = p_1^{n_1} \cdots p_r^{n_r}$ una decomposizione di $N(I)$ in fattori primi. Poiché il prodotto a secondo membro, per il Lemma 23.22, appartiene a *I*, che è un ideale primo, segue che $p_i \in I$ per qualche *i*. Se esistessero *p, q* primi distinti appartenenti a *I*, allora, per il Lemma di Bézout, si avrebbe che $1 \in I$, e quindi *I* non sarebbe un ideale proprio. Segue la tesi. □

Corollario 23.24 Se *I* è un ideale primo non nullo di D_K, allora $N(I) = p^m$, per qualche primo *p* e qualche intero positivo $m \leq [K : \mathbf{Q}]$.

Dimostrazione: Se $p \in I$, allora, in virtù del Corollario 23.20, $N(I)$ divide $N(p)$. Ma, in base all'Osservazione 23.2, $N(p) = p^{[K:\mathbf{Q}]}$. □

Utilizzando i risultati precedenti, è facile dare una caratterizzazione delle norme degli ideali primi degli anelli D_K, quando *K* è un campo quadratico.

Esempio 23.25 Sia $K = \mathbf{Q}(\sqrt{m})$, con *m* un intero privo di quadrati tale che $m \equiv 2$ o $m \equiv 3$ (mod 4). Sia *I* un ideale primo non nullo di D_K. In virtù del Corollario 23.24, se *p* è l'unico numero primo tale che $p \in I$, allora $N(I) = p$ oppure $N(I) = p^2$. Questo secondo caso equivale a $N(I) = N((p))$, ossia, essendo $(p) \subset I$, per il Corollario 23.19, si ha che $I = (p)$. In base alla Proposizione 22.8, ciò avviene se e solo se la congruenza quadratica $x^2 \equiv m$ (mod *p*) non ha soluzione.

Esercizio 23.26 Sia *P* un ideale primo di D_K. Provare che esiste solo un numero finito di ideali primi *Q* di D_K tali che $N(P) = N(Q)$.

Svolgimento: Se $P = (0)$, allora *P* è l'unico ideale di D_K avente norma nulla. Sia allora $P \neq (0)$, così che $N(P)$ è un numero intero maggiore di 1 (per il Corollario 23.24, è infatti una potenza positiva di un primo). Se *Q* è un ideale primo di D_K tale che $N(P) = N(Q)$, allora, in base al Lemma 23.22, $N(P) \in Q$, ossia $(N(P)) \subset Q$, equivalentemente, *Q* divide $(N(P))$. Ma ogni ideale proprio non nullo di D_K possiede solo un numero finito di divisori primi. Ciò basta per concludere.