UMBERTO ZANNIER

Corso di Teoria dei Numeri

Anno Accademico 1996/97

Note raccolte da Maurizio Candilera

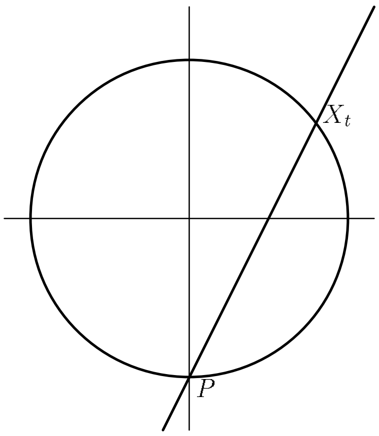
Dipartimento di Matematica Pura e Applicata - Via Belzoni, 7 - 35100 PADOVA

I
Interi algebrici

1. Esempi introduttivi

In questa sezione vogliamo dare alcuni esempi di risoluzione con metodi elementari di alcuni problemi diofantei .

1.1 Problema 1. Cominciamo occupandoci del classico problema di costruzione dei numeri pitagorici, ovvero di determinare le soluzioni intere dell'equazione $x^2 + y^2 = z^2$.



Si verifica direttamente che ciò è equivalente a determinare le soluzioni razionali dell'equazione $x^2 + y^2 = 1$ e tale problema può essere facilmente risolto per 'via geometrica' osservando che la circonferenza è una curva razionale, ovvero le coordinate di tutti i suoi punti, eccetto un numero finito, possono essere espresse come valori di funzioni razionali in $\mathbb{Q}(t)$. Infatti, fissato il punto $P = (0, -1)$, vi è corrispondenza biunivoca tra i punti della circonferenza (ad eccezione di P) e le rette per P (ad eccezione della tangente al circolo) e tale corrispondenza associa alla retta $x = t(y + 1)$ il punto $X_t = \begin{pmatrix} \frac{2t}{1+t^2} \\ \frac{1-t^2}{1+t^2} \end{pmatrix}$.

Passando a coordinate omogenee e ritornando al problema iniziale, si ottiene che i numeri pitagorici sono tutti della forma

$$\begin{cases} x = 2ab \\ y = b^2 - a^2 \\ z = b^2 + a^2 \end{cases} \qquad \text{al variare di } (a, b) \in \mathbb{Z}^2. \tag{1.2}$$

Era possibile un approccio allo stesso problema un po' meno geometrico, ma basato su argomenti di fattorizzazione in $\mathbb{Z}$. Cerchiamo quindi soluzioni intere dell'equazione $x^2 + y^2 = z^2$ e soggette alla condizione $\mathrm{Mcd}(x, y, z) = 1$, che non è restrittiva, trattandosi di un'equazione omogenea. Se (x, y, z) è una tale soluzione, si osserva facilmente che x ed y non possono essere né entrambo pari, né entrambo dispari; infatti, nel primo caso si avrebbe che anche z dovrebbe essere pari, contro l'ipotesi $\mathrm{Mcd}(x, y, z) = 1$, mentre nel secondo caso, si avrebbe $x^2 + y^2 \equiv 2 \pmod 4$, contro l'ipotesi che questa somma sia un quadrato. Supponiamo allora che $x = 2x'$ sia pari e quindi che y e z siano dispari e scriviamo $x'^2 = \frac{z+y}{2}\,\frac{z-y}{2}$, ove si osserva che, essendo $\mathrm{Mcd}(x, y, z) = 1$, i due fattori sono coprimi e quindi ciascuno dei fattori deve essere un quadrato in $\mathbb{Z}$. Si ottiene quindi

$$\begin{cases} z - y = 2a^2 \\ z + y = 2b^2 \end{cases}$$

da cui si deducono facilmente le formule (I.1.2).

1.3 Problema 2. Ora vogliamo mostrare che non esistono soluzioni intere non-triviali (cioè con $xyz \neq 0$) dell'equazione $x^4 + y^4 = z^4$; più precisamente, faremo vedere che non esistono soluzioni intere non-triviali (cioè con $xyz \neq 0$) dell'equazione $x^4 + y^4 = z^2$, soggette alla condizione $\mathrm{Mcd}(x, y, z) = 1$.(*) Supponiamo che (x, y, z) sia una soluzione non-triviale di tale equazione. Da quanto visto per i numeri pitagorici, possiamo dedurre

$$\begin{cases} x^2 = 2ab \\ y^2 = b^2 - a^2 \end{cases}$$

ove a e b sono interi non nulli che non possono essere né entrambo pari, né entrambo dispari. Possiamo quindi scrivere

$$a = 2r, \quad x = 2x', \quad \begin{cases} x' = rb \\ y^2 = b^2 - 4r^2 \end{cases},$$

ove b ed r sono coprimi ed il loro prodotto è un quadrato. Se ne deduce

$$r = s^2, \quad b = c^2, \quad \text{e} \quad b^2 = y^2 + 4r^2,$$

e questa è ancora un'equazione pitagorica, per cui, da (I.1.2) si ottiene

$$\begin{cases} 2r = 2tu \\ y = t^2 - u^2 \\ b = t^2 + u^2 \end{cases},$$

ove t ed u sono ancora coprimi ed il loro prodotto è un quadrato, per cui si ha

$$t = v^2, \quad u = w^2, \quad \text{con} \quad c^2 = v^4 + w^4.$$

Dunque, se (x, y, z) è una soluzione non-triviale dell'equazione $x^4 + y^4 = z^2$, abbiamo costruito una soluzione non-triviale (v, w, c) della stessa equazione con $|c| < |z|$, essendo $z = a^2+b^2$ e $c^2 = b$. Utilizzando lo stesso procedimento con la nuova soluzione (v, w, c) ed alle soluzioni così costruite da quest'ultima, si otterrebbe una successione di numeri interi diversi da zero e di valore assoluto strettamente decrescente, che non può chiaramente esistere.

1.4 Problema 3. Vogliamo mostrare ora che le sole soluzioni intere dell'equazione $y^2 = x^3 - 2$ sono $\{(3, -5), (3, 5)\}$. Possiamo usare un approccio simile a quello usato nei casi precedenti, scrivendo

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

ed utilizzando degli argomenti di fattorizzazione unica nell'anello $\mathbb{Z}[\sqrt{-2}]$ che, come vedremo nel seguito, è un anello a fattorizzazione unica. Cominciamo osservando che gli unici elementi invertibili di $\mathbb{Z}[\sqrt{-2}]$ sono 1 e -1. Infatti, dall'uguaglianza $(a + b\sqrt{-2})(c + d\sqrt{-2}) = 1$, si ottengono le condizioni

$$\begin{cases} ad + bc = 0 \\ ac - 2bd = 1 \end{cases}.$$

Allora, $a \mid bc$ in base alla prima condizione ed $\mathrm{Mcd}(a, b) = 1$ per la seconda delle due; da ciò si deduce che $a \mid c$ ed allo stesso modo $d \mid ad$ ed $\mathrm{Mcd}(c, d) = 1$, da cui si deduce che $c \mid a$ e quindi $a = \pm c$. Ragionando analogamente, si vede che $b = \pm d$ e si verifica che deve aversi

$$\begin{cases} a = c \\ b = -d \\ a^2 + 2b^2 = 1 \end{cases}$$

(*) Si osservi che, ponendo $u = \frac{x}{y}$ e $v = \frac{z}{y^2}$, si vede che i punti cercati sono in corrispondenza biunivoca con i punti razionali della curva $v^2 = u^4 + 1$, che *non* è una curva razionale e quindi i ragionamenti geometrici fatti per i numeri pitagorici sono inapplicabili al caso presente.

e ciò può accadere solo se $a = \pm 1$ e $b = 0$. Con analoghe considerazioni, si può dimostrare che $\sqrt{-2}$ è irriducibile in $\mathbb{Z}[\sqrt{-2}]$. Lasciamo questo compito al lettore e torniamo all'equazione $x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$. Osserviamo che i due fattori a destra devono essere coprimi; infatti, se vi fosse un fattore irriducibile $\alpha \in \mathbb{Z}[\sqrt{-2}]$ in comune, ovvero

$$\begin{cases} y + \sqrt{-2} = \alpha q_1 \\ y - \sqrt{-2} = \alpha q_2 \end{cases},$$

prendendo la differenza tra le due uguaglianze, si ottiene che α deve dividere $\sqrt{-2}$, che è irriducibile. Quindi, sommando le due uguaglianze e ricordando che $y \in \mathbb{Z}$, si ottiene che $2 \mid y$, e quindi, ricordando che $x^3 = y^2 + 2$, si ottiene che x è pari e $x^3 \equiv 2 \pmod 4$, che è assurdo.

Dunque, se i due fattori sono coprimi ed il loro prodotto è un cubo, devono essere entrambo dei cubi e deve quindi aversi

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 \quad \text{e} \quad y - \sqrt{-2} = (c + d\sqrt{-2})^3, \quad \text{con } a, b, c, d \in \mathbb{Z}. \tag{1.5}$$

Considerando il coefficiente di $\sqrt{-2}$, dalla prima uguaglianza si ottiene la condizione $b(3a^2 - 2b^2) = 1$, che si ha solo se $a = \pm 1$ e $b = 1$ che applicate a (I.1.5), permettono di dedurre che gli unici valori possibili. per x ed y sono quelli indicati sopra.

1.6 Problema 4. Vogliamo concludere questo numero considerando il problema di Fermat nell'anello dei polinomi $\mathbb{C}[t]$. Trattandosi di un anello euclideo, e quindi a fattorizzazione unica, si potranno usare anche in questo caso degli argomenti di divisibilità. Precisamente, vogliamo mostrare il seguente

Teorema. *Sia n un intero maggiore di 2. Gli unici polinomi $X, Y, Z \in \mathbb{C}[t]$ soddisfacenti alle condizioni*

$$\begin{cases} X^n + Y^n = Z^n \\ XYZ \neq 0 \\ \mathrm{Mcd}(X, Y, Z) = 1 \end{cases}$$

sono costanti.

dim. Possiamo quindi scrivere

$$X^n = \prod_{\xi^n = 1} (Z - \xi Y),$$

ove i fattori di questo prodotto sono a due a due coprimi. Allora, ognuno dei fattori è una potenza n-esima in $\mathbb{C}[t]$ e quindi, al variare di ξ tra le radici n-esime di 1, si ha $Z - \xi Y = U_\xi^n$, per un opportuno $U_\xi \in \mathbb{C}[t]$. Prese quindi tre radici distinte ξ, η, ζ, si ottengono le relazioni

$$\begin{cases} Z - \xi Y - U_\xi^n = 0 \\ Z - \eta Y - U_\eta^n = 0 \\ Z - \zeta Y - U_\zeta^n = 0 \end{cases} \quad \text{e quindi} \quad \det \begin{pmatrix} 1 & -\xi & U_\xi^n \\ 1 & -\eta & U_\eta^n \\ 1 & -\zeta & U_\zeta^n \end{pmatrix} = 0,$$

e ciò produce una relazione lineare a coefficienti costanti tra U_ξ^n, U_η^n ed U_ζ^n. Poichè tutte le costanti in $\mathbb{C}$ sono potenze n-esime, esistono delle costanti a, b, c tali che i polinomi aU_ξ^n, bU_η^n e cU_ζ^n siano di nuovo soluzioni del problema posto nell'enunciato, con grado positivo e strettamente più piccolo del grado delle soluzioni di partenza, se queste avevano grado positivo. Iterando il procedimento, si ottiene un assurdo come nel caso del Problema 2. . **CVD** □

Questo conclude la discussione del problema di Fermat nell'anello dei polinomi e la serie di esempi introduttivi.

2. Richiami di Teoria di Galois.

In questa sezione, raccogliamo alcuni richiami di teoria dei corpi, al solo scopo di fissare le notazioni che saranno utilizzate nel seguito e senza alcuna pretesa di dare una trattazione dell'argomento.

Siano $K \subset L$ due corpi –che supporremo sempre commutativi– allora L è uno spazio vettoriale su K. In tal caso, diremo che L è un'*estensione* di K e chiameremo *grado* dell'estensione la dimensione del K-spazio vettoriale L. Scriveremo $[L : K]$ per indicare il grado dell'estensione.

Se $K \subset L$ e $K \subset L'$ sono due estensioni di K, un omomorfismo $\phi : L \to L'$ è un K-omomorfismo se induce l'identità sugli elementi di K; ovvero, indicate con $j : K \to L$ e $j' : K \to L'$ le inclusioni, se il diagramma

$$\begin{tikzcd} L \arrow[r, "\phi"] & L' \\ K \arrow[u, "j"] \arrow[ur, "j'"'] & \end{tikzcd}.$$

è commutativo.

Se $K \subset L \subset M$ sono estensioni di grado finito, vale l'uguaglianza

$$[M : K] = [M : L][L : K] \qquad [\textit{Regola dei gradi}], \tag{2.1}$$

che si può dimostrare osservando che se $\{l_1, \dots, l_r\}$ è una base di L su K ed $\{m_1, \dots, m_s\}$ è una base di M su L, allora $\{\, m_i l_j \,|\, 1 \le j \le r, \quad 1 \le i \le s \,\}$ è una base di M su K.

La regola dei gradi si può facilmente estendere al caso di estensioni di grado infinito.

Sia $K \subset L$ un'estensione, un elemento $y \in L$ si dice *algebrico* su K se esiste un polinomio $P(X) \in K[X]$, diverso da zero, tale che $P(y) = 0$; ovvero se gli elementi $1, y, y^2, \dots$ di L sono linearmente dipendenti su K. Un'estensione $K \subset L$ si dirà *algebrica* se ogni elemento di L è algebrico su K. Ad esempio, un'estensione di grado finito è necessariamente algebrica.

Un corpo Ω si dice *algebricamente chiuso* se ogni estensione algebrica di Ω coincide con Ω stesso. Una *chiusura algebrica* del corpo K è un'estensione algebrica $K \subset \Omega$, con Ω algebricamente chiuso.

Si dimostra che, per ogni corpo K, esiste una chiusura algebrica e che questa è unica, a meno di isomorfismo (cf. Bourbaki, Algèbre, Chap. V, §.4, n.2, Théorèmes 1 e 2).

Sia $K \subset L$ un'estensione, dato un elemento $y \in L$, algebrico su K, si chiama *polinomio minimo* di y su K il generatore monico dell'ideale $I_y = \{\, f(X) \in K[X] \,|\, f(y) = 0 \,\}$. Poichè I_y è il nucleo dell'omomorfismo di anelli $\varepsilon_y : K[X] \to L$, che manda $g(X) \mapsto g(y)$, ed L è un corpo, si ha che I_y è un ideale primo e quindi massimale in $K[X]$, che ogni generatore di I_y è un polinomio irriducibile in $K[X]$, che l'immagine di ε_y è un sottocorpo $K(y) \subset L$ e infine, che il grado del polinomio minimo di y è uguale a $[K(y) : K]$. In particolare, se L ha grado finito su K, dalla regola dei gradi, si deduce che il grado del polinomio minimo di $y \in L$ divide $[L : K]$.

Un elemento $y \in L$, algebrico su K, si dice *separabile* se il polinomio minimo di y su K è privo di radici multiple. Indicando con $f(X)$ il polinomio minimo di y su K, si ha che y è separabile se, e solo se, $f(X)$ ed il suo derivato $f'(X)$ non hanno radici comuni.

Un'estensione algebrica $K \subset L$ si dice *separabile* se ogni elemento di L è separabile su K. Si dimostra che, se K è un corpo perfetto(*) allora ogni estensione algebrica di K è separabile (cf. Bourbaki, Algèbre, Chap. V, §.7, n.3, Proposition 4).

Per le estensioni separabili, vale il seguente risultato (cf. Bourbaki, Algèbre, Chap. V, §.7, n.7, Proposition 12, ove è dimostrato per i corpi infiniti e §.11, n.4, ove il risultato si generalizza ai corpi finiti)

(*) Un corpo K è *perfetto* se, e solo se, K ha caratteristica 0, oppure $\mathit{char} K = p > 0$ e l'omomorfismo $x \mapsto x^p$ è un isomorfismo di K in sé. Si osservi che, se K è un corpo finito, dall'iniettività dell'omomorfismo $x \mapsto x^p$, discende che K è perfetto.

2.2 Proposizione. *(Teorema dell'elemento primitivo) Se L è un estensione finita e separabile di K, allora esiste un elemento $y \in L$ tale che $L = K(y)$; ogni tale y si dice un elemento primitivo per l'estensione L.*

Un altro risultato sulle estensioni separabili che utilizzeremo nel seguito è dato dalla seguente Proposizione (cf. Bourbaki, Algèbre, Chap. V, §.7, n.5, Proposition 8),

2.3 Proposizione. *Sia Ω un'estensione algebricamente chiusa del corpo K e sia E una sottoestensione di Ω, di grado finito su K. Il numero dei K-omomorfismi di E in Ω è al più uguale a $[E : K]$ e vale l'uguaglianza se, e solo se, E è separabile su K.*

Siano K, E ed Ω come nella *Proposizione I.2.3*, ed indichiamo con $\sigma_1, \dots, \sigma_r$ i K-omomorfismi (distinti) di E in Ω. Allora, dato un elemento $x \in E$, chiameremo *coniugati* di x gli elementi $\sigma_1(x), \dots, \sigma_r(x)$ di Ω[†]. Osserviamo che, poichè $\sigma_1, \dots, \sigma_r$ sono K-omomorfismi, i coniugati di $x \in E$ devono avere lo stesso polinomio minimo di x su K.

Vogliamo ricordare un risultato spesso utile sui caratteri di un gruppo G, ovvero sugli omomorfismi di G a valori nel gruppo moltiplicativo di un campo.

2.4 Proposizione. (Teorema di indipendenza dei caratteri) *Siano G un gruppo ed L un corpo. Se $\sigma_1, \dots, \sigma_n$ sono omomorfismi distinti da G sul gruppo moltiplicativo $L^\times$, allora $\sigma_1, \dots, \sigma_n$ sono linearmente indipendenti su L.*

dim. Se $\sigma_1, \dots, \sigma_n$ non fossero linearmente indipendenti su L, esisterebbe una relazione di dipendenza di lunghezza minima; ovvero, a meno di riordinare i caratteri, si ha che esistono delle costanti $z_1, \dots, z_m$ in L, tutte diverse da zero e con $m \geq 2$ e minimo rispetto alla condizione

$$(*) \qquad z_1\sigma_1(g) + \cdots + z_m\sigma_m(g) = 0, \qquad \text{per ogni } g \in G.$$

Poichè i caratteri sono distinti, sia $g_0 \in G$ tale che $\sigma_1(g_0) \neq \sigma_2(g_0)$. Fissato comunque $g \in G$, consideriamo la relazione $(*)$, sia applicata al prodotto gg_0 che applicata a g e moltiplicata per $\sigma_1(g_0)$. Facendo la differenza tra le due si ottiene la relazione $\sum_{i=2}^{m} z_i(\sigma_i(g_0) - \sigma_1(g_0))\sigma_i(g) = 0$ il che è in contrasto con la minimalità di m. **CVD** □

Diamo la definizione di alcune importanti classi di estensioni

Un'estensione algebrica $K \subset L$ si dice *normale* (su K) se ogni polinomio irriducibile in $K[X]$, che abbia almeno una radice in L, si decompone come prodotto di fattori lineari (non necessariamente distinti) in $L[X]$.

Se $K \subset L$ è un'estensione, i K-isomorfismi del corpo L in sé formano un gruppo che è detto il *Gruppo di Galois* di L su K e che indicheremo col simbolo $\mathrm{Gal}(L/K)$. È facile verificare che il sottoinsieme

$$L^G = \{\, x \in L \mid \sigma(x) = x,\ \forall \sigma \in \mathrm{Gal}(L/K)\,\}$$

è un sottocorpo di L e si ha $K \subset L^G \subset L$.

Diremo che un'estensione algebrica $K \subset E$ è *di Galois* se $K = E^G$.

Le estensioni di Galois si possono caratterizzare nel modo seguente (cf. Bourbaki, Algèbre, Chap. V, §.10, n.1, Proposition 1).

2.5 Proposizione. *Sia $K \subset E$ un'estensione algebrica, sono equivalenti:*
(i) E è estensione di Galois;
(ii) E è un'estensione normale e separabile;
(iii) il polinomio minimo su K di ogni elemento $x \in E$ è prodotto di fattori lineari distinti in $E[X]$.

La seguente proposizione descrive le sottoestensioni di un'estensione di Galois in termini dei loro gruppi di Galois (cf. Bourbaki, Algèbre, Chap. V, §.10, n.2, Propositions 2 e 4).

[†] Una definizione più generale di elementi coniugati, valida per estensioni qualunque, si può trovare in Bourbaki, Algèbre, Chap. V, §.6, n.2.

2.6 Proposizione. *Siano $K \subset E$ un'estensione di Galois e $K \subset L \subset E$. Allora*

(i) E è un'estensione di Galois su L e si ha $\mathrm{Gal}(E/L) \subset \mathrm{Gal}(E/K)$*;*

(ii) L è estensione di Galois su K se, e solo se, $\mathrm{Gal}(E/L)$ *è un sottogruppo normale di* $\mathrm{Gal}(E/K)$ *ed in tal caso si ha* $\mathrm{Gal}(L/K) = \mathrm{Gal}(E/K)/\mathrm{Gal}(E/L)$.

Ogni estensione di Galois $K \subset E$ è unione di sottoestensioni di Galois di grado finito (cf. Bourbaki, Algèbre, Chap. V, §.10, n.1, Corollaire) e per le estensioni di Galois di grado finito vale il seguente Teorema (cf. Bourbaki, Algèbre, Chap. V, §.10, n.5, Théorème 3).

2.7 Teorema. [Teorema fondamentale della teoria di Galois] *Sia $K \subset E$ un'estensione di Galois di grado finito. Per ogni sottogruppo $H \subset \mathrm{Gal}(E/K)$, indichiamo con*

$$E^H := \{\, x \in E \mid \sigma(x) = x,\ \forall \sigma \in H \,\}$$

il sottocorpo degli elementi di E invarianti rispetto ad H. Allora, $\mathrm{Gal}(E/K)$ *è un gruppo finito e la corrispondenza che ad ogni corpo intermedio $K \subset L \subset E$ associa il sottogruppo* $\mathrm{Gal}(E/L) \subset \mathrm{Gal}(E/K)$ *è biiettiva e si ha*

$$E^{\mathrm{Gal}(E/L)} = L \quad \textit{per ogni corpo intermedio } K \subset L \subset E,$$
$$\mathrm{Gal}(E/E^H) = H \quad \textit{per ogni sottogruppo } H \subset \mathrm{Gal}(E/K).$$

Inoltre,

$$\sharp(\mathrm{Gal}(E/L)) = [E : L] \qquad e \qquad (\mathrm{Gal}(E/K) : \mathrm{Gal}(E/L)) = [L : K],$$

ove $(\mathrm{Gal}(E/K) : \mathrm{Gal}(E/L))$ *denota l'indice del sottogruppo* $\mathrm{Gal}(E/L)$ *in* $\mathrm{Gal}(E/K)$ *e* $\sharp(\mathrm{Gal}(E/L))$ *indica il numero di elementi del gruppo finito* $\mathrm{Gal}(E/L)$.

2.8 Remark. Nel caso di estensioni di Galois di grado infinito (ad es. la chiusura algebrica di $\mathbb{Q}$ o di un corpo primo $\mathbb{F}_p$) non vi è più (in generale) corrispondenza biunivoca tra sottogruppi del gruppo di Galois e corpi intermedi dell'estensione. Per ottenere un risultato analogo al *Teorema I.2.7*, è necessario introdurre una topologia sul gruppo di Galois.

Precisamente, data un'estensione di Galois $K \subset E$, di grado infinito, sia $G = \mathrm{Gal}(E/K)$ il suo gruppo di Galois. Allora, al variare di L tra le sottoestensioni di Galois di E, di grado finito su K, i sottogruppi $\mathrm{Gal}(E/L) \subset \mathrm{Gal}(E/K)$ sono sottogruppi normali e formano un sistema fondamentale di intorni dell'elemento neutro, che rendono $\mathrm{Gal}(E/K)$ un gruppo topologico. Vale quindi il seguente

2.9 Teorema. *Sia $K \subset E$ un'estensione di Galois. Per ogni sottogruppo chiuso* $H \subset \mathrm{Gal}(E/K)$*, indichiamo con*

$$E^H := \{\, x \in E \mid \sigma(x) = x,\ \forall \sigma \in H \,\}$$

il sottocorpo degli elementi di E invarianti rispetto ad H. Allora, la corrispondenza che ad ogni corpo intermedio $K \subset L \subset E$ associa il sottogruppo chiuso $\mathrm{Gal}(E/L) \subset \mathrm{Gal}(E/K)$ *è biiettiva e si ha*

$$E^{\mathrm{Gal}(E/L)} = L \quad \textit{per ogni corpo intermedio } K \subset L \subset E,$$
$$\mathrm{Gal}(E/E^H) = H \quad \textit{per ogni sottogruppo chiuso } H \subset \mathrm{Gal}(E/K).$$

Per dettagli ed approfondimenti, rimandiamo il lettore a Bourbaki, Algèbre, Chap. V, Appendice II

Richiamiamo ora le proprietà fondamentali di traccia e norma per gli elementi di estensioni finite.

Sia L un'estensione finita del corpo K e sia $n = [L : K] := \dim_K L$. Allora, dato un elemento $x \in L$ si può considerare l'endomorfismo (di K-spazi vettoriali) $\mu_x : L \to L$, definito ponendo $\mu_x(y) = xy$ al variare di $y \in L$. Si definiscono quindi la *norma* e la *traccia* di x ponendo

$$N_{L/K}(x) := \det \mu_x, \qquad Tr_{L/K}(x) := \operatorname{tr} \mu_x. \tag{2.10}$$

Richiamiamo le proprietà elementari di traccia e norma nella seguente

2.11 Proposizione. *Siano L' un'estensione finita del corpo L ed L un'estensione finita del corpo K, di gradi $[L' : L] = m$ ed $[L : K] = n$. Allora, dati comunque $x, y \in L$, si ha*

(i) $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$, *e* $Tr_{L/K}(x+y) = Tr_{L/K}(x) + Tr_{L/K}(y)$;

(ii) $N_{L/K}(a) = a^n$ *e* $Tr_{L/K}(a) = na$ *per ogni* $a \in K$;

(iii) $N_{L'/K}(x) = N_{L'/L}(N_{L/K}(x)) = N_{L/K}(x)^m$ *e* $Tr_{L'/K}(x) = Tr_{L'/L}(Tr_{L/K}(x)) = mTr_{L/K}(x)$.

(iv) *Sia* $p(X) = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} + X^r$ *il polinomio minimo di* x *su* K, *allora si ha* $N_{K(x)/K}(x) = (-1)^r a_0$ *e* $Tr_{K(x)/K}(x) = -a_{r-1}$.

dim. Le proprietà (i) e (ii) sono conseguenza diretta delle proprietà del determinante e della traccia degli endomorfismi di K-spazi vettoriali di dimensione finita. La proprietà (iii) si può dedurre dal fatto che è possibile costruire una base di L' su K del tipo $\{\, s_i l_j \mid 1 \le i \le m,\ 1 \le j \le n \,\}$, ove $\{\, s_i \mid 1 \le i \le m \,\}$ è una base di L' su L ed $\{\, l_j \mid 1 \le j \le n \,\}$ è una base di L su K ed utilizzando tale base per scrivere la matrice di $\mu_x : L' \to L'$, si ottengono le relazioni enunciate tra $N_{L'/K}(x)$ e $N_{L/K}(x)$ e tra $Tr_{L'/K}(x)$ e $Tr_{L/K}(x)$. Infine, la proprietà (iv) si ottiene con un calcolo diretto dalla matrice di μ_x rispetto alla base $\{\, 1, x, \ldots, x^{r-1} \,\}$ di $K(x)$ su K, che è la matrice compagna del polinomio $p(X)$. **CVD** □

Sia ora L un'estensione finita e separabile del corpo K. Allora, in base alla *Proposizione I.2.3*, vi sono $n = [L : K]$ immersioni distinte $\sigma_1, \ldots, \sigma_n$ di L in una chiusura algebrica di K. Dato un elemento $x \in L$ ed indicato con $p(X) = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} + X^r$ il polinomio minimo di x su K, vogliamo mostrare che si ha

$$N_{L/K}(x) = (-1)^n (a_0)^{n/r} = \prod_{j=1}^{n} \sigma_j(x) \qquad \text{e} \qquad Tr_{L/K}(x) = -\frac{n}{r} a_{r-1} = \sum_{j=1}^{n} \sigma_j(x). \tag{2.12}$$

Poichè x è separabile, in una chiusura algebrica Ω di K vi sono r radici distinte di $p(X)$; inoltre, poichè L è separabile su $K(x)$ ed $[L : K(x)] = n/r$, fissata una radice $u \in \Omega$ di $p(X)$, si deduce dalla *Proposizione I.2.3*, che vi sono al più n/r K-omomorfismi di L in Ω che mandano x su u. Ripetendo il discorso per tutte le radici di $p(X)$ si ottiene che ognuna delle radici di questo polinomio compare esattamente n/r volte tra i coniugati di x. Ricordando che $-a_{r-1}$ e $(-1)^r(a_0)$ sono esattamente la somma ed il prodotto delle radici del polinomio $p(X)$ si ottiene la formula (I.2.12).

Vi è una facile conseguenza delle proprietà della traccia, che ci sarà utile nel seguito.

2.13 Corollario. *Sia L un'estensione finita e separabile del corpo K, allora l'applicazione*

$$\begin{array}{ccc} L \times L & \to & K \\ (x, y) & \mapsto & Tr_{L/K}(xy) \end{array}$$

è un'applicazione K-bilineare, simmetrica e non-degenere.

dim. Fissato comunque un elemento $0 \ne x \in L$, l'applicazione $y \mapsto xy$ è una biiezione di L in sé e quindi è sufficiente dimostrare che esiste un elemento $u \in L$ per cui si abbia $Tr_{L/K}(u) \ne 0$.

Se fosse $Tr_{L/K}(y) = 0$ per ogni $y \in L$, in base a *I.2.12* si otterrebbe una relazione di dipendenza lineare tra i K-omomorfismi $\sigma_1, \ldots, \sigma_n$ e ciò contraddice il teorema di indipendenza dei caratteri (cf. *Proposizione I.2.4*). **CVD** □

Concludiamo questa sezione richiamando un risultato elementare sui polinomi simmetrici. Sia A un anello (commutativo con 1); un polinomio $f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ è *simmetrico* se, per ogni permutazione $\sigma \in \Sigma_n$, si ha $f^\sigma = f$, ove $f^\sigma := f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.

Ad esempio, i polinomi

$$s_1 = X_1 + \cdots + X_n, \quad \ldots \quad s_k = \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k}, \quad \ldots \quad s_n = X_1 \cdots X_n$$

sono polinomi simmetrici e sono detti i *polinomi simmetrici elementari*(*) I polinomi simmetrici elementari svolgono un ruolo fondamentale nella costruzione dei polinomi simmetrici; infatti, è immediato verificare che, dato comunque un polinomio $h(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$, il polinomio $h(s_1, \dots, s_n)$ è un polinomio simmetrico. Mostreremo che ogni polinomio simmetrico si scrive in questo modo.

Sia $f(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$ un polinomio simmetrico non nullo, e sia M un monomio monico, che compare in f con un coefficiente non nullo. Allora, poichè f è simmetrico anche tutti i monomi M^σ, al variare di $\sigma \in \Sigma_n$ compaiono in f con lo stesso coefficiente; dunque, posto

$$\tau(M) = \sum_{M^\sigma \in I_M} M^\sigma, \qquad \text{ove } I_M \text{ è l'insieme dei monomi } \textit{distinti} \text{ che compaiono in } \{\, M^\sigma \mid \sigma \in \Sigma_n \,\},$$

possiamo scrivere $f(X) = \sum_{M \in J} c_M \tau(M)$ ove J è un insieme finito di monomi monici nelle indeterminate $X_1, \dots, X_n$.

Il risultato fondamentale sui polinomi simmetrici può essere così enunciato.

2.14 Teorema. *Sia M un monomio monico in $A[X_1, \dots, X_n]$, allora esiste un polinomio $\phi(Y_1, \dots, Y_n) \in \mathbb{Z}[Y_1, \dots, Y_n]$ tale che $\tau(M) = \phi(s_1, \dots, s_n)$, ove $s_1, \dots, s_n)$ sono i polinomi simmetrici elementari.*

dim. Poichè il grado del polinomio simmetrico elementare s_j è uguale a j, introduciamo un *peso* per i polinomi in $\mathbb{Z}[Y_1, \dots, Y_n]$, attribuendo peso j all'indeterminata Y_j per $j = 1, \dots, n$. Mostreremo quindi che, se M è un monomio nelle indeterminate $X_1, \dots, X_n$, di grado k, allora il corrispondente polinomio $\phi(Y_1, \dots, Y_n) \in \mathbb{Z}[Y_1, \dots, Y_n]$ dell'enunciato, deve avere peso k.

Facciamo induzione sul numero delle variabili n, osservando che, per $n = 1$ la tesi è banalmente vera. Inoltre, se n è qualunque e $k = 0$ o $k = 1$, ancora una volta la tesi è banalmente vera; dunque faremo induzione anche sul grado k.

Sia quindi $\tau(M) = f(X_1, \dots, X_n)$ e si consideri il polinomio $f(X_1, \dots, X_{n-1}, 0)$. Essendo quest'ultimo un polinomio simmetrico in $n-1$ indeterminate, possiamo applicare l'ipotesi induttiva e scrivere

$$f(X_1, \dots, X_{n-1}, 0) = \psi(s'_1, \dots, s'_{n-1}),$$

ove $\psi(Y_1, \dots, Y_{n-1}) \in \mathbb{Z}[Y_1, \dots, Y_{n-1}]$ ed $s'_j = s_j(X_1, \dots, X_{n-1}, 0)$, per $j = 1, \dots, n-1$, sono i polinomi simmetrici elementari in $n-1$ indeterminate.

Consideriamo ora il polinomio

$$g(X_1, \dots, X_n) = f(X_1, \dots, X_n) - \psi(s_1, \dots, s_{n-1}).$$

Poichè X_n divide g, e g è un polinomio simmetrico, si conclude che $s_n = X_1 \cdots X_n$ divide $g(X_1, \dots, X_n)$ e quindi, se $g \neq 0$, si ha $g = s_n h$, ove $h(X_1, \dots, X_n) \neq 0$ è un polinomio simmetrico di grado minore del grado di f e quindi, si può applicare l'ipotesi induttiva sul grado per concludere. **CVD** $\square$

(*) Un modo semplice per ricordare la definizione dei polinomi simmetrici elementari e verificarne la simmetria è il seguente. Si introduca un'ulteriore indeterminata T e si osservi che in $A[X_1, \dots, X_n, T]$ si ha

$$\prod_{i=1}^{n} (T - X_i) = T^n + \sum_{j=1}^{n} (-1)^j s_j T^{n-j}.$$

3. Interi di un'estensione algebrica.

Cominciamo con una definizione

3.1 Definizione. Sia L un campo ed $A \subset L$ un sottoanello. Un elemento $x \in L$ si dice *intero* su A se soddisfa ad un'equazione monica a coefficienti in A; ovvero se esistono $a_0, \dots, a_{n-1} \in A$ tali che $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n = 0$.

Un anello $B \supset A$ è *intero* su A, se ogni elemento di B è intero su A.

Vi è una semplice caratterizzazione degli elementi interi che sarà utile nel seguito

3.2 Proposizione. *Sia L un campo ed $A \subset L$ un sottoanello. Sono equivalenti*
(i) x è intero su A;
(ii) l'anello $A[x]$ è un A-modulo finitamente generato;
(iii) esiste un A-modulo $(0) \neq M \subset L$, finitamente generato su A e tale che $xM \subseteq M$.

dim. *(i) ⇒ (ii) ⇒ (iii).* Sia $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n = 0$, con $a_0, \dots, a_{n-1} \in A$; allora $A[x] = A + Ax + \cdots + Ax^{n-1} \subset L$ e ciò è sufficiente per concludere.
(iii) ⇒ (i). Sia $\{e_1, \dots, e_n\}$ un insieme di generatori l'A-modulo M. Essendo $xM \subseteq M$, esiste una matrice $A = (a_{i,j})_{1 \le i,j \le n}$ ad elementi in A tale che

$$xe_j = \sum_{i=1}^{n} a_{i,j} e_i \qquad \text{per} \quad j = 1, \dots, n.$$

Se ne deduce che x è una radice del polinomio caratteristico di A, $\det(X\mathbf{1}_n - A)$, che è un polinomio monico, di grado n, a coefficienti in A. **CVD** □

3.3 Corollario. *Siano L un campo ed $A \subset B \subset C \subset L$ sottoanelli, con B intero su A e C intero su B. Allora C è intero su A.*

dim. Sia $x \in C$ e sia $b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n = 0$, con $b_1, \dots, b_n \in B$. Allora x è intero sull'anello $B_0 = A[b_0, \dots, b_n]$, che è un A-modulo finitamente generato, per *Proposizione I.3.2.(ii)*. Dunque, $B_0[x]$ è un modulo finitamente generato su B_0, che, a sua volta è finitamente generato su A. Si conclude che $B_0[x]$ è un A-modulo finitamente generato, chiuso rispetto alla moltiplicazione per x e quindi, per la *Proposizione I.3.2*, x è intero su A. **CVD** □

3.4 Remark. Da quanto abbiamo dimostrato discende che gli elementi di L interi su A formano un sottoanello di L, detto la *chiusura integrale* (o *chiusura aritmetica*) di A in L. Infatti, se x ed y sono interi su A tali sono anche $x + y$ ed xy, perchè l'algebra $A[x, y]$ è un modulo finitamente generato su $A[x]$ e quindi su A, ed $A[x, y]$ è chiuso rispetto alla moltiplicazione per $x + y$ ed xy.

Diamo un'altra dimostrazione più 'classica' del fatto che gli interi su $\mathbb{Z}$ formano un anello, basata sul teorema fondamentale sui polinomi simmetrici (cf. *Teorema I.2.14*). Siano α_1 e β_1 due elementi interi su $\mathbb{Z}$, e si decompongano le loro equazioni intere nella forma

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \qquad \text{e} \qquad g(X) = (X - \beta_1) \cdots (X - \beta_n).$$

I polinomi

$$h(X) = \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (X - \alpha_i - \beta_j) \qquad \text{e} \qquad k(X) = \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (X - \alpha_i \beta_j)$$

sono polinomi a coefficienti in $\mathbb{Z}$, perchè tali coefficienti sono polinomi simmetrici nelle α_i e β_j, e quindi polinomi a coefficienti interi nelle funzioni simmetriche elementari di $\alpha_1, \dots, \alpha_n$ e $\beta_1, \dots, \beta_m$, e quest'ultime coincidono con i coefficienti dei polinomi $f(X)$ e $g(X)$, che appartengono a $\mathbb{Z}$.

3.5 Definizione. Sia B un dominio ed $A \subset B$. Si dice che A è *integralmente chiuso in B* se non vi sono elementi di B, interi su A, e non appartenenti ad A.

Un dominio A è *integralmente chiuso* se è integralmente chiuso nel suo corpo dei quozienti.

La Proposizione che segue mette in evidenza un'importante classe di domini integralmente chiusi. A tale scopo, ricordiamo che si chiama *dominio fattoriale* un dominio di integrità su cui valga il teorema di fattorizzazione unica; ovvero un dominio in cui ogni elemento $x \neq 0$ si scriva come prodotto di elementi irriducibili, determinati da x a meno di moltiplicazione per unità dell'anello.

Ricordiamo che l'anello degli interi razionali $\mathbb{Z}$ e, più in generale, ogni dominio ad ideali principali è un dominio fattoriale. Inoltre, se A è un dominio fattoriale, allora anche l'anello dei polinomi $A[X_1, \dots, X_n]$ è fattoriale (cf.[...]).

3.6 Proposizione. *Sia A un dominio fattoriale e K il suo corpo delle frazioni. Allora*
(i) A è integralmente chiuso.
(ii) Sia L un'estensione di K. Un elemento $x \in L$ è intero su A se, e solo se, il suo polinomo minimo $p(X) \in K[X]$ ha i coefficienti nell'anello A.

dim. (i) Sia $x \in K$ un elemento intero su A e supponiamo che $x = \frac{a}{b}$, con a e b elementi di A privi di fattori irriducibili comuni. Moltiplicando per b^n la relazione $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n = 0$, si ottiene che $-a_0b^n - a_1ab^{n-1} - \cdots - a_{n-1}a^{n-1}b = a^n$ e quindi che $b \mid a^n$. Poichè a e b non hanno fattori irriducibili in comune, ciò è possibile solo se b è un'unità, ovvero se $x \in A$.
(ii) Sia $g(X) \in A[X]$ un polinomio monico, di grado minimo rispetto alla condizione $g(x) = 0$. Allora il polinomio minimo $p(X)$ divide $g(X)$, ma, per il Lemma di Gauss (cf. [...]), se vi fossero due fattori di grado positivo in $K[X]$, g si decomporrebbe anche in $A[X]$, contro l'ipotesi che g sia di grado minimo. Dunque, essendo entrambi polinomi monici, deve aversi $p(X) = g(X)^{(*)}$. **CVD** □

Nel seguito di questa sezione daremo due dimostrazioni del fatto che la chiusura integrale B di un dominio integralmente chiuso A, in un'estensione finita e separabile L del corpo dei dei quozienti $K = Frac\, A$, è un A-modulo finitamente generato.
Cominciamo con un lemma

3.7 Lemma. *Siano A un dominio ed L un'estensione finita del corpo dei quozienti $K = Frac\, A$. Allora,*
(i) Se $x \in L$, esiste una costante $0 \neq c \in A$ tale che cx sia intero su A.
(ii) Esiste una base di L su K fatta da elementi interi su A.

dim. (i). Moltiplicando per il prodotto dei denominatori dei coefficienti del polinomio minimo di x su K, si ottiene una relazione del tipo $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n = 0$, con i coefficienti in A ed $a_n \neq 0$. Moltiplicando quest'ultima relazione per a_n^{n-1}, si ottiene un'equazione monica, a coefficienti in A, soddisfatta dall'elemento a_nx che è perciò intero su A.
(ii). Discende banalmente dal punto precedente. **CVD** □

Possiamo quindi enunciare e dimostrare il risultato annunciato.

3.8 Teorema. *Sia A un dominio noetheriano, integralmente chiuso e sia L un'estensione finita e separabile del campo dei quozienti $K = Frac\, A$. Allora la chiusura integrale B di A in L è un A-modulo finitamente generato.*

dim. Sia $\omega_1, \dots, \omega_n$ una base di L su K fatta da elementi interi su A (cf. *Lemma I.3.7*); vogliamo mostrare che tutti gli $x \in B$ si scrivono nella forma

$$x = \frac{a_1}{c}\omega_1 + \cdots + \frac{a_n}{c}\omega_n, \qquad \text{con } a_j \in A \text{ e } c \text{ indipendente da } x.$$

(*) Più in generale, osserviamo che, se x è intero su A, allora i coefficienti del polinomio minimo di x sono in K e sono interi su A, perchè sono funzioni simmetriche nei coniugati di x, che sono tutti interi; dunque, *se A è integralmente chiuso, i coefficienti del polinomio minimo di x appartengono ad A.*

Se ciò è vero si ha che B è un sottomodulo del modulo finitamente generato $A\frac{\omega_1}{c} + \cdots + A\frac{\omega_n}{c}$ e quindi, poichè A è noetheriano si conclude.

Per quanto visto nel *Corollario I.2.13*, l'applicazione bilineare su L $(x,y) \mapsto Tr_{L/K}(xy)$ è non degenere e quindi esistono degli elementi $\omega_1^*, \dots, \omega_n^*$ di L che formino una base duale della base data. Si ha quindi $B \ni x = b_1\omega_1 + \cdots + b_n\omega_n$, con $b_j = Tr_{L/K}(x\omega_j^*)$, per $j = 1, \dots, n$.

Per il *Lemma I.3.7*, esiste una costante $0 \neq c \in A$ tale che ciascuno degli elementi $c\omega_1^*, \dots, c\omega_n^*$ sia intero su A; ne consegue che $b_j = \dfrac{cb_j}{c}$, per $j = 1, \dots, n$, e che $cb_j = Tr_{L/K}(xc\omega_j^*) \in B \cap K$ perchè è una somma di coniugati di elementi interi su A (cf. (I.2.12)). Poichè A è integralmente chiuso, si conclude che $B \cap K = A$ e quindi c è il denominatore cercato. **CVD** □

Nel seguito daremo un'altra dimostrazione del Teorema precedente, ove sia descritto in modo più esplicito il denominatore c che compare nella dimostrazione precedente; prima di fare questo, vogliamo enunciare alcune conseguenze del risultato appena dimostrato.

3.9 Corollario. *Siano A un dominio ad ideali principali, K il suo corpo dei quozienti ed L un'estensione finita di K. Allora la chiusura integrale B di A in L è un modulo libero finito sull'anello A, di rango uguale al grado $[L : K]$.*

dim. In base alla *Proposizione I.3.6.(i)*, valgono tutte le ipotesi del *Teorema I.3.8* e quindi B è un A-modulo finitamente generato, inoltre, essendo contenuto nel corpo L, B è un modulo senza torsione e quindi libero su A.

Per quanto riguarda il rango di tale modulo, è sufficiente osservare che B contiene una base di L su K (cf. *Lemma I.3.7*). **CVD** □

3.10 Definizione. Siano A un dominio ad ideali principali, K il suo corpo dei quozienti, L un'estensione finita di K e B la chiusura integrale di A in L. Si chiama *base intera* di B ogni sistema libero di generatori di B come A-modulo.

Possiamo quindi dare un'altra dimostrazione del teorema sulla struttura della chiusura integrale.

dim. (seconda dimostrazione del *Teorema I.3.8*) Sia $\omega_1, \dots, \omega_n$ una base di L su K fatta da elementi interi su A (cf. *Lemma I.3.7*); e sia $x \in B$. Scriviamo quindi

$$(*) \qquad x = b_1\omega_1 + \cdots + b_n\omega_n, \qquad \text{ove } b_1, \dots, b_n \in K.$$

Dalla *Proposizione I.2.3*, sappiamo che esistono $n = [L : K]$ K-omomorfismi distinti $\sigma_1, \dots, \sigma_n$ di L verso una chiusura algebrica $\bar{K}$ di K. Applicando questi omomorfismi alla relazione $(*)$, possiamo scrivere

$$\sigma_i(x) = \sum_{j=1}^{n} b_j \sigma_i(\omega_j), \qquad i = 1, \dots, n,$$

poichè $b_1, \dots, b_n \in K$.

Osserviamo che $\det(\sigma_i(\omega_j))_{1 \leq i,j \leq n} \neq 0$. Infatti, se esistessero delle costanti $z_1, \dots, z_n \in \bar{K}$ tali che $\sum_{i=1}^{n} z_i\sigma_i(\omega_j) = 0$, per $i = 1, \dots, n$, sfruttando la K-linearità degli omomorfismi $\sigma_1, \dots, \sigma_n$, si dedurrebbe $\sum_{i=1}^{n} z_i\sigma_i(y) = 0$, per ogni y nel gruppo moltiplicativo $L^\times$, e ciò non può aversi in base al Teorema di indipendenza dei caratteri (cf. *Proposizione I.2.4*).

Allora, tramite l'usuale regola di Cramer per i sistemi lineari, possiamo scrivere i coefficienti b_j nella forma

$$b_j = \frac{N_j}{D^2}, \qquad \text{ove } D = \det\begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_n) \end{pmatrix}$$

ed N_j è un polinomio a coefficienti in $\mathbb{Z}$ negli elementi $\sigma_h(\omega_k)$ (per tutti gli h e $k \neq j$), D e $\sigma_h(x)$. Osserviamo che si ha $D^2 = \sigma_j(D^2)$ per ogni $j = 1, \ldots, n$ e perciò $D^2 \in K$, ed essendo $N_j = D^2 b_j$, si ha anche $N_j \in K$. Inoltre, tutte le entrate della matrice che definisce D sono elementi interi su A e quindi lo stesso possiamo dire del determinante D. Ed, analogamente, sono interi su A anche i numeratori N_j in quanto funzioni polinomiali a coefficienti interi calcolate su elementi interi su A. Dunque, poichè A è integralmente chiuso, possiamo concludere che $D^2 \in A$ ed $N_j \in A$, per $j = 1, \ldots, n$; ovvero che

$$B \subset A\frac{\omega_1}{D^2} + \cdots + A\frac{\omega_n}{D^2},$$

ed essendo A noetheriano, si conclude. **CVD** $\square$

Diamo quindi la seguente

3.11 Definizione. Siano A un dominio noetheriano ed integralmente chiuso, K il suo corpo dei quozienti, L un'estensione finita e separabile di K e B la chiusura integrale di A in L. Fissata una base $\omega_1, \ldots, \omega_n$ una base di L su K fatta da elementi interi su A (cf. *Lemma I.3.7*), si chiama *discriminante* della base fissata l'elemento

$$D^2 = \Delta(\omega_1, \ldots, \omega_n) = \det \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\omega_1) & \ldots & \sigma_n(\omega_n) \end{pmatrix}^2 \in A,$$

ove $\sigma_1, \ldots, \sigma_n$ sono i K-omomorfismi distinti di L verso una chiusura algebrica $\bar{K}$ di K (cf. *Proposizione I.2.3*).

La seguente proposizione chiarisce le relazioni tra le due dimostrazioni del *Teorema I.3.8*.

3.12 Proposizione. *Siano A un dominio noetheriano ed integralmente chiuso, K il suo corpo dei quozienti, L un'estensione separabile di K, di grado n, e B la chiusura integrale di A in L. Fissata una base $\omega_1, \ldots, \omega_n$ una base di L su K fatta da elementi di B, si ha*

$$\Delta(\omega_1, \ldots, \omega_n) = \det(Tr_{L/K}(\omega_i\omega_j))_{1 \leq i,j \leq n},$$

ove $\Delta(\omega_1, \ldots, \omega_n)$ indica il discriminante della base fissata (cf. Definizione I.3.11).

dim. Siano $\sigma_1, \ldots, \sigma_n$ i K-omomorfismi distinti di L verso una chiusura algebrica $\bar{K}$ di K (cf. *Proposizione I.2.3*) e si consideri la matrice $M = (\sigma_i(\omega_j))_{1 \leq i,j \leq n}$. Allora, in base alla definizione di discriminante, si ha

$$\Delta(\omega_1, \ldots, \omega_n) = \det({}^tMM)$$

e l'elemento di posto (i, j) della matrice ${}^tMM$ è uguale a (cf. I.2.12)

$$\sum_{h=1}^{n} \sigma_h(\omega_i)\sigma_h(\omega_j) = \sum_{h=1}^{n} \sigma_h(\omega_i\omega_j) = Tr_{L/K}(\omega_i\omega_j),$$

che conclude la discussione. **CVD** $\square$

Concludiamo con un ultima osservazione sul discriminante.

3.13 Remark. Osserviamo che se A è un dominio ad ideali principali, e B è la chiusura integrale di A in un'estensione finita separabile di $K = Frac A$, allora B è un A-modulo libero e, fissato un sistema libero di generatori $\beta_1, \ldots, \beta_n$ di B su A (cf. *Definizione I.3.10*), si può considerare il discriminante $\Delta(\beta_1, \ldots, \beta_n)$. Si osservi che

- *l'ideale di A generato da $\Delta(\beta_1, \dots, \beta_n)$ è indipendente dalla scelta della base intera ed è quindi detto il discriminante di B su A.*

Se $\beta'_1, \dots, \beta'_n$ è un'altra base intera di B, si ha $(\beta'_1, \dots, \beta'_n) = (\beta_1, \dots, \beta_n)T$, ove $T \in \mathrm{GL}(n, A)$; quindi, scelto comunque un K-omomorfismo σ di L verso una (fissata) chiusura algebrica $\bar{K}$ di K, si ha

$$(\sigma(\beta'_1), \dots, \sigma(\beta'_n)) = (\sigma(\beta_1), \dots, \sigma(\beta_n))T.$$

Si conclude perciò che

$$\Delta(\beta'_1, \dots, \beta'_n) = \Delta(\beta_1, \dots, \beta_n)(\det T)^2, \qquad \text{e} \quad \det T \in A^\times.$$

In particolare, da quanto osservato discende che, se $A = \mathbb{Z}$, allora il discriminante stesso (e non solo l'ideale generato) è indipendente dalla scelta della base intera e viene perciò detto il discriminante dell'estensione L di $\mathbb{Q}$ (o del suo anello di interi).

4. Corpi quadratici e corpi ciclotomici

In questa sezione ci occupiamo delle grandezze introdotte nella sezione precedente, nel caso di alcune particolari estensioni di $\mathbb{Q}$. Cominciamo quindi ad occuparci dei *corpi quadratici*, ovvero delle estensioni di $\mathbb{Q}$ del tipo $K = \mathbb{Q}(\sqrt{d})$, ove d è un intero, non quadrato e *square-free*, ovvero, soddisfacente alla condizione $f^2 \mid d$, $f \in \mathbb{Z} \Rightarrow f = \pm 1$. Sia B l'anello degli interi di K, ovvero la chiusura integrale di $\mathbb{Z}$ in K, e cerchiamo di caratterizzare gli elementi di B ed una sua base intera (cf. *Definizione I.3.10*). Sia quindi

$$x = \frac{a + b\sqrt{d}}{q} \in B,$$

con $a, b, q \in \mathbb{Z}$, $q \neq 0$ ed $\mathrm{Mcd}(a, b, q) = 1$ e supponiamo inoltre che sia $b \neq 0$, ovvero che x abbia grado 2 su $\mathbb{Q}$, perchè già sappiamo che $B \cap \mathbb{Q} = \mathbb{Z}$, perchè $\mathbb{Z}$ è integralmente chiuso (cf. *Proposizione I.3.6*). Allora x deve soddisfare alla relazione $(qx - a)^2 = b^2 d$, da cui si deduce che

$$p(X) = X^2 - \frac{2a}{q}X + \frac{a^2 - b^2 d}{q^2}$$

è il polinomio minimo di x su $\mathbb{Q}$ e, quindi, per il risultato già citato, $p(X)$ ha i coefficienti in $\mathbb{Z}$ e perciò

$$q \mid 2a, \qquad q^2 \mid (a^2 - b^2 d). \tag{4.1}$$

Ciò implica che q deve essere uguale ad 1 oppure a 2. Infatti, se $p > 2$ è un numero primo e $p \mid q$, dalla prima delle (I.4.1) discende che $p \mid a$ e quindi, utilizzando la seconda, che $p^2 \mid b^2 d$. Poichè d è square-free, si ha che $p \mid b$ e ciò non è possibile perchè $\mathrm{Mcd}(a, b, q) = 1$. Dunque q non ha fattori primi diversi da 2 e inoltre, da $4 \mid q$, si deduce che 2 divide anche a e b, e ciò contrasta di nuovo con l'ipotesi $\mathrm{Mcd}(a, b, q) = 1$. Supponiamo ora $q = 2$ ed osserviamo che, sempre in base a (I.4.1), se d fosse pari, si avrebbe $4 \mid (a^2 - b^2 d)$ e quindi che 2 dovrebbe dividere sia a che b e ciò è sempre in contrasto con l'ipotesi che i tre interi a, b e q siano primi tra loro.

Sia dunque d un numero dispari ed osserviamo che, se $d \equiv 3 \pmod 4$, allora $q = 1$. Perchè, se fosse $q = 2$, si avrebbe

$$0 \equiv a^2 - b^2 d \equiv a^2 + b^2 \pmod 4$$

e ciò è impossibile, perchè, essendo $(a, b, q) = 1$, a e b devono essere entrambi dispari e ciò è assurdo.

Infine, osserviamo che, se $d \equiv 1 \pmod 4$, può aversi $q = 2$, con $a \equiv b \equiv 1 \pmod 2$; infatti, in tal caso $\frac{1+\sqrt{d}}{2}$ è un intero di K. Possiamo quindi riassumere le considerazioni precedenti nella seguente

4.2 Proposizione. *Sia $K = \mathbb{Q}(\sqrt{d})$, ove d è un intero, non quadrato e square-free e sia B la chiusura integrale di $\mathbb{Z}$ in K. Allora*

(i) se $d \equiv 2 \pmod 4$ o $d \equiv 3 \pmod 4$ una base di B come $\mathbb{Z}$-modulo è $\{1, \sqrt{d}\}$, e quindi $B = \mathbb{Z}[\sqrt{d}]$;

(ii) se $d \equiv 1 \pmod 4$ una base di B come $\mathbb{Z}$-modulo è $\{1, \frac{1+\sqrt{d}}{2}\}$, e quindi $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = B$.

Si deduce quindi, con un calcolo di determinanti.

4.3 Corollario. *Sia $K = \mathbb{Q}(\sqrt{d})$, ove d è un intero, non quadrato e square-free e sia B la chiusura integrale di $\mathbb{Z}$ in K. Allora, indicato con Δ il discriminante di B (cf. Remark I.3.13), si ha*

(i) se $d \equiv 2 \pmod 4$ o $d \equiv 3 \pmod 4$, allora $\Delta = 4d$;

(ii) se $d \equiv 1 \pmod 4$, allora $\Delta = d$.

Ora vogliamo occuparci dei *corpi ciclotomici*, che sono i sottocorpi di $\mathbb{Q}(\zeta_n)$, ove ζ_n è una radice n-esima primitiva di 1. In questo primo approccio ci occuperemo solo dei corpi ciclotomici principali, ovvero del tipo di $\mathbb{Q}(\zeta_n)$; e cominciamo osservando che, poichè ζ_n è una radice n-esima primitiva di 1, $\mathbb{Q}(\zeta_n)$ è il corpo di decomposizione del polinomio

$$X^n - 1 = \prod_{j=0}^{n-1}(X - \zeta_n^j).$$

Il grado dell'estensione $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, è il grado del polinomio minimo $\phi_n(X) \in \mathbb{Z}[X]$ di ζ_n (*polinomio ciclotomico* di ordine n), che è un divisore di $\frac{X^n-1}{X-1} = 1 + X \cdots + X^{n-1}$. Per determinare il grado di $\phi_n(X)$, possiamo contare il numero dei $\mathbb{Q}$-automorfismi di $Q(\zeta_n)$ in sé (cf. *Proposizione I.2.3*), e per fare ciò, osserviamo che i $\mathbb{Q}$-automorfismi di $Q(\zeta_n)$ sono completamente inviduati dall'immagine dell'elemento ζ^n, che deve essere ancora una radice n-esima primitiva di 1, quindi, deve aversi $\zeta_n \mapsto \zeta_n^a$, per un qualche $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, e la corrispondenza così costruita tra $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $(\mathbb{Z}/n\mathbb{Z})^\times$ è chiaramente un isomorfismo di gruppi.

Dunque, si ha

$$\deg \phi_n(X) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \sharp(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})) = \sharp((\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(n) = n \prod_{\substack{p \text{ primo} \\ p|n}} (1 - \tfrac{1}{p}), \tag{4.4}$$

ove $\varphi : \mathbb{N} \to \mathbb{N}$ è la *funzione di Eulero*, ovvero la funzione che conta gli interi minori di n e primi con n (che rappresentano perciò gli invertibili dell'anello $\mathbb{Z}/n\mathbb{Z}$)[(†)].

(†) La formula

$$\varphi(n) = n \prod_{\substack{p \text{ primo} \\ p|n}} (1 - \tfrac{1}{p})$$

si può dimostrare nel modo seguente. Dapprima si verifica che è vera quando $n = p$ è un numero primo, perchè vi sono esattamente $p-1$ elementi invertibili nel campo $\mathbb{Z}/p\mathbb{Z}$. Poi, si osserva che, sempre se p è un numero primo, si ha la sequenza esatta

$$0 \to p^n\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

da cui si deduce che la controimmagine di ogni elemento invertibile in $\mathbb{Z}/p^n\mathbb{Z}$ è invertibile in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, e quindi $\varphi(p^{k+1}) = p\varphi(p^k)$; per cui la formula è vera anche per le potenze di un primo. Infine, si conclude osservando che, se n ed m sono coprimi, si ha l'isomorfismo di anelli (Teorema cinese del resto)

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

e quindi anche il gruppo degli elementi invertibili è prodotto diretto dei due gruppi di invertibili. Da cui si deduce che se $\mathrm{Mcd}(n, m) = 1$, allora $\varphi(nm) = \varphi(n)\varphi(m)$ e ciò permette di concludere che la formula è vera in generale.

4.5 Remark. Vi era un altro modo di dimostrare che $\deg \phi_n(X) = \varphi(n)$, ovvero è sufficiente dimostrare che

- *Se ζ è una radice del polinomio ciclotomico di ordine n, $\phi_n(X)$, e $p < n$ è un numero primo che non divide n, allora $\phi_n(\zeta^p) = 0$.*

Infatti, da questa osservazione si ottiene che tutte le potenze ζ^a, con $a < n$ e $\mathrm{Mcd}(a, n) = 1$ sono radici distinte del polinomio ciclotomico e quindi il grado di $\phi_n(x)$ deve essere maggiore o uguale di $\varphi(n)$, che è il numero delle radici n-esime primitive di 1. Dunque i due numeri devono essere uguali.

Passiamo quindi a dimostrare l'asserzione sulle radici del polinomio ciclotomico. Sia $g(X) \in \mathbb{Z}[X]$ il polinomio minimo di ζ^p; deve quindi aversi $\phi_n(X) \mid g(X^p)$ in $\mathbb{Q}[X]$ e, per il Lemma di Gauss, si ha $g(X^p) = \phi_n(X)G(X)$, per un opportuno $G(X) \in \mathbb{Z}[X]$. Riducendo modulo p i coefficienti dei polinomi, si ottiene la relazione

$$\bar{g}(X^p) = (\bar{g}(X))^p = \bar{\phi}_n(X)\bar{G}(X) \qquad \text{in } \mathbb{F}_p[X],$$

e quindi $\bar{\phi}_n(X)$ e $\bar{g}(X)$ devono avere dei fattori in comune in $\bar{\mathbb{F}}_p[X]$. Dunque, se $\phi_n(X) \neq g(X)$, essendo entrambi polinomi irriducibili, deve aversi

$$X^n - 1 = \phi_n(X)g(X)H(X) \qquad \text{in } \mathbb{Z}[X],$$

e quindi riducendo modulo p questa identità, si deduce che $X^n - 1$ deve avere radici multiple in $\bar{\mathbb{F}}_p$, e ciò è assurdo, perchè il derivato di $X^n - 1$ è $nX^{n-1} \neq 0$ in $\mathbb{F}_p[X]$, perchè p non divide n. Deve quindi essere $\phi_n(X) = g(X)$.

Vogliamo occuparci ora dell'anello degli interi di $\mathbb{Q}(\zeta_p)$ ove p è un primo razionale. In tal caso $\varphi(p) = p - 1$ e quindi

$$\phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1}.$$

Osserviamo a margine che l'irriducibilità del polinomio $1 + X + \cdots + X^{p-1}$ si può verificare in modo diretto applicando il *Criterio di Eisenstein*(*) al polinomio $\phi_p(X+1) = \sum_{j=1}^{p} \binom{p}{j} X^{j-1}$.

Vogliamo quindi dimostrare la seguente

4.6 Proposizione. *Sia p un primo razionale e ζ una radice p-esima primitiva di 1. Allora la chiusura integrale di $\mathbb{Z}$ in $K = \mathbb{Q}(\zeta)$ è uguale a $\mathbb{Z}[\zeta]$.*

Indicato con Δ il discriminante di $\mathbb{Z}[\zeta]$, (cf. Remark I.3.13), si ha

$$\Delta = \prod_{1 \leq a \neq b \leq p-1} (\zeta^a - \zeta^b) = \prod_{j=1}^{p-1} \phi_p'(\zeta^j).$$

dim. Gli elementi $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$, formano una base di K fatta di elementi interi su $\mathbb{Z}$, possiamo quindi calcolare il discriminante ad essa associato (cf. *Definizione I.3.11*). Si ottiene così il quadrato di un

---

(*) Il Criterio di irriducibilità di Eisenstein si può enunciare nel modo seguente

Teorema. *Il polinomio $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in \mathbb{Z}[X]$ è irriducibile (in $\mathbb{Q}[X]$) se esiste un primo razionale p tale che $p \mid a_j$ per $j = 0, \ldots, n-1$, ma p^2 non divide a_0.*

La dimostrazione procede nel modo seguente. Se f fosse riducibile in $\mathbb{Q}[X]$, per il Lemma di Gauss, si avrebbe $f(X) = g(X)h(X)$ in $\mathbb{Z}[X]$ e quindi, riducendo i coefficienti dei polinomi modulo p, si otterrebbe una fattorizzazione di X^n in $\mathbb{F}_p[X]$. Ciò implica che p dovrebbe dividere il termine noto sia di g che di h e quindi $p^2 \mid a_0$ contro l'ipotesi.

determinante di Van der Monde, ovvero

$$\Delta(1,\zeta,\zeta^2,\dots,\zeta^{p-2}) = \det\begin{pmatrix} 1 & 1 & \dots & 1 \\ \zeta & \zeta^2 & \dots & \zeta^{p-1} \\ \vdots & \vdots & & \vdots \\ \zeta^{p-2} & \zeta^{2(p-2)} & \dots & \zeta^{(p-2)(p-1)} \end{pmatrix}^2 =$$

$$= \left[\prod_{1\le a<b\le p-1}(\zeta^a-\zeta^b)\right]^2 = \prod_{1\le a\ne b\le p-1}(\zeta^a-\zeta^b).$$

Osservando poi che

$$\phi_p(X) = \prod_{i=1}^{p-1}(X-\zeta^i), \qquad \text{e quindi } \phi_p'(X) = \sum_{i=1}^{p-1}\frac{\phi_p(X)}{(X-\zeta^i)},$$

si ottiene $\phi_p'(\zeta^a) = \prod_{i\ne a}^{p-1}(\zeta^a-\zeta^i)$ e quindi

$$\Delta(1,\zeta,\zeta^2,\dots,\zeta^{p-2}) = \prod_{j=1}^{p-1}\phi_p'(\zeta^j).$$

Si osservi poi che $X^p-1=(X-1)\phi_p(X)$ e quindi, derivando ambo i membri si ottiene $pX^{p-1} = \phi_p(X)+(X-1)\phi_p'(X)$, e quindi, calcolando nelle varie potenze di ζ, si ha

$$p\zeta^{a(p-1)} = (\zeta^a-1)\phi_p'(\zeta^a)$$

e si conclude che p è l'unico primo che divide $\Delta = \Delta(1,\zeta,\zeta^2,\dots,\zeta^{p-2}) \in \mathbb{Z}$.

Indichiamo con B la chiusura integrale di $\mathbb{Z}$ in K e ricordiamo che ogni elemento $x\in B$ si scrive nella forma

$$x = \frac{a_0}{\Delta}+\frac{a_1}{\Delta}\zeta+\dots+\frac{a_{p-2}}{\Delta}\zeta^{p-2}, \qquad \text{ove } a_j\in\mathbb{Z}$$

e, posto $\lambda=\zeta-1$, si ha $\mathbb{Z}[\lambda]=\mathbb{Z}[\zeta]$ ed

$$x = \frac{b_0}{\Delta}+\frac{b_1}{\Delta}\lambda+\dots+\frac{a_{b-2}}{\Delta}\lambda^{p-2}, \qquad \text{ove } b_j\in\mathbb{Z}.$$

L'unico fattore primo di Δ è p, possiamo semplificare le frazioni che compaiono come coefficienti nella scrittura di x. Supponiamo quindi di aver ridotto le frazioni e che i coefficienti che ne risultano non siano interi. Questo significa che

$$c_0+c_1\lambda+\dots+c_{p-2}\lambda^{p-2} = p^r x\in pB$$

ove $c_0,c_1,\dots,c_{p-2}\in\mathbb{Z}$, ma non sono tutti divisibili per p. Sia quindi s l'intero per cui

$$\begin{cases} c_0\equiv c_1\equiv\dots\equiv c_{s-1}\equiv 0 \pmod p \\ c_s\not\equiv 0 \pmod p \end{cases}$$

allora, si ha $c_s\lambda^s+\dots+c_{p-2}\lambda^{p-2} = py\in pB$.

Si osservi che

$$p = \phi_p(1) = (1-\zeta)\dots(1-\zeta^{p-2}) = \lambda^{p-1}\prod_{a=1}^{p-1}\frac{1-\zeta^a}{1-\zeta};$$

ed inoltre, per ogni a, $\frac{1-\zeta^a}{1-\zeta}$ è invertibile in B, perchè, scelto un intero b tale che $ab\equiv 1 \pmod p$, si ha

$$\frac{1-\zeta}{1-\zeta^a} = \frac{1-\zeta^a b}{1-\zeta^a} = 1+\zeta^a+\dots+\zeta^{a(b-1)}\in B.$$

Dunque $p=\lambda^{p-1}u$ in B e, dalla relazione $c_s\lambda^s+\dots+c_{p-2}\lambda^{p-2}=py$, si deduce che $\lambda\mid c_s$ in B, ma $c_s\in\mathbb{Z}$ e quindi $p\mid c_s$ che è una contraddizione. Si conclude che deve essere $x=c_0+c_1\lambda+\dots+c_{p-2}\lambda^{p-2}$, ovvero che $B=\mathbb{Z}[\lambda]=\mathbb{Z}[\zeta]$. **CVD** □

Concludiamo questo numero con un osservazione

4.7 Remark. Se L è un'estensione finita di $\mathbb{Q}$, per il Teorema dell'elemento primitivo (cf. *Proposizione I.2.2*), si ha che $L = \mathbb{Q}(y)$, per un opportuno $y \in L$, allora può essere spontaneo chiedersi se anche per la chiusura integrale B di $\mathbb{Z}$ in L, vale un analogo risultato, ovvero se $B = \mathbb{Z}[\alpha]$ per un opportuno intero α, come abbiamo visto accadere per i corpi quadratici e per i corpi ciclotomici (principali). Diciamo subito che la risposta è negativa, come si può vedere dal seguente esempio.

Sia $K = \mathbb{Q}(\sqrt{10}, \sqrt{7})$, allora una base di K su $\mathbb{Q}$ è data da $\{1, \sqrt{7}, \sqrt{10}, \sqrt{70}\}$, che sono interi su $\mathbb{Z}$ ed il discriminante associato a tale base è

$$\Delta = \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ \sqrt{7} & -\sqrt{7} & \sqrt{7} & -\sqrt{7} \\ \sqrt{10} & \sqrt{10} & -\sqrt{10} & -\sqrt{10} \\ \sqrt{70} & -\sqrt{70} & -\sqrt{70} & \sqrt{70} \end{pmatrix}^2 = (1120)^2 = 2^{10}5^2 7^2.$$

Sia ora

$$x = \frac{a}{\Delta} + \frac{b}{\Delta}\sqrt{7} + \frac{c}{\Delta}\sqrt{10} + \frac{d}{\Delta}\sqrt{70} \in B$$

ed osserviamo che, poichè $\Delta \not\equiv 0 \pmod 3$, si ha $x^3 - x \in 3B$ e, con un calcolo diretto, $x^3 - x = 3\frac{\gamma}{\Delta}$ con $\gamma \in B$. Dunque, se fosse $B = \mathbb{Z}[\alpha]$, si avrebbe in particolare

$$\alpha^3 - \alpha = \frac{3g(\alpha)}{\Delta}, \qquad \text{ove } \ g(X) \in \mathbb{Z}[X],$$

ciò è assurdo perchè, uguagliando le due espressioni, dovrebbe aversi che $3 \mid \Delta$.

5. L'equazione di Pell

In questa sezione ci occuperemo di determinare le soluzioni non-banali di un'equazione diofantea. Precisamente, ci interessano le soluzioni intere, diverse da $(\pm 1, 0)$, dell'*equazione di Pell*, ovvero di

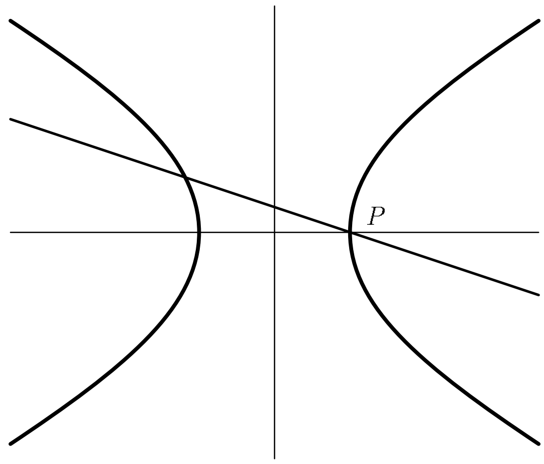
$$X^2 - dY^2 = 1 \qquad \text{con } \ 0 < d \in \mathbb{Z},$$

ove d non è il quadrato di un numero intero[†]. Cominciamo la discussione, osservando che un approccio 'geometrico', simile a quello usato per determinare i numeri pitagorici (cf. *I, §.1*), non porterebbe a risultati utili.

La curva di equazione $X^2 - dY^2 = 1$ è una conica, sia $P = (1, 0)$ un suo punto razionale e si consideri una generica retta passante per P, di equazione $Y = t(X - 1)$. Per quasi tutti i valori di t, questa retta ha un'altra intersezione con la conica e precisamente, deve aversi $0 = X^2 - dt^2(X-1)^2 - 1 = (X-1)[X + 1 - dt^2(X-1)]$, da cui si ottiene la parametrizzazione della curva tramite le funzioni razionali

$$\begin{cases} x = \frac{1+dt^2}{dt^2-1} \\ y = \frac{2t}{dt^2-1} \end{cases}$$

ed in tal modo si possono determinare tutti i punti a coordinate in $\mathbb{Q}$.



(†) Se fosse $d = n^2$, allora l'equazione assumerebbe la forma $(X - nY)(X + nY) = 1$ che ha solo soluzioni banali.

Poniamo quindi $t = \frac{p}{q}$, con $\mathrm{Mcd}(p, q) = 1$, e si ottiene

$$x = \frac{q^2 + dp^2}{dp^2 - q^2}, \quad y = \frac{2pq}{dp^2 - q^2}.$$

La condizione che i punti abbiano coordinate intere può essere espressa nel modo seguente: posto $N = dp^2 - q^2 \in \mathbb{Z}$, deve essere

$$N \mid 2pq \qquad \text{e} \qquad N \mid (q^2 + dp^2) = N + 2q^2.$$

Se $\ell \neq 2$ è un fattore primo di N, allora ℓ deve dividere q^2 e quindi q ed inoltre, essendo $q^2 \equiv dp^2 \pmod N$, con $\mathrm{Mcd}(p, q) = 1$, si ottiene $\ell \mid d$. Inoltre, se ora ℓ è un primo qualsiasi ed $\ell^\alpha \mid N$, con $\alpha \geq 2$, allora $\ell^\alpha \mid q^{2}$(*), ed essendo $dp^2 \equiv q^2 \pmod N$, si conclude che $\ell^\alpha \mid d$.

Dunque i fattori primi di N sono da cercarsi tra i fattori primi di d, con molteplicità non maggiore di quella con cui compaiono in d, con l'eccezione del fattore 2 che potrebbe comparire, con molteplicità al più 1, anche quando d è dispari.

In particolare, dai calcoli fatti, si vede che per determinare i valori del parametro $t = \frac{p}{q}$, con $\mathrm{Mcd}(p, q) = 1$, per cui i punti della conica hanno coordinate in $\mathbb{Z}$, dobbiamo scegliere p e q tra le soluzioni di equazioni del tipo $N = dp^2 - q^2$, ove N è legato a d nel modo descritto sopra. Queste condizioni sono dello stesso ordine di difficoltà del problema di partenza, il che significa che la parametrizzazione della curva $X^2 - dY^2 = 1$, non ci è d'aiuto nella soluzione dell'equazione di Pell.

Cerchiamo quindi un approccio diverso all'equazione di Pell ponendoci nel corpo quadratico $\mathbb{Q}(\sqrt{d})$. Su questo corpo si ha

$$X^2 - dY^2 = (X + \sqrt{d}Y)(X - \sqrt{d}Y)$$

e quindi, se $(x, y) \in \mathbb{Z}^2$ è una soluzione non-banale dell'Equazione di Pell con x ed y entrambi positivi, deve aversi

$$|x - y\sqrt{d}| = \frac{1}{x + y\sqrt{d}} \leq \frac{1}{2y(\sqrt{d} - \varepsilon)}, \quad \text{che scriveremo brevemente } |x - y\sqrt{d}| \lessapprox \frac{1}{2y\sqrt{d}},$$

ove $|-|$ indica il valore assoluto reale e ε è un opportuno numero reale $0 \leq \varepsilon < 1$. Ciò perchè la prima uguaglianza dice che x e $y\sqrt{d}$ differiscono per un numero reale minore di 1 e quindi la loro somma è maggiore del doppio del più piccolo tra i due addendi. In particolare, la disuguaglianza appena stabilita significa che, se $(x, y) \in \mathbb{Z}^2$ è come sopra, si ha

$$\left| \frac{x}{y} - \sqrt{d} \right| \lessapprox \frac{1}{2y^2\sqrt{d}}.$$

È chiaro che, se α è un qualsiasi numero irrazionale, si ha genericamente

$$\min_{x \in \mathbb{Z}} \left| \frac{x}{y} - \alpha \right| \leq \frac{1}{2y};$$

quindi le soluzioni dell'equazione di Pell forniscono *buone approssimazioni* di $\sqrt{d}$ tramite numeri razionali. Occupiamoci quindi in modo più approfondito del problema di trovare buone approssimazioni di numeri irrazionali e cominciamo con il seguente

(*) Se $\ell = 2$, si ha che $2^{\alpha-1} \mid q^2$ e $2^{\alpha-1} \mid pq$; quindi $2^{\alpha-1} \mid q$, perchè $\mathrm{Mcd}(p, q) = 1$, e perciò $2^\alpha \mid 2^{2(\alpha-1)} \mid q^2$, perchè $\alpha \geq 2$.

5.1 Teorema. (Dirichlet) *Siano $\xi \in \mathbb{R} \setminus \mathbb{Q}$ e Q un intero positivo. Allora, esistono degli interi x ed y tali che*

$$\left|\frac{x}{y} - \xi\right| \leq \frac{1}{yQ} \qquad e \qquad 0 < y \leq Q.$$

dim. Si considerino i $Q+1$ numeri reali

$$0, \{\xi\}, \{2\xi\}, \dots, \{Q\xi\} \in [0,1),$$

ove il simbolo $\{x\}$ indica la *parte frazionaria* del numero reale x, ovvero $\{x\} := x - [x]$, ove $[x] = \max\{\, n \in \mathbb{Z} \mid n \leq x \,\}$. Se si considerano i Q intervalli

$$I_n = \left[\frac{n}{Q}, \frac{n+1}{Q}\right), \quad \text{per } n = 0, 1, \dots, Q-1,$$

allora esiste un indice n tale che $\{r\xi\}, \{s\xi\} \in I_n$, per due opportuni interi $r < s$. Si ha perciò

$$\frac{1}{Q} > |\{r\xi\} - \{s\xi\}| = |(s-r)\xi - ([s\xi] - [r\xi])|$$

e quindi, posto $x = [s\xi] - [r\xi] \in \mathbb{Z}$ ed $y = s - r \in \mathbb{Z}_{>0}$, si ha l'approssimazione richiesta nell'enunciato. **CVD** □

Possiamo quindi ricavare una stima sulle 'buone approssimazioni' dei numeri irrazionali (che non vale nel caso di numeri razionali).

5.2 Corollario. *Se $\xi \in \mathbb{R} \setminus \mathbb{Q}$, esistono infinite frazioni $\dfrac{x}{y} \in \mathbb{Q}$, con $\mathrm{Mcd}(x,y) = 1$, tali che*

$$\left|\frac{x}{y} - \xi\right| \leq \frac{1}{y^2}.$$

dim. Se vi fosse un numero finito di tali approssimazioni, siano $\frac{x_1}{y_1}, \dots, \frac{x_n}{y_n}$, si consideri

$$0 < \varepsilon = \min_{1 \leq i \leq n} \left|\frac{x_i}{y_i} - \xi\right|$$

(ove $\varepsilon > 0$ perchè $\xi \notin \mathbb{Q}$). Allora, scelto $Q > \frac{1}{\varepsilon}$, ed applicato il Teorema di Dirichlet, si trova una contraddizione con la minimalità di ε. **CVD** □

5.3 Remark. Facciamo una breve digressione, osservando che il risultato del Corollario precedente può essere migliorato dalla disuguaglianza

$$\left|\frac{x}{y} - \xi\right| \leq \frac{1}{y^2\sqrt{5}}$$

che non è ulteriormente migliorabile. Il problema che ci siamo posti, non è però la buona approssimazione di un generico numero irrazionale, ma di numeri del tipo $\sqrt{d}$ con $d \geq 2$, non quadrato in $\mathbb{Z}$. In particolare, si tratta di numeri algebrici e vogliamo ricordare un risultato fondamentale sulla 'cattiva approssimabilità' dei numeri algebrici tramite numeri razionali, ovvero il seguente

Teorema. (Roth) *Se $\alpha \in \bar{\mathbb{Q}}$ ed $\varepsilon > 0$, vi è un numero finito di soluzioni alla disuguaglianza*

$$\left|\frac{x}{y} - \alpha\right| \leq \frac{1}{y^{2+\varepsilon}}.$$

Questo Teorema migliora risultati precedenti di Thue, Siegel e Dyson, ma non è un risultato effettivo, perchè non dice come determinare le soluzioni e dà solo una stima sul loro numero.

Torniamo al problema iniziale, e consideriamo, in base al *Corollario I.5.2*, le infinite frazioni soddisfacenti alla condizione

$$\left|\frac{x}{y} - \sqrt{d}\right| \leq \frac{1}{y^2} \qquad \text{con} \quad y > 0.$$

Allora, moltiplicando per $y|x + y\sqrt{d}| > 0$, si ottiene la disuguaglianza

$$|x^2 - dy^2| \leq \frac{|x + y\sqrt{d}|}{y} \leq \frac{2y\sqrt{d} + 1}{y} \leq 2\sqrt{d} + 1,$$

ove si è utilizzata l'osservazione

$$|x - y\sqrt{d}| \leq \frac{1}{y} \quad \Rightarrow \quad x < 1 + y\sqrt{d}.$$

Poichè $x^2 - dy^2 \in \mathbb{Z}$ ed esiste un numero finito di interi soddisfacenti alla condizione $n \leq 2\sqrt{d} + 1$, possiamo concludere che esiste un intero M per cui l'equazione $X^2 - dY^2 = M$ ha infinite soluzioni $(x, y) \in \mathbb{Z}^2$.

Da questa osservazione possiamo ricavare informazioni sulle soluzioni dell'equazione di Pell. Sia $K = \mathbb{Q}(\sqrt{d})$ e si consideri il sottoanello $\mathbb{Z}[\sqrt{d}]$; essendovi infinite soluzioni in $\mathbb{Z}^2$ dell'equazione $X^2 - dY^2 = M$ ed essendo $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$ finito, esistono degli elementi

$$\begin{matrix} x + y\sqrt{d}, \\ x' + y'\sqrt{d} \end{matrix} \quad \text{in } \mathbb{Z}[\sqrt{d}] \text{ tali che} \quad \begin{cases} (x + y\sqrt{d})(x - y\sqrt{d}) = M = (x' + y'\sqrt{d})(x' - y'\sqrt{d}) \\ \frac{x}{y} \neq \frac{x'}{y'} \\ x \equiv x' \pmod{M} \\ y \equiv y' \pmod{M} \end{cases} . \tag{5.4}$$

Allora si ha

$$(x + y\sqrt{d})(x' - y'\sqrt{d}) = A + B\sqrt{d} \qquad \text{ed} \qquad (x' + y'\sqrt{d})(x - y\sqrt{d}) = A - B\sqrt{d}$$

con $(A, B) \in \mathbb{Z}^2$, perchè i fattori del secondo prodotto sono i coniugati dei fattori del primo; e quindi

$$A^2 - dB^2 = (x^2 - dy^2)({x'}^2 - d{y'}^2) = M^2. \tag{5.5}$$

Inoltre, dalle ipotesi fatte su $x + y\sqrt{d}$ ed $x' + y'\sqrt{d}$, si ricava

$$\begin{cases} A = xx' - dyy' \equiv x^2 - dy^2 \equiv 0 \pmod{M} \\ B = xy' - yx' \equiv 0 \pmod{M} \end{cases}$$

e quindi $A = MA'$, $B = MB'$, da cui si deduce, in base a (I.5.5), che $(A', B') \in \mathbb{Z}^2$ è una soluzione non banale dell'equazione di Pell.

Possiamo quindi raccogliere le conseguenze della discussione sin qui fatta.

5.6 Proposizione. *Fissato $0 < d \in \mathbb{Z}$ non quadrato in $\mathbb{Z}$, esistono infinite soluzioni non banali $(x, y) \in \mathbb{Z}^2$ dell'equazione $X^2 - dY^2 = 1$.*

6. Complementi. Unità di un corpo quadratico reale.

Le soluzioni dell'equazione di Pell $X^2 - dY^2 = 1$ permettono di determinare delle unità dell'anello degli interi $\mathcal{O}_d$ del corpo quadratico (reale) $\mathbb{Q}(\sqrt{d})$, con $d \geq 2$. Cominciamo con un'osservazione di carattere generale sulle unità.

6.1 Proposizione. *Sia K un'estensione finita di $\mathbb{Q}$ e sia B la chiusura integrale di $\mathbb{Z}$ in K. Un elemento $\xi \in B$ è invertibile in B se, e solo se, $N_{K/\mathbb{Q}}(\xi) = \pm 1$.*

dim. Si osservi che $N_{K/\mathbb{Q}}(\xi) \in \mathbb{Q}$ ed è intero su $\mathbb{Z}$, in quanto prodotto dei coniugati di $\xi \in B$ e quindi, essendo $\mathbb{Z}$ integralmente chiuso, si ha $N_{K/\mathbb{Q}}(\xi) \in \mathbb{Z}$. Inoltre, l'applicazione $N_{K/\mathbb{Q}} : K^\times \to \mathbb{Q}^\times$ è un omomorfismo di gruppi moltiplicativi (cf. *Proposizione I.2.11*) e quindi $N_{K/\mathbb{Q}}(B^\times) \subseteq \mathbb{Z}^\times = \{\pm 1\}$.

Viceversa, dato un elemento $\xi \in B$ con $N_{K/\mathbb{Q}}(\xi) = \pm 1$, si ha che $\xi^{-1} \in K$ è un prodotto di coniugati di ξ, moltiplicato per ± 1, e quindi ξ^{-1} è intero su $\mathbb{Z}$ e perciò appartiene a B. **CVD** □

Tornando all'anello $\mathcal{O}_d$, si ha quindi che l'elemento $x + y\sqrt{d}$ è invertibile se, e solo se,

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2 = \pm 1;$$

in particolare, se (x, y) è soluzione dell'equazione di Pell, allora $x + y\sqrt{d}$ è invertibile in $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_d$.

Studiamo ora più in dettaglio la struttura del gruppo delle unità $\mathcal{O}_d^\times$ e consideriamo perciò l'omomorfismo

$$\Phi : \begin{array}{ccc} \mathcal{O}_d^\times & \to & \mathbb{R} \\ \xi & \mapsto & \log|\xi| \end{array}.$$

Il nucleo di Φ è il sottogruppo $\{\pm 1\}$, mentre l'immagine è un *sottogruppo discreto*(†) del gruppo additivo dei numeri reali. Infatti, fissato $a > 0$, dalla condizione $-a < \log|\xi| < a$ si ricava $e^{-a} < |\xi| < e^a$ e quindi lo stesso vale per il coniugato $\xi' = \frac{1}{\xi}$; ovvero $e^{-a} < |\xi'| < e^a$. Ora $\xi = r + s\sqrt{d} \in \mathcal{O}_d$ e quindi $r, s \in \frac{1}{2}\mathbb{Z}$ (cf. *Proposizione I.4.2*); inoltre, $\xi' = r - s\sqrt{d}$, e perciò deve aversi

$$|r| = \left|\frac{\xi + \xi'}{2}\right| < e^a \qquad \text{e} \qquad |s| = \left|\frac{\xi - \xi'}{2\sqrt{d}}\right| < \frac{e^a}{\sqrt{d}}; \tag{6.2}$$

ed in $\frac{1}{2}\mathbb{Z}$ vi è solo un numero finito di soluzioni per queste due disuguaglianze.

Dunque si ha la sequenza esatta

$$0 \longrightarrow \{\pm 1\} \longrightarrow \mathcal{O}_d^\times \longrightarrow \mathbb{Z} \longrightarrow 0$$

da cui si deduce ($\mathbb{Z}$ è un gruppo libero) che

$$\mathcal{O}_d^\times \cong \{\pm 1\} \times \mathbb{Z}. \tag{6.3}$$

Gli elementi di $O_d^\times$ che si proiettano sui generatori del gruppo ciclico sono dette le *unità fondamentali* dell'anello O_d. Le disuguaglianze (I.6.2) permettono di determinare in modo effettivo un'unità fondamentale, dovendo fare un numero finito di verifiche per determinare r ed s affinchè $\log|r + s\sqrt{d}|$ sia minimo (in valore assoluto).

Vogliamo ora raccogliere alcune osservazioni sull'equazione di Pell e sulle equazioni ad essa collegate.

(†) Un sottogruppo H di $(\mathbb{R}, +)$ si dice *discreto* se, per ogni $\delta > 0$, l'insieme $H \cap (-\delta, \delta)$ ha un numero finito di elementi. In particolare, ogni sottogruppo discreto di $(\mathbb{R}, +)$ è ciclico ed è generato da un qualsiasi elemento di valore assoluto minimo tra gli elementi non-nulli.

6.4 Remark. (Risoluzione effettiva dell'equazione di Pell). Dalla discussione fatta in §.1, sappiamo che esiste un numero intero positivo $M \leq 2\sqrt{d}+1$ per cui l'equazione $X^2 - dY^2 = M$ ha infinite soluzioni intere. Se prendiamo M^2+1 soluzioni di questa equazione troviamo certamente due elementi soddisfacenti alle condizioni (I.5.4), e quindi una soluzione dell'equazione di Pell. Ripercorriamo quindi la costruzione del numero precedente al fine di ottenere un procedimento effettivo, che ci conduca a determinare una soluzione non banale dell'equazione di Pell dopo un numero finito di passi.

Si considerino quindi delle buone approssimazioni di $\sqrt{d}$, ovvero siano $(x_i, y_i) \in \mathbb{Z}^2$, tali che

$$\left|\frac{x_i}{y_i} - \sqrt{d}\right| < \frac{1}{y_i^2}, \qquad \text{per } i = 1, \dots, n, \qquad \text{e sia } 0 < y_1 < y_2 < \dots < y_n.$$

Vogliamo mostrare che si può fissare un intero positivo Q di modo che la buona approssimazione di $\sqrt{d}$ costruita tramite il Teorema di Dirichlet (cf. *Teorema I.5.1*) sia diversa da quelle sin qui determinate. Sia

$$\varepsilon_i = \left|\frac{x_i}{y_i} - \sqrt{d}\right| < \frac{1}{y_i^2}, \qquad \text{per } i = 1, \dots, n,$$

ed osserviamo che, per ogni $i = 1, \dots, n$, si ha

$$1 \leq |x_i^2 - dy_i^2| = |x_i + y_i\sqrt{d}| y_i \varepsilon_i;$$

da cui si ottiene la disuguaglianza

$$\frac{1}{\varepsilon_i} \leq \left|\frac{x_i}{y_i} - \sqrt{d}\right| y_i^2 \leq y_i^2(2\sqrt{d}+1)).$$

In particolare, poichè gli y_i sono crescenti, si ha che

$$\frac{1}{(1+2\sqrt{d})y_n^2} < \varepsilon = \min_{i=1,\dots n} \varepsilon_i.$$

Dunque, se si fissa un intero $Q > (1+2\sqrt{d})y_n^2$, si ottiene tramite il Teorema di Dirichlet una coppia di interi $(x_{n+1}, y_{n+1}) \in \mathbb{Z}^2$, con $1 \leq y_{n+1} \leq Q$, tale che

$$\varepsilon_{n+1} = \left|\frac{x_{n+1}}{y_{n+1}} - \sqrt{d}\right| < \frac{1}{y_{n+1}Q} < \frac{\varepsilon}{y_{n+1}} \leq \varepsilon$$

e quindi si tratta di una buona approssimazione di $\sqrt{d}$, diversa dalle precedenti.

Poichè $Q > (1+2\sqrt{d})y_n^2$, deve essere un intero, una scelta minimale può essere fatta prendendo $Q \leq (2+2\sqrt{d})y_n^2$; ed essendo $y_{n+1} \leq Q \leq (2+2\sqrt{d})y_n^2$, otteniamo così una limitazione effettiva per la grandezza del denominatore y_{n+1} di una nuova buona approsimazione di $\sqrt{d}$ che può quindi essere determinata dopo un numero finito di tentativi(*).

6.5 Remark. (Risoluzione dell'equazione $X^2 - dY^2 = m$). Ci occuperemo ora di descrivere un metodo effettivo per determinare le soluzioni intere dell'equazione $X^2 - dY^2 = m$. Supponiamo che esista una soluzione $(x, y) \in \mathbb{Z}^2$ e che $(u, v) \in \mathbb{Z}^2$ sia una soluzione non banale dell'equazione di Pell, con $u > 0 < v$. Poniamo

$$\alpha = x + y\sqrt{d} \qquad \text{e} \qquad \xi = u + v\sqrt{d},$$

(*) Si è così ottenuta una stima di tipo esponenziale della crescita dei denominatori delle buone approssimazioni di $\sqrt{d}$, ovvero $y_n \leq (2+2\sqrt{d})^{2n}$. Tale stima non è ottimale, ma ricordiamo che una possibile stima ottimale è ancora di tipo esponenziale (cf. ???).

e ricordiamo che ξ è invertibile in $\mathbb{Z}[\sqrt{d}]$ ed il suo inverso è il coniugato (algebrico) $\xi' = u - v\sqrt{d}$; inoltre, indicato con $\alpha' = x - y\sqrt{d}$ il coniugato di α, si ha per costruzione $\alpha\alpha' = m$.

Si consideri l'anello $\mathbb{Z}[\sqrt{d}]$ immerso in $\mathbb{R}$ ($d > 0$) e sia k un intero per cui si abbia

$$\sqrt{\frac{|m|}{\xi}} \leq \frac{\alpha}{\xi^k} < \sqrt{|m|\xi}.$$

Si ponga $\beta = \frac{\alpha}{\xi^k} = x' + y'\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ e, indicato con $\beta' = x' - y'\sqrt{d}$ il suo coniugato algebrico, si ha

$$\beta' = \frac{\alpha'}{\xi'^k} = \frac{m}{\alpha}\xi^k = \frac{m}{\beta},$$

e quindi $\beta\beta' = m$, ovvero (x', y') è una soluzione dell'equazione $X^2 - dY^2 = m$ e si ha

$$|\beta'| \leq \frac{m}{\sqrt{\frac{|m|}{\xi}}} = \sqrt{|m|\xi},$$

da cui si ricava

$$|x'| = \left|\frac{\beta + \beta'}{2}\right| \leq \sqrt{|m|\xi} \quad \text{ed} \quad |y'| = \left|\frac{\beta - \beta'}{2\sqrt{d}}\right| \leq \sqrt{\frac{|m|\xi}{d}}. \tag{6.6}$$

Dunque, se esiste una soluzione dell'equazione $X^2 - dY^2 = m$ esiste anche una soluzione della stessa equazione, le cui coordinate sono limitate da una grandezza che dipende solo da m, d e da una qualsiasi soluzione non banale dell'equazione di Pell. L'insieme delle soluzioni dell'equazione $X^2 - dY^2 = m$ soddisfacenti alle condizioni (I.6.6) è un insieme finito e dunque l'equazione $X^2 - dY^2 = m$ ha soluzioni in $\mathbb{Z}^2$ se, e solo se, vi sono soluzioni (x', y'), soddisfacenti alle condizioni (I.6.6). Inoltre, ogni soluzione di tale equazione si ottiene da una di quelle soddisfacenti alle condizioni dette e da un'opportuna potenza di $\xi = u + v\sqrt{d}$, ove $(u, v) \in \mathbb{Z}^2$ è una soluzione non banale dell'equazione di Pell.

6.7 Remark. [*Soluzioni intere e congruenze*] Consideriamo l'equazione a coefficienti interi $X^2 - dY^2 = m$. Per ogni intero positivo N, possiamo considerare la congruenza $X^2 - dY^2 \equiv m \pmod N$ e ci chiediamo che relazioni ci siano tra eventuali soluzioni intere dell'equazione e le soluzioni delle congruenze, al variare di N. È ovvio che, se $(x, y) \in \mathbb{Z}^2$ è una soluzione dell'equazione allora, riducendo modulo N, si ottiene una soluzione a ciascuna delle congruenze. Però, l'esistenza di soluzioni alle congruenze per ogni N è una condizione necessaria, ma non sufficiente per l'esistenza di soluzioni intere dell'equazione di partenza(*). Infatti, si potrebbe mostrare (ma non lo faremo) che l'equazione $X^2 - 82Y^2 = 2$ non ha soluzioni intere, mentre le congruenze ad essa associate sono risolubili per ogni intero N.

Dimostriamo quindi il seguente risultato sulla risoluzione di congruenze.

6.8 Proposizione. *Siano d ed $m \geq 2$ due interi. Allora esiste $p_0 = p_0(m, d)$ tale che*
(i) se $p > p_0$, la congruenza $x^2 - dy^2 \equiv m \pmod{p^h}$ ha soluzione per ogni h;
(ii) se $p \leq p_0$ esiste un esponente h_0 tale che la congruenza $x^2 - dy^2 \equiv m \pmod{p^h}$ ha soluzione per ogni h se, e solo se la congruenza ha soluzione per $h = h_0$.

dim. Sia $h = 1$. e si osservi che in tal caso la congruenza $x^2 - dy^2 \equiv m \pmod p$ ha soluzione. Se $p = 2$, è una verifica immediata; se p è dispari, si può osservare che le due funzioni $x \mapsto x^2$ ed $y \mapsto m + dy^2$ assumono entrambe $\frac{p+1}{2}$ valori distinti in $\mathbb{F}_p$; quindi ci sono almeno due valori coincidenti, ovvero una soluzione della congruenza. Inoltre, posto $f(X, Y) = X^2 - dY^2 - m \in \mathbb{Z}[X]$, si ha

$$\frac{\partial f}{\partial X} = 2X \qquad \text{e} \qquad \frac{\partial f}{\partial Y} = -2dY;$$

quindi il risultato è una conseguenza del lemma qui sotto, per enunciare il quale introduciamo la notazione $p^r \parallel n$ per indicare che p^r è la massima potenza di p che divide l'intero n.

(*) Vedremo nella seconda parte del corso come la condizione diventi necessaria e sufficiente per i polinomi omogenei di secondo grado (forme quadratiche) in forza del Teorema di Hasse-Minkowsky.

6.9 Lemma. *Siano $f(\underline{X}) \in \mathbb{Z}[X_1, \dots, X_n]$ e p un primo razionale. Supponiamo che esista una n-upla di interi $\underline{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$ per cui*

$$p^c \parallel \mathrm{Mcd}(\tfrac{\partial f}{\partial x_1}(\underline{a}), \dots, \tfrac{\partial f}{\partial x_n}(\underline{a})), \qquad p^b \parallel f(\underline{a}), \qquad b > 2c.$$

Allora la congruenza $f(\underline{x}) \equiv 0 \pmod{p^h}$ ha soluzioni per ogni esponente h.

dim. Per ipotesi, si ha $f(\underline{a}) \equiv 0 \pmod{p}^b$. Quindi supponiamo che per un intero positivo h, esista $\underline{b} \in \mathbb{Z}^n$ tale che

- $f(\underline{b}) = p^h\delta$, e $p \not| \delta$;
- $\frac{\partial f}{\partial x_1}(\underline{b}) = p^c\xi_i$ per $i = 1, \dots, n$, ove $p \not| \xi_i$ per qualche i;
- $h > 2c$.

Sotto tali ipotesi, mostriamo che esistono degli interi $q_1, \dots, q_n$ ed un esponente μ tali che $\underline{b}^* = \underline{b} + p^\mu \underline{q}$ sia una soluzione della congruenza $f(\underline{b}^*) \equiv 0$ per una potenza di p di esponente superiore ad h e che siano ancora soddisfatte le condizioni scritte sopra con $\underline{b}^*$ in luogo di $\underline{b}$.

Applicando la Formula di Taylor al polinomio f calcolato in $\underline{b}^*$, si ottiene

$$f(\underline{b}^*) = f(\underline{b}) + p^\mu \sum_{i=1}^n q_i \frac{\partial f}{\partial X_i}(\underline{b}) = p^h\delta + p^{\mu+c}\sum_{i=1}^n q_i\xi_i.$$

Quindi, posto $\mu = h - c > c$, poichè gli ξ_i non sono tutti nulli modulo p, si possono trovare degli opportuni q_i per cui si abbia

$$f(\underline{b}^*) = p^h\left(\delta + \sum_{i=1}^n q_i\xi_i\right) \equiv 0 \pmod{p^{2\mu}}$$

e $2\mu = 2h - 2c > 2h - h = h$. Inoltre, poichè $\mu > c$, si ha si ha

$$\frac{\partial f}{\partial X_i}(\underline{b}^*) \equiv \frac{\partial f}{\partial X_i}(\underline{b}) \pmod{p^{c+1}},$$

e quindi si ha ancora

$$p^c \parallel \mathrm{Mcd}(\tfrac{\partial f}{\partial X_1}(\underline{b}^*), \dots, \tfrac{\partial f}{\partial X_n}(\underline{b}^*));$$

e $2\mu > h > 2c$. Quindi la costruzione può proseguire per esponenti arbitrariamente grandi di p. **CVD** □

Ciò conclude anche la dimostrazione della Proposizione.

6.10 Remark. (Risoluzione della generica equazione di secondo grado). Nell'osservazione precedente, abbiamo descritto un metodo effettivo per determinare se l'equazione $X^2 - dY^2 = m$ abbia soluzioni intere. Vogliamo ora occuparci di determinare soluzioni intere dell'equazione

$$aX^2 + bXY + cY^2 + dX + eY + f = 0 \tag{6.11}$$

a coefficienti interi e con $a \neq 0$ (a meno di facili cambiamenti di variabile, si vede che questa condizione non è restrittiva). Se si considerano i polinomi

$$\begin{cases} T = 2aX + bY + d \\ U = (b^2 - 4ac)Y + bd - 2ae \end{cases}$$

e si pone

$$\alpha = b^2 - 4ac, \qquad \beta = bd - 2ae, \qquad \gamma = 4af - d^2,$$

allora, le soluzioni intere (x, y) di (I.6.11), sono in corrispondenza con i numeri $(u, t) \in \mathbb{Z}^2$ soddisfacenti alle condizioni

$$\begin{cases} u^2 - \alpha t^2 = \beta^2 + \alpha\gamma \\ u \equiv \beta \pmod{\alpha} \\ \alpha t \equiv b(u - \beta) + \alpha d \end{cases} .$$

Sappiamo dalla discussione precedente che, se $\alpha > 0$ e non è un quadrato in $\mathbb{Z}$, le soluzioni (u, t) dell'equazione $u^2 - \alpha t^2 = \beta^2 + \alpha\gamma$ sono in corrispondenza con gli elementi $u + t\sqrt{\alpha} \in \mathbb{Z}[\sqrt{\alpha}]$ del tipo $u + t\sqrt{\alpha} = \lambda_i \xi^k$, ove λ_i varia in un opportuno insieme finito di soluzioni, e $\xi = x_0 + y_0\sqrt{\alpha}$, soddisfa alla condizione $\xi\xi' = 1$, ove con ξ' indichiamo il coniugato algebrico di ξ.

Osserviamo che, modulo l'ideale $J = 2a\alpha\mathbb{Z}[\sqrt{d}]$, vi è solo un numero finito di potenze di ξ distinte, perchè l'anello $\mathbb{Z}[\sqrt{d}]/J$ è finito; quindi, devo verificare su un numero finito di soluzioni dell'equazione $u^2 - \alpha t^2 = \beta^2 + \alpha\gamma$ se sono soddisfatte le congruenze scritte sopra e quindi si ha così una procedura effettiva per verificare se la generica equazione di secondo grado ha soluzioni intere.

Notiamo a margine di questa discussione che, più in generale, non esistono analoghe procedure per determinare le soluzioni intere di equazioni algebriche di grado elevato. In generale è vero che, se $f(X, Y) \in \mathbb{Z}[X, Y]$ è un polinomio assolutamente irriducibile, allora l'equazione $f(X, Y) = 0$ si può risolvere in $\mathbb{Z}$ se, e solo se, il genere della curva è 0 oppure 1.

Concludiamo questa sezione osservando come le osservazioni fatte in questo numero per i corpi quadratici reali si generalizzino ad estensioni finite di $\mathbb{Q}$.

Sia dunque K un'estensione finita di $\mathbb{Q}$, di grado n, e supponiamo che delle n immersioni di K in $\mathbb{C}$ (cf. *Proposizione I.2.3*), ve ne siano r_1 la cui immagine è contenuta in $\mathbb{R}$, mentre le rimanenti $2r_2$ hanno elementi non reali nell'immagine(*). Allora, se indichiamo con $\mathcal{O}_K$ la chiusura integrale di $\mathbb{Z}$ in K, si ha ancora che il gruppo delle unità è (cf. *Proposizione I.6.1*)

$$\mathcal{O}_K^\times = \{\, x \in \mathcal{O} \mid N_{K/\mathbb{Q}}(x) = 1 \,\}.$$

Inoltre, il Teorema di Dirichlet si può estendere(†) e mostrare che

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1} \qquad \text{ove } \mu_K = \{\, x \in K \mid x^r = 1,\ \exists r \geq 1 \,\}. \tag{6.12}$$

Osserviamo infine che, analogamente al caso dei corpi quadratici, dopo aver fissato una base intera di $\mathcal{O}$, la determinazione di elementi $x \in \mathcal{O}$ tali che $N_{K/\mathbb{Q}}(x) = 1$ oppure $N_{K/\mathbb{Q}}(x) = 1 = m$, si trasforma nel problema di determinare le soluzioni intere di una certa funzione polinomiale a coefficienti interi in n indeterminate e queste sono la generalizzazione dell'equazione di Pell e dell'equazione $X^2 - dY^2 = m$.

(*) Le immersioni non-reali sono in numero pari perchè per ogni tale immersione $\sigma : K \to \mathbb{C}$ viè anche l'immersione $\bar{\sigma}$, ottenuta componendo σ con il coniugio di $\mathbb{C}$; ed è ovviamente diversa da σ perchè $\sigma(K) \not\subset \mathbb{R}$.

(†) Per una dimostrazione di (I.6.12) si veda ad esempio H. Hida *Elementary Theory of L-functions and Eisenstein series*, Cambridge Univ. Press 1993, § 1.2.

7. Corpi finiti. Reciprocità quadratica.

In questa sezione vogliamo raccogliere alcune proprietà fondamentali dei corpi finiti e delle loro estensioni. La prima osservazione è contenuta nel seguente

7.1 Teorema. (Wedderburn) *Ogni corpo finito è commutativo.*

dim. Sia F un corpo finito e sia Z il suo centro, ovvero $Z = \{\, x \in F \mid xy = yx\, \forall y \in F \,\}$. Allora Z è un corpo commutativo (campo) con un numero finito di elementi, sia $\sharp(Z) = q$. In particolare, F è uno spazio vettoriale su Z e quindi si ha $\sharp(F) = q^n$, ove $n = \dim_Z F$. Consideriamo su $F^\times$ la relazione di equivalenza (coniugio)

$$x \sim y \quad \Longleftrightarrow \quad y = zxz^{-1}\ \exists z \in F;$$

ed indichiamo con $C_1, \dots, C_r$ le classi di coniugio in $F^\times$. In particolare, si ha

$$\sharp(F^\times) = q^n - 1 = \sum_{i=1}^{r} \sharp(C_i),$$

e quindi cerchiamo di stimare il numero di elementi contenuti in una classe di coniugio C_i. Ciò significa, fissato qualunque elemento x di tale classe, determinare il numero di elementi distinti contenuti nell'immagine dell'applicazione $y \mapsto yxy^{-1}$ ed è immediato verificare che $yxy^{-1} = zxz^{-1}$ se, e solo se, $z = yt$, per un qualche $t \in Z^*(x)$, ove $Z^*(x) = \{\, u \in F^\times \mid ux = xu \,\}$ è il centralizzatore di x. Ora $Z^*(x) \cup (0)$ è un sottocampo di F che contiene Z, quindi

$$\sharp(C_i) = \frac{\sharp(F^\times)}{\sharp(Z^*(x))} = \frac{q^n - 1}{q^{\delta(x)} - 1},$$

ove $\delta(x) = \dim_Z(Z^*(x) \cup (0)) \mid n$. Si conclude che, scelti dei rappresentanti $x_1, \dots, x_r$ in ogni classe di coniugio, si ha

$$q^n - 1 = \sum_{i=1}^{r} \frac{q^n - 1}{q^{\delta(x_i)} - 1} = q - 1 + \sum_{i=q}^{r} \frac{q^n - 1}{q^{\delta(x_i)} - 1},$$

ove abbiamo supposto che le prime $q - 1$ classi siano quelle contenenti gli elementi non nulli del centro Z di F.

Sia ora $\phi_n(X)$ il polinomio ciclotomico di ordine n, allora, $\phi_n(X) \mid (X^n - 1)$, e $(\phi_n(X), X^m - 1) = 1$ per $m < n$, perchè $\phi_n(X) = \prod_{i=1}^{\varphi(n)} (X - \zeta_i)$ ove $\zeta_1, \dots, \zeta_{\varphi(n)}$ sono tutte e sole le radici n-esime primitive di 1 (cf. I.4.4). Dunque, se δ è uno qualunque dei $\delta(x_i)$, per $i = q, \dots, r$, poichè $\delta \mid n$, si ha

$$\frac{X^n - 1}{X^\delta - 1} = \phi_n(X)\psi(X) \qquad \text{ove } \psi(X) \in \mathbb{Z}[X].$$

Ciò è vero per ciascuno dei quozienti $\frac{X^n - 1}{X^{\delta(x_i)} - 1}$ e, perciò $\phi_n(q)$ divide ciascuno dei quozienti $\frac{q^n - 1}{q^\delta - 1}$ e divide $q^n - 1$, si conclude che divide $q - 1$ e ciò è assurdo se $n > 1$, perchè

$$|\phi_n(q)| = \prod_{i=1}^{\varphi(n)} |q - \zeta_i| \geq (q - 1)^{\varphi(n)},$$

essendo, per ogni i. $|q - \zeta_i| \geq |q| - |\zeta_i| = q - 1$. **CVD** □

Un'altra osservazione fondamentale è la seguente.

7.2 Teorema. *Sia F un campo finito. Il gruppo moltiplicativo $F^\times$ è ciclico.*

dim. Sia $x \in F^\times$ un elemento di ordine massimo e sia N il suo ordine. Allora, preso comunque $y \in F^\times$, l'ordine M di y deve dividere l'ordine di x; infatti, se fosse $M = \ell^a M_1$ ed $N = \ell^b M_1$, ove ℓ è un primo razionale, $\ell \not| N_1$ e $0 \le b < a$ sono numeri interi; si avrebbe che l'ordine di $y^{M_1} x^{\ell^b}$ sarebbe divisibile sia per ℓ^a che per N_1, ed essendo coprimi, l'ordine dovrebbe essere divisibile per $\ell^a N_1 > N$, contro l'ipotesi che N sia il massimo ordine.

Dunque, se $N = MK$, $(K \in \mathbb{Z})$, allora sia y che x^{jK}, per $j = 0, \dots, M-1$, sono elementi di F che soddisfano all'equazione $X^M = 1$, e tale equazioni ha al più M radici distinte nel corpo F. Si conclude che $y = x^{jK}$, per qualche $j = 0, \dots, M-1$, visto che le potenze di x con esponenti compresi tra 0 ed $N-1$ sono tutte distinte. Si conclude che x è un generatore di $F^\times$. **CVD** □

Possiamo trarre le prime conseguenze dei due Teoremi testé dimostrati sulla struttura dei corpi finiti.

7.3 Remark. Un campo finito F, di caratteristica $p > 0$, è uno spazio vettoriale di dimensione finita sul campo primo $\mathbb{F}_p$ e quindi il numero di elementi di F è $q = p^n$ e tutti gli elementi di $F^\times$ sono radici del polinomio $X^{q-1} - 1$. Si conclude che gli elementi di F sono tutte e sole le radici dell'equazione $X^q - X$ (a coefficienti in $\mathbb{F}_p$) e quindi, in una chiusura algebrica di $\mathbb{F}_p$, vi è un unico campo finito con q elementi e perciò F è un'estensione normale e separabile di $\mathbb{F}_p$ (cf. I.2.5).

D'ora in poi, indicheremo con $\mathbb{F}_q$, il campo con q elementi. Osserviamo che $\mathbb{F}_q \subset \mathbb{F}_{q^m}$, per ogni intero $m \ge 1$, ed un automorfismo di $\mathbb{F}_{q^m}$, che lasci fisso $\mathbb{F}_q$ è $\phi_q : x \mapsto x^q$. Dunque $\phi_q \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ e questo gruppo ha ordine $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$ (cf. I.2.7); poichè l'ordine di ϕ_q è esattamente m (come si verifica applicandolo ripetutamente ad un generatore del gruppo ciclico $\mathbb{F}_{q^m}^\times$), si conclude che $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ è *un gruppo ciclico, generato da ϕ_q*.

La struttura dei campi finiti (e delle loro estensioni) ha delle interessanti applicazioni. Ad esempio, da ciò si deduce che *esistono polinomi irriducibili in $\mathbb{Z}[X]$ la cui riduzione ad $\mathbb{F}_p[X]$ è invece riducibile per $p \gg 0$*. Infatti, se si considera l'estensione biquadratica $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, ove b, a e b/a non siano quadrati in $\mathbb{Q}$, si verifica facilmente che un elemento primitivo per tale estensione (cf. I.2.2) è $\sqrt{a} + \sqrt{b}$, che soddisfa ad un polinomio irriducibile, di grado 4. Ma aggiungere $\sqrt{a}$ e $\sqrt{b}$ al campo $\mathbb{F}_p$, per $p \gg 0$, non produce un'estensione di grado maggiore di 2, perchè vi è un'unica estensione di grado 2 in una chiusura algebrica $\bar{\mathbb{F}}_p$. Però ricordiamo che *se $f(X) \in \mathbb{Z}[X]$ è irriducibile e di grado > 1, allora esistono infiniti primi p tali che f non abbia radici in $\mathbb{F}_p$*.

Consideramo ora un'altra applicazione. Sia $f(X) = X^3 + aX + b$ un polinomio irriducibile sul campo K ed indichiamo con $\Delta = -4a^3 - 27b^2$ il suo discriminante. Se α_1, α_2, α_3 sono le radici di $f(X)$, ci chiediamo quando accade che $K(\alpha_1)$ sia il corpo di decomposizione di $f(X)$. Ciò è equivalente a chiedere che $K(\alpha_1)$ sia normale su K e, ciò corrisponde a chiedere che $u = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ sia in $K(\alpha_1)$ e, ricordando che $u^2 = \Delta \in K$ e che $[K(\alpha_1) : K] = 3$, si conclude u deve appartenere a K, ovvero che *$K(\alpha_1)$ è normale se, e solo se, Δ è un quadrato in K*.

Ogni estensione di un corpo finito è normale e quindi possiamo enunciare il seguente

7.4 Corollario. *Siano a e b due interi tali che la riduzione di $X^3 + aX + b$ sia irriducibile in $\mathbb{F}_p[X]$. Allora $-4a^3 - 27b^2$ è un quadrato in $\mathbb{F}_p$.*

Il seguito di questa sezione sarà dedicato alla determinazione dei quadrati nei corpi primi. Precisamente, fissato un primo razionale $p > 2$, vogliamo determinare quando accade che un numero intero a è un quadrato in $\mathbb{F}_p$[(†)]. Cominciamo con una definizione.

7.5 Definizione. Diremo che l'intero a è un *residuo quadratico* modulo p, se si può risolvere la congruenza $x^2 \equiv a \pmod{p}$.

(†) È immediato verificare che ogni elemento di un corpo finito di caratteristica 2 è un quadrato, perchè, in tal caso, l'applicazione $x \mapsto x^2$ è un omomorfismo iniettivo.

Al variare di a in $\mathbb{Z}$ si definisce la funzione

$$[\textit{Simbolo di Legendre}] \qquad \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } a \equiv 0 \pmod p \\ 1 & \text{se } a \text{ è residuo quadratico modulo } p \\ -1 & \text{se } a \text{ non è residuo quadratico modulo } p \end{cases} .$$

Richiamiamo di seguito le proprietà del simbolo di Legendre.

- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ e $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, come si verifica direttamente dalla definizione(*). In particolare, da quanto visto si deduce che

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} -1 & \text{se } p \equiv 3 \pmod 4 \\ 1 & \text{se } p \equiv 1 \pmod 4 \end{cases} \tag{7.6}$$

  e quindi non ci resta che calcolare il valore del simbolo di Legendre sui primi razionali. Per quanto riguarda 2, si può fare un calcolo diretto.

- $\left(\frac{2}{p}\right) = 1$ se, e solo se, $p \equiv \pm 1 \pmod 8$. Per dimostrarlo possiamo ragionare come segue. Indichiamo con i una radice quarta primitiva di 1 in $\bar{\mathbb{F}}_p$ ed osserviamo che $(1+i)^2 = 2i$ e quindi in $\bar{\mathbb{F}}_p$ si ha

$$\left(\frac{2}{p}\right) i^{\frac{p-1}{2}} = (2i)^{\frac{p-1}{2}} = (1+i)^{p-1}$$

  e quindi, moltiplicando ambo i membri per $(1+i)$, si ottiene

$$\left(\frac{2}{p}\right) = \frac{1+i^p}{i^{\frac{p-1}{2}}(1+i)} = \begin{cases} -1 & \text{se } p \equiv \pm 3 \pmod 8 \\ 1 & \text{se } p \equiv \pm 1 \pmod 8 \end{cases} . \tag{7.7}$$

Resta quindi da calcolare il valore del simbolo di Legendre sui primi dispari ed il risultato fondamentale in questo senso è dato dalla legge di reciprocità quadratica, ovvero

7.8 Teorema. [Gauss] *Siano p ed ℓ due primi dispari allora*

$$\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} \left(\frac{p}{\ell}\right).$$

dim. Sia $\phi_\ell(X) \in \mathbb{Z}[X]$ il polinomio ciclotomico di ordine ℓ (cf. I,§.4) ed indichiamo con $f(X)$ la sua riduzione ad $\mathbb{F}_p[X]$. Sia ζ una radice di $\phi_\ell(X)$ e si considerino

$$D = \prod_{1 \le b < a \le \ell-1} (\zeta^a - \zeta^b) \qquad \text{e} \qquad \Delta = D^2 = (-1)^{\frac{(\ell-1)(\ell-2)}{2}} \prod_{1 \le b \neq a \le \ell-1} (\zeta^a - \zeta^b)$$

ed osserviamo che, essendo ℓ dispari, $\frac{(\ell-1)(\ell-2)}{2}$ ha la stessa parità di $\frac{\ell-1}{2}$ e quindi si può semplificare l'esponente di -1.

Supponiamo vero il seguente

Claim. $\left(\frac{\Delta}{p}\right) = \left(\frac{p}{l}\right)$

(*) Si può osservare che, si ha la sequenza esatta di gruppi moltiplicativi

$$1 \longrightarrow (\mathbb{F}_p^\times)^2 \longrightarrow \mathbb{F}_p^\times \xrightarrow{\psi} \{\pm 1\} \longrightarrow 1$$

ove $\psi(x) = x^{\frac{p-1}{2}}$; e inoltre, se $\mathbb{Z} \ni a \not\equiv 0 \pmod p$, il simbolo di Legendre di a coincide con l'immagine tramite ψ della riduzione $\bar{a} \in \mathbb{F}_p$ di a.

Ed osserviamo che da questa uguaglianza si deduce la tesi con un calcolo diretto; infatti, si ha

$$\Delta = (-1)^{\frac{\ell-1}{2}} \prod_{1\le b\ne a\le \ell} (\zeta^a - \zeta^b) = (-1)^{\frac{\ell-1}{2}} \prod_{a=1}^{\ell-1} \zeta^a \prod_{\substack{c=1\\ c\not\equiv -a \pmod{\ell}}}^{\ell-1} (1-\zeta^c)$$

e, moltiplicando e dividendo per uno stesso fattore, si ottiene

$$\Delta = (-1)^{\frac{\ell-1}{2}} \prod_{a=1}^{\ell-1} \frac{\zeta^a}{1-\zeta^{-a}} \prod_{c=1}^{\ell-1}(1-\zeta^c) = (-1)^{\frac{\ell-1}{2}} \ell^{\ell-2}$$

ove si osservi che

$$\ell = \phi_\ell(1) = \prod_{c=1}^{\ell-1}(1-\zeta^c) = \prod_{a=1}^{\ell-1}(1-\zeta^{-a}) \quad \text{e} \quad \prod_{a=1}^{\ell-1}\zeta^a = \zeta^{\frac{\ell(\ell-1)}{2}} = 1.$$

Dunque, dall'uguaglianza $\left(\frac{\Delta}{p}\right) = \left(\frac{p}{l}\right)$, si deduce

$$\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{\ell-1}{2}}\ell^{\ell-2}}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}} \left(\frac{\ell}{p}\right)^{\ell-2} = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} \left(\frac{\ell}{p}\right),$$

perchè $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ ed $\ell - 2$ è dispari.

Occupiamoci quindi di dimostrare il **Claim** e consideriamo $\left(\frac{\Delta}{p}\right)$. Nelle notazioni dell'inizio della dimostrazione, si ha che Δ è un quadrato in $\mathbb{F}_p$ se, e solo se, $D \in \mathbb{F}_p$, ovvero se, e solo se, $\phi_p(D) = D$ ove ϕ_p è l'endomorfismo di Frobenius di $\mathbb{F}_p$ (cf. *Remark I.7.3*). Consideriamo quindi il polinomio ridotto $f(X) \in \mathbb{F}_p[X]$, e sia $\mathbb{F}_q$ il suo campo di decomposizione, con $q = p^r$. Ogni elemento di $\mathbb{F}_q^\times$, è una radice del polinomio $X^{q-1} - 1$, e quindi deve aversi che $\ell \mid (p^r - 1)$ ed r è il minimo esponente di p per cui si ha questa divisibilità. Ciò significa che i fattori irriducibili di $f(X)$ in $\mathbb{F}_p[X]$ sono tutti dello stesso grado r, ovvero

$$f(X) = f_1(X)\dots f_s(X), \qquad \text{con } \deg f_i(X) = r, \text{ per } i = 1,\dots,s, \quad \text{ed } rs = \ell - 1.$$

L'endomorfismo ϕ_p agisce sui fattori di D come una permutazione e, per quanto visto, questa permutazione deve essere il prodotto di s-cicli di ordine r, ovvero si ha

$$\operatorname{sgn}\phi_p = (-1)^{(r+1)s} = (-1)^{(\ell-1)+s} = (-1)^s$$

e dunque Δ è un quadrato in $\mathbb{F}_p$ se, e solo se, s è pari, ovvero

$$\left(\frac{\Delta}{p}\right) = (-1)^s;$$

quindi dobbiamo dimostrare che $\left(\frac{p}{\ell}\right) = 1$ se, e solo se, s è pari. Sia $\mathbb{F}_\ell^\times = \langle g\rangle$ e sia $\bar{p} = g^h$; dunque p è un quadrato in $\mathbb{F}_\ell$ se, e solo se, h è pari. Ricordiamo che $\ell \mid (p^r - 1)$ e quindi $g^{hr} = 1$, da cui si deduce che $rs = \ell - 1 \mid rh$ e quindi $s \mid h$. Dunque, se s è pari anche h lo è. Se s fosse dispari e $h = ks$ pari, allora anche r dovrebbe essere pari, perchè il prodotto $rs = \ell - 1$ lo è, e quindi si avrebbe

$$\ell - 1 = rs \mid \frac{rh}{2} = \frac{r}{2}h,$$

contro l'ipotesi che r sia il minimo intero che soddisfa alla condizione $g^{hr} = 1$. Ciò conclude la dimostrazione. **CVD** $\square$

7.9 Remark. [*Un'altra dimostrazione della reciprocità quadratica*] Riportiamo un'altra possibile dimostrazione del *Teorema I.7.8* basata sulla costruzione, tramite una somma di Gauss, di una radice di $\pm\ell$ in una chiusura algebrica di $\mathbb{F}_p$. Sia quindi $\bar{\mathbb{F}}_p$ una chiusura algebrica di $\mathbb{F}_p$ e sia $\omega \in \bar{\mathbb{F}}_p$ una radice ℓ-esima primitiva di 1. Si consideri l'elemento (somma di Gauss)

$$y = \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \omega^x \in \bar{\mathbb{F}}_p;$$

allora si ha

(i) $y^2 = (-1)^{\frac{\ell-1}{2}}\ell$;
(ii) $y^{p-1} = \left(\frac{p}{\ell}\right)$;

e da queste proprietà si deduce la legge di reciprocità quadratica con un calcolo diretto. Dimostriamo quindi gli asserti enunciati sopra. Per quanto riguarda *(i)*, dalla moltiplicatività del simbolo di Legendre, si deduce

$$y^2 = \left[\sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \omega^x\right]^2 = \sum_{x,z\in\mathbb{F}_\ell} \left(\frac{xz}{\ell}\right) \omega^{x+z} = \sum_{t\in\mathbb{F}_\ell} \omega^t \sum_{u\in\mathbb{F}_\ell} \left(\frac{u(t-u)}{\ell}\right).$$

Inoltre, possiamo supporre $u \in \mathbb{F}_\ell^\times$ e si ha

$$\left(\frac{u(t-u)}{\ell}\right) = \left(\frac{-u^2}{\ell}\right)\left(\frac{1-u^{-1}t}{\ell}\right) = (-1)^{\frac{\ell-1}{2}}\left(\frac{1-u^{-1}t}{\ell}\right);$$

e

$$\sum_{u\in\mathbb{F}_\ell^\times} \left(\frac{u(t-u)}{\ell}\right) = (-1)^{\frac{\ell-1}{2}} \sum_{u\in\mathbb{F}_\ell^\times} \left(\frac{1-u^{-1}t}{\ell}\right) = (-1)^{\frac{\ell-1}{2}} \begin{cases} \displaystyle\sum_{u\in\mathbb{F}_\ell^\times} \left(\frac{1}{\ell}\right) = \ell - 1 & \text{se } t = 0 \\ \displaystyle -\left(\frac{1}{\ell}\right) + \sum_{s\in\mathbb{F}_\ell^\times} \left(\frac{s}{\ell}\right) = -1 & \text{se } t \neq 0 \end{cases}.$$

Dunque, possiamo concludere che

$$y^2 = (-1)^{\frac{\ell-1}{2}} \left[\ell - 1 - \sum_{t\in\mathbb{F}_\ell^\times} \omega^t\right] = (-1)^{\frac{\ell-1}{2}}\ell,$$

essendo $\displaystyle\sum_{t\in\mathbb{F}_\ell^\times} \omega^t = \left[\sum_{t\in\mathbb{F}_\ell} \omega^t\right] - \omega^0 = -1$. Ciò conclude la dimostrazione di *(i)*.

Per quanto riguarda *(ii)*, basta ricordare che $\phi_p : a \mapsto a^p$ è un automorfismo in ogni estensione finita di $\mathbb{F}_p$ per concludere che

$$y^p = \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \omega^{xp} = \sum_{z\in\mathbb{F}_\ell} \left(\frac{zp^{-1}}{\ell}\right) \omega^z = \left(\frac{p^{-1}}{\ell}\right) y = \left(\frac{p}{\ell}\right) y.$$

Dunque, mettendo insieme *(i)* e *(ii)*, si conclude

$$\left(\frac{p}{\ell}\right) = y^{p-1} = \left[(-1)^{\frac{\ell-1}{2}}\ell\right]^{\frac{p-1}{2}} = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \left(\frac{\ell}{p}\right).$$

Infine, vogliamo osservare che presa in luogo di $\omega \in \bar{\mathbb{F}}_p$, una radice ℓ-esima primitiva di 1, $\zeta_\ell \in \bar{\mathbb{Q}}$, e posto

$$\eta = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \zeta_\ell^x \in \mathbb{Z}[\zeta_p],$$

si ottiene con calcoli analoghi a quelli fatti sopra, che $\mathbb{Q}(\sqrt{\ell}) \subseteq \mathbb{Q}(\zeta_p)$ e questo è un caso particolare di un importante risultato (cf. ??? per la dimostrazione):

Teorema. [Kronecker-Weber] *Ogni estensione abeliana di $\mathbb{Q}$ è ciclotomica.*

7.10 Remark. [*Irriducibilità di $\phi_\ell(X) \in \mathbb{Z}[X]$*] Possiamo usare alcune delle considerazioni fatte nella dimostrazione del *Teorema I.7.8* per ottenere un'altra dimostrazione dell'irriducibilità in $\mathbb{Q}[X]$ del polinomio ciclotomico $\phi_\ell(X) = X^{\ell-1} + X^{\ell-2} + \cdots + 1$. Infatti, se fosse $\phi_\ell(X) = g(X)h(X)$ in $\mathbb{Z}[X]$, riducendo modulo p, si avrebbe

$$\bar{\phi}_\ell(X) = f_1(X) \dots f_s(X), \qquad \text{con } \deg f_1(X) = \cdots = \deg f_1(X) = r_p = \min \{ \alpha \in \mathbb{N} \mid p^\alpha \equiv 1 \pmod{\ell} \},$$

ove ciascuno degli $f_i(X)$ è irriducibile in $\mathbb{F}_p[X]$. Allora, r_p deve dividere $\deg g(X) = \gamma < \ell - 1$. Dunque, posto $m = \mathrm{Mcd}(\gamma, \ell - 1)$, dovrebbe aversi che $r_p \mid m$ per ogni primo p. Invece possiamo mostrare(*) che, *per ogni divisore proprio m di $\ell - 1$, esistono infiniti primi p tali che $r_p \nmid m$.*

Fissato un tale m, osserviamo che gli elementi di $\mathbb{F}_\ell^\times$ il cui periodo divide m, formano un sottogruppo proprio $\Gamma \subset \mathbb{F}_\ell^\times$, e quindi dobbiamo mostrare che esistono infiniti primi $p \in \mathbb{Z}$, la cui classe modulo ℓ non appartiene a Γ. Se $p_1, \dots, p_s$ sono primi la cui classe modulo ℓ non stà in Γ, scelto un intero a, tale che

$$\bar{a} \notin \Gamma \qquad \text{e} \qquad \mathrm{Mcd}(a, \prod_{i=1}^s p_i) = 1,$$

è sufficiente osservare che tra i fattori primi di $\ell \prod_{i=1}^s p_i + a$ c'è un primo diverso da $p_1, \dots, p_s$.

7.11 Remark. [*Soluzioni intere dell'equazione $a^2 + b^2 = p$*] Abbiamo osservato (cf. I.7.6) che -1 è un residuo quadratico modulo p se, e solo se, $p \equiv 1 \pmod 4$. Vogliamo mostrare che, sotto tale ipotesi sul primo p, possiamo dedurre dal Teorema di Dirichlet sulle approssimazioni diofantee (cf. *Teorema I.5.1*) l'esistenza di soluzioni intere per l'equazione $a^2 + b^2 = p$.

Sia r un intero tale che $r^2 \equiv -1 \pmod p$ ed osserviamo che, se $(a, b) \in \mathbb{Z}^2$ è una soluzione dell'equzione proposta, allora deve aversi $a^2 + b^2 \equiv 0 \pmod p$ e quindi $a \equiv rb \pmod p$; e non è restrittivo supporre $0 < a, b < \sqrt{p}$. Dunque, deve esistere un intero m tale che

$$|rb - mp| < \sqrt{p} \qquad \text{ovvero} \qquad \left| \frac{r}{p} - \frac{m}{b} \right| < \frac{1}{b\sqrt{p}}.$$

Siamo quindi nelle condizioni per applicare il citato Teorema di Dirichlet, con $\xi = \frac{r}{p}$ e $Q = [\sqrt{p}]$ (parte intera di $\sqrt{p}$). Dunque, esistono degli interi x ed y tali che

$$\left| \frac{r}{p} - \frac{x}{y} \right| < \frac{1}{y[\sqrt{p}]} \quad \text{e} \quad 1 \le y \le [\sqrt{p}].$$

(*) La dimostrazione che verrà esposta si basa su un'osservazione elementare; ci limitiamo a menzionare il fatto che il risultato in questione si poteva anche dedurre dal seguente

Teorema. [Dirichlet] *Se* $\mathrm{Mcd}(a, b) = 1$, *esistono infiniti primi p tali che* $p \equiv a \pmod b$.

La dimostrazione di questo risultato è però di gran lunga più difficile degli argomenti che esporremo.

Quindi $|xp - ry| < \frac{p}{[\sqrt{p}]}$ e, posto $z = xp - ry$, deve aversi

$$y^2 + z^2 \equiv 0 \pmod{p} \qquad \text{e} \qquad 0 < y^2 + z^2 < [\sqrt{p}]^2 + \frac{p^2}{[\sqrt{p}]^2} < 3p,$$

Dunque[(†)] o si ha $y^2 + z^2 = p$ e così si è determinata la soluzione, oppure $y^2 + z^2 = 2p$, in tal caso y e z devono essere entrambi dispari e si ha $\left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = p$.

Osserviamo infine che, in generale non è vero che, fissato d con $\left(\frac{d}{p}\right) = 1$, esistano soluzioni dell'equazione $x^2 - dy^2 = p$, ma si potrebbe dimostrare che esiste un intero λ (dipendente da d, tale che $x^2 - dy^2 = \lambda p$. Non dimostriamo questa affermazione.

Concludiamo questa sezione sui campi finiti, mostrando che questi fanno parte di una classe più generale di campi.

7.12 Definizione. Un campo K si dice di classe $\mathcal{C}_1$ se, preso comunque un polinomio omogeneo $f(\underline{X}) \in K[X_1, \dots, X_n]$, di grado minore di n, $f(\underline{X})$ ha uno zero non banale in K^n.

I campi finiti sono di classe $\mathcal{C}_1$, come si deduce dal seguente

7.13 Teorema. [Chevalley-Warning] *Siano p un primo razionale e $q = p^r$. Dato $f(\underline{X}) \in \mathbb{F}_q[X_1, \dots, X_n]$, di grado $d < n$, allora*

$$N_f := \sharp\left(\{\, \underline{x} \in \mathbb{F}_q^n \mid f(\underline{x}) = 0 \,\}\right) \equiv 0 \pmod{p}.$$

dim. Dato $\underline{x} \in F_q^n$, si ha

$$f(\underline{x})^{q-1} = \begin{cases} 1 & \text{se } f(\underline{x}) \neq 0 \\ 0 & \text{se } f(\underline{x}) = 0 \end{cases};$$

quindi, la classe di N_f modulo p, è uguale a

$$\bar{N}_f = \sum_{\underline{x} \in F_q^n} (1 - f(\underline{x})^{q-1}) \in \mathbb{F}_q.$$

Si tratta quindi di mostrare che la somma in questione è nulla in $\mathbb{F}_q$.

È quindi sufficiente dimostrare che, dato un monomio che compare in $f(\underline{X})^{q-1}$, sia $X_1^{d_1} \cdots X_n^{d_n}$, con $d_1 + \cdots + d_n \le (q-1)d < (q-1)n$, si ha $\sum_{\underline{x} \in F_q^n} x_1^{d_1} \cdots x_n^{d_n} = 0$. Si osservi che

$$\sum_{\underline{x} \in F_q^n} x_1^{d_1} \cdots x_n^{d_n} = \prod_{i=1}^{n} \sum_{x_i \in F_q} x_i^{d_i}, \tag{7.14}$$

e quindi non è restrittivo supporre $d_i > 0$ per ogni $i = 1, \dots, n$, perchè altrimenti uno almeno dei fattori del prodotto è nullo (in $\mathbb{F}_q$). Consideriamo quindi

$$\sum_{x \in F_q} x^d, \qquad \text{con } d > 0.$$

(†) La disuguaglianza $[\sqrt{p}]^2 + \frac{p^2}{[\sqrt{p}]^2} < 3p$ è certamente vera per $p = 5$. Più in generale, posto $n = [\sqrt{p}]$ ed $u = \sqrt{p} - n$, la disuguaglianza è equivalente a

$$n^4 + (n+u)^4 < 3n^2(n+u)^2, \qquad \text{ovvero} \qquad ((n+u)^2 - n^2)^2 < n^2(n+u)^2;$$

e si ha $((n+u)^2 - n^2)^2 < (2n+1)^2$ ed $n^4 < n^2(n+u)^2$. Con le tecniche elementari del calcolo, è facile verificare che $n^4 > (2n+1)^2$ per $n > 2$ e dunque, per tutti i primi $p > 5$ tali che $p \equiv 1 \pmod{4}$.

Se g è un generatore di $\mathbb{F}_q^\times$, possiamo scrivere

$$\sum_{x\in F_q} x^d = \sum_{x\in F_q^\times} x^d = \sum_{h=0}^{q-2} g^{dh} = \begin{cases} -1 & \text{se } g^d = 1 \\ \frac{(g^d)^{q-1}-1}{g^d-1} = 0 & \text{se } (q-1)\nmid d \end{cases}.$$

Allora, uno almeno dei fattori nel prodotto ($I.7.14$) è uguale a zero perchè, se $q-1$ dividesse tutti gli esponenti $d_i > 0$, non potrebbe aversi $d_1 + \cdots + d_n < (q-1)n$. **CVD** □

Si deduce immediatamente il seguente

7.15 Corollario. *I campi finiti sono di classe $\mathcal{C}_1$.*

dim. Nelle notazioni del Teorema precedente, preso comunque un polinomio omogeneo $f(\underline{X})$ appartenente ad $\mathbb{F}_q[X_1, \dots, X_n]$ e di grado minore di n, si ha $N_f \geq 1$, perchè f ha lo zero banale ed essendo $N_f \equiv 0 \pmod p$, devono esistere zeri non banali. **CVD** □

7.16 Remark. Molte delle proprietà dei campi finiti si estendono ai campi $\mathcal{C}_1$; ad esempio mostriamo che *non esistono estensioni finite non-commutative di campi* $\mathcal{C}_1$. Sia F un corpo (non-commutativo) con centro k, di classe $\mathcal{C}_1$. È noto che esiste un'estensione finita, di Galois k' di k, tale che $F\otimes_k k'$, sia isomorfo ad un'anello di matrici su k' (cf. ad esempio: Serre: Corps Locaux, Paris 1962, Ch. X, §.5, Proposition 7, e vedi Bourbaki, Algebre, Ch.VIII,§.5, 10, per una dimostrazione). Dunque ogni elemento di F si identifica con una matrice quadrata A, di ordine n ed il determinante di A è un polinomio omogeneo (a coefficienti in $\mathbb{Z}$) di grado n nelle n^2 entrate della matrice. Poichè k è di classe $\mathcal{C}_1$, vi è uno zero non banale in k^{n^2} per tale polinomio, contro l'ipotesi che ogni elemento di F sia invertibile.

Chiudiamo questa sezione, richiamando una famosa congettura

Congettura. [E. Artin] *Il campo che si ottiene aggiungendo a $\mathbb{Q}$ tutte le radici di 1 è un campo $\mathcal{C}_1$.*

8. Ideali ed estensioni intere

Sia A un dominio integralmente chiuso, con corpo dei quozienti K, e sia B la chiusura integrale di A in un'estensione finita e separabile di K. Siamo interessati a studiare le relazioni che intercorrono tra gli ideali primi dei due anelli.

Più in generale ci occuperemo della situazione in cui $A \subseteq B$ sono domini e B è intero su A; in particolare, diremo che un ideale $\mathfrak{q}$ di B *sta sopra* ad un ideale $\mathfrak{p}$ di A se $A \cap \mathfrak{q} = \mathfrak{p}$.

Iniziamo la discussione con un risultato preliminare che ci sarà utile nel seguito.

8.1 Lemma di Nakayama. *Sia A un anello e sia M un A-modulo finitamente generato. Se $\mathfrak{a}$ è un ideale di A contenuto in tutti i massimali di tale anello, allora $\mathfrak{a}M = M$ se, e solo se, $M = (0)$.*

dim. Siano $m_1, \dots, m_n$ dei generatori di M; dalla relazione $\mathfrak{a}M = M$, si deduce che esistono degli elementi $a_1, \dots, a_n$ di $\mathfrak{a}$ tali che $m_1 = a_1m_1 + \cdots + a_nm_n$. Poichè $\mathfrak{a}$ è contenuto in tutti gli ideali massimali, $1 - a_1$ è invertibile in A e quindi M può essere generato da $m_2, \dots, m_n$. Continuando allo stesso modo, si possono eliminare tutti i generatori ed ottenere quindi $M = (0)$. **CVD** □

Verifichiamo che esistono ideali primi di B sopra ad ogni dato primo di A.

8.2 Proposizione. *Siano A un dominio e B un dominio intero su A. Dato un ideale primo $\mathfrak{p}$ di A, allora $\mathfrak{p}B \neq B$ e quindi esiste un ideale primo $\mathfrak{q}$ di B che sta sopra a $\mathfrak{p}$. Inoltre $\mathfrak{p}$ è massimale in A se, e solo se, $\mathfrak{q}$ è massimale in B.*

dim. Si consideri l'anello $B_\mathfrak{p} = B \otimes_A A_\mathfrak{p}$, intero sull'anello locale $A_\mathfrak{p}$. Se fosse $\mathfrak{p}B_\mathfrak{p} = B_\mathfrak{p}$, si avrebbe che

$$1 = x_1b_1 + \cdots + x_nb_n, \qquad \text{con } x_1, \dots, x_n \in \mathfrak{p} \text{ e } b_1, \dots, b_n \in B_\mathfrak{p}.$$

Considerando ora l'anello $B_0 = A_\mathfrak{p}[b_1,\dots,b_n]$, si è nelle ipotesi del Lemma di Nakayama, da cui si otterrebbe $B_0 = 0$, che è assurdo. Quindi $\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$ ed esiste un ideale massimale $\mathfrak{m} \subset B_\mathfrak{p}$ contenente $\mathfrak{p}B_\mathfrak{p}$. Sia quindi $\mathfrak{q} = \mathfrak{m} \cap B$ ed osserviamo che si tratta di un ideale primo(*) di B, contenente $\mathfrak{p}B$ e si ha

$$\mathfrak{q} \cap A = \mathfrak{m} \cap A = (\mathfrak{m} \cap A_\mathfrak{p}) \cap A = \mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{p}.$$

Osserviamo che, se $\mathfrak{p}$ è massimale in A allora ogni elemento $y \in B/\mathfrak{q}$ è intero e quindi algebrico sul campo $A/\mathfrak{p}$. Poichè $A/\mathfrak{p}[y]$ è un campo, si conclude che ogni elemento di $B/\mathfrak{q}$ è invertibile e quindi tale anello è un campo. D'altra parte, se $B/\mathfrak{q}$ è un campo, allora $A/\mathfrak{p}$ è un sottoanello di tale campo e per ogni elemento diverso da zero $x \in A/\mathfrak{p}$, esiste l'inverso $x^{-1} \in B/\mathfrak{q}$. Dunque x^{-1} è intero su $A/\mathfrak{p}$ e quindi esistono $a_1,\dots,a_r \in A/\mathfrak{p}$, tali che

$$x^{-r} + a_1x^{-r+1} + \cdots + a_r = 0;$$

da cui, moltiplicando per x^{r-1}, si deduce $x^{-1} \in A/\mathfrak{p}$. **CVD** □

8.3 Complementi. [*Teoremi di going-up e going-down*] Come facile conseguenza della Proposizione precedente, si ottiene che, nelle ipotesi dette, è possibile 'rialzare' a B delle catene ascendenti di ideali primi di A. Precisamente, si può enunciare il seguente

Teorema di going-up. *Siano $A \subseteq B$ due domini e B sia intero su A. Se $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ è una catena di primi di A e $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$, con $m < n$, è una catena di primi di B tali che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, per $i = 1,\dots,m$; allora la catena $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$ si può estendere ad una catena $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ tale che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, per $i = 1,\dots,n$.*

dim. È chiaro che è sufficiente dimostrare il Teorema nel caso in cui $n = m + 1$. In tal caso, basta osservare che $B/\mathfrak{q}_m$ è intero su $A/\mathfrak{p}_m$ e quindi, per la *Proposizione I.8.2*, esiste un ideale $\bar{\mathfrak{q}}_{m+1}$ di $B/\mathfrak{q}_m$ che sta sopra all'immagine di $\mathfrak{p}_{m+1}$ in $A/\mathfrak{p}_m$. Rialzando $\bar{\mathfrak{q}}_{m+1}$ a B si conclude. **CVD** □

La situazione è un po' più complicata nel caso in cui si vogliano rialzare catene discendenti di ideali primi. Vale però un risultato analogo nel caso in cui A sia integralmente chiuso (cf. *Definizione I.3.5*).

Teorema di going-down. *Sia A un dominio integralmente chiuso e sia $B \supseteq A$ un dominio, intero su A. Se $\mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$ è una catena di primi di A e $\mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_m$, con $m < n$, è una catena di primi di B tali che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, per $i = 1,\dots,m$; allora la catena $\mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_m$ si può estendere ad una catena $\mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_n$ tale che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, per $i = 1,\dots,n$.*

dim. È chiaro che è sufficiente dimostrare il Teorema nel caso in cui $m = 1$ ed $n = 2$ ed, in particolare, si tratta di mostrare che $\mathfrak{p}_2B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2$. Ogni elemento $x \in \mathfrak{p}_2B_{\mathfrak{q}_1}$ è della forma $x = \frac{y}{s}$ con $y \in \mathfrak{p}_2B$ ed $s \in B \setminus \mathfrak{q}_1$. Poichè A è integralmente chiuso, il polinomio minimo di y su $K = Frac\,A$, è del tipo

$$y^r + u_1y^{r-1} + \cdots + u_r, \tag{*}$$

con $u_1,\dots,u_r \in \mathfrak{p}_2$(†). Se $x \in \mathfrak{p}_2B_{\mathfrak{q}_1} \cap A$, allora si ha che il polinomio minimo di $s = yx^{-1}$ su K, si ottiene da (*) moltiplicando per x^{-r} ed, essendo s intero su A, si conclude che $v_i = u_ix^{-i} \in A$, per $i = 1,\dots,r$. Se $x \notin \mathfrak{p}_2$,

(*) Perchè $B/\mathfrak{q}$ è un sottoanello del campo $B_\mathfrak{p}/\mathfrak{m}$ e quindi è un dominio.

(†) È chiaro che, il polinomio minimo di y ha i coefficienti in A, perchè $y \in \mathfrak{p}_2B$ è intero su A ed A è integralmente chiuso. In generale, se $A \subset B$ sono due domini, ed $\mathfrak{a}$ è un ideale di A, diremo che $x \in B$ è *intero su* $\mathfrak{a}$ se x soddisfa ad un'equazione monica a coefficienti in $\mathfrak{a}$. Vale il seguente

Lemma. *Siano $A \subset B$ due domini, con A integralmente chiuso e B intero su A e sia $\mathfrak{a}$ un ideale di A. Allora*
(i) l'insieme degli elementi di B interi su $\mathfrak{a}$ è il radicale $\sqrt{\mathfrak{a}B}$ di $\mathfrak{a}B$;
(ii) il polinomio minimo di x su K ha i coefficienti nel radicale $\sqrt{\mathfrak{a}}$ di $\mathfrak{a}$.

dim. (i) Se $x \in B$ è intero su $\mathfrak{a}$, allora $x^n = a_1x^{n-1} + \cdots + a_n$ con $a_1,\dots,a_n \in \mathfrak{a}$ e quindi $x \in \sqrt{\mathfrak{a}B}$. Viceversa, se $x \in \sqrt{\mathfrak{a}B}$, allora $x^n = \sum a_ix_i$, per qualche $n > 0$, con $a_i \in \mathfrak{a}$ ed $x_i \in B$. Considerando l'A-modulo finitamente generato $M = A[x_1,\dots,x_r]$, si conclude che $x^nM \subseteq \mathfrak{a}M$ e perciò che x^n (e quindi x) è intero su $\mathfrak{a}$.
(ii) I coefficienti del polinomio minimo sono funzioni simmetriche sui coniugati di x, che sono tutti interi su $\mathfrak{a}$ e quindi, per il punto precedente, i coefficienti del polinomio minimo sono in A e nel radicale di $\mathfrak{a}B$ e quindi nel radicale di $\mathfrak{a}$. **CVD** □

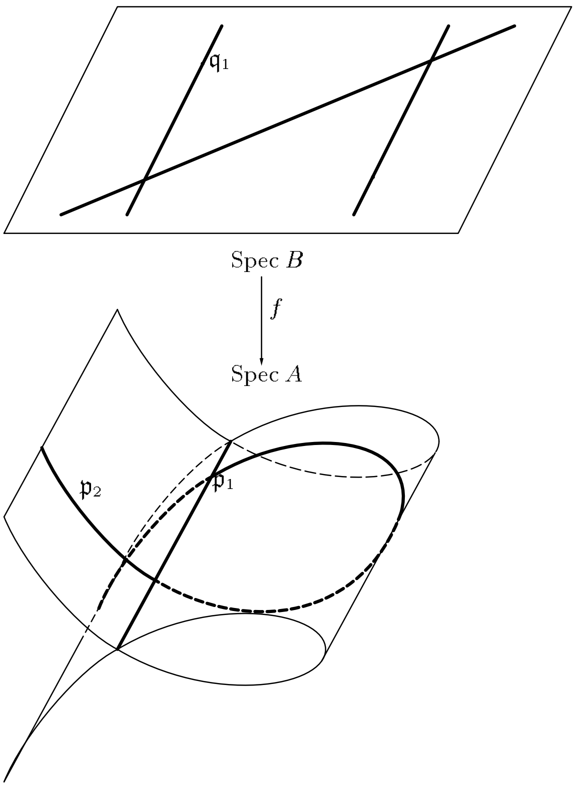
Poichè $\mathfrak{p}_2$ è un ideale primo, il Lemma ci permette di concludere.

dalla relazione $x^i v_i = u_i \in \mathfrak{p}_2$, si ottiene che tutti i coefficienti del polinomio minimo di s stanno in $\mathfrak{p}_2$ e quindi $s^r \in \mathfrak{p}_2 B \subset \mathfrak{p}_1 B \subseteq \mathfrak{q}_1$, da cui si deduce che $s \in \mathfrak{q}_1$, il che è assurdo. Si conclude quindi che $x \in \mathfrak{p}_2$ e dunque $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2$. **CVD** □

Da ultimo, vogliamo dare un esempio di come l'ipotesi che A sia integralmente chiuso sia essenziale per la validità del Teorema di going-down.

Siano $A = k[x,y,z]/(y^2 - x^3 - x^2)$ e $B = k[m,t]$, ove x, y, z, m, t sono indeterminate sul corpo k, che supporremo algebricamente chiuso e di caratteristica 0. Si consideri l'omomorfismo iniettivo di k-algebre $f : A \to B$ definito ponendo $f(x) = m^2 - 1$, $f(y) = m(m^2 - 1)$, $f(z) = t$ e d'ora in poi supporremo A contenuto in B, identificandolo con la sua immagine tramite f.

Il disegno a fianco da un'interpretazione geometrica della situazione che andiamo a descrivere ed invitiamo perciò il lettore a riferirsi ad esso. Nel disegno, sperando di non creare confusione, indichiamo con lo stesso simbolo gli ideali degli anelli in questione e le sottovarietà affini che ad essi corrispondono.



Si considerino gli ideali primi

$$A \supseteq \mathfrak{p}_1 = (x, y, z - 1) \supset \mathfrak{p}_2 = (y - zx, z^2 - x - 1)$$

e

$$B \supseteq \mathfrak{q}_1 = (m + 1, t - 1)$$

e si osservi che $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Si verifica con un calcolo diretto che l'immagine di $\mathfrak{p}_2$ in $B_{\mathfrak{q}_1}$ è l'ideale massimale di tale anello e quindi che non può esistere un ideale di B, contenuto in $\mathfrak{q}_1$, che stia sopra a $\mathfrak{p}_2$. Ciò doverbbe essere evidente 'geometricamente' osservando che non c'e' nessuna sottovarietà di Spec B, contenente $\mathfrak{q}_1$ che si proietti sulla curva $\mathfrak{p}_2$ di Spec A.

Ciò conclude la digressione sui teoremi di going-up e going-down di Cohen–Seidenberg. Il lettore che volesse approfondire l'argomento può consultare, ad esempio, il libro: *D. Eisenbud*, Commutative Algebra with a view toward Algebraic Geometry, Springer 1994.

Torniamo quindi a discutere delle relazioni tra gli ideali di un'estensione intera, occupandoci di un esempio.

8.4 Esempio. Sia A un dominio integralmente chiuso, con corpo dei quozienti K, e sia $B = A[\alpha]$ intero su A. Indichiamo con $f(X) \in A[X]$ il polinomio minimo di α su K (cf. la *Proposizione I.3.6* e la nota a pie' di pagina relativa alla sua dimostrazione). Dato un ideale massimale $\mathfrak{p}$ di A, possiamo considerare la riduzione $\bar{f}(X) \in A/\mathfrak{p}[X]$ del polinomio $f(X)$ e la sua decomposizione in fattori irriducibili $\bar{f}(X) = \bar{f}_1(X)^{e_1} \cdots \bar{f}_r(X)^{e_r}$, ove $f_1(X), \dots, f_r(X) \in A[X]$ sono monici ed a due a due coprimi.

Mostriamo che gli ideali di $B = A[\alpha]$ che stanno sopra a $\mathfrak{p}$ sono $\mathfrak{q}_1, \dots, \mathfrak{q}_r$, ove $\mathfrak{q}_j = \mathfrak{p}B + (f_j(\alpha))$, per $j = 1, \dots, r$. Infatti se $y \in \mathfrak{q}_j \cap A$, allora $y = h(\alpha) + g(\alpha) f_j(\alpha)$, con $g(x) \in A[X]$ ed $h(x) \in \mathfrak{p}[X]$ ed $y \in A$. Riducendo modulo $\mathfrak{p}$, si ottiene $\bar{y} \in (\bar{f}_j(X))$ che è un ideale irriducibile non banale di $A/\mathfrak{p}[X]$, dunque, deve aversi $y \in \mathfrak{p}$.

Inoltre, osserviamo che

$$B/\mathfrak{q}_j = A[\alpha]/\mathfrak{q}_j \cong \frac{A/\mathfrak{p}[X]}{(\bar{f}_j(X))}$$

e quest'ultimo è un corpo, perchè $\bar{f}_j(X)$ è irriducibile. Quindi l'ideale $\mathfrak{q}_j$ è massimale.

L'esempio precedente descrive una situazione relativamente generale. Infatti, nel caso in cui B sia l'anello degli interi di un campo di numeri, ci si trova nella situazione descritta se si localizza rispetto a quasi tutti i primi di $\mathbb{Z}$ (con l'eccezione di un numero finito). Precisamente, sia L un'estensione finita di $\mathbb{Q}$, di grado n, e sia B la chiusura integrale di $\mathbb{Z}$ in L. Se consideriamo un elemento primitivo α per L che sia intero su $\mathbb{Z}$ (cf. *Proposizione I.2.2* e *Lemma I.3.7*); allora $B \subseteq \frac{1}{d}\mathbb{Z}[\alpha]$, ove $d = \Delta(1, \alpha, \dots, \alpha^{n-1})$ è il discriminante di B su $\mathbb{Z}$ (cf. *Teorema I.3.8*). Se p è un primo di $\mathbb{Z}$ che non divide d, localizzando rispetto all'ideale (p), si ottiene $B_{(p)} = \mathbb{Z}_{(p)}[\alpha]$ e si può ragionare come nell'esempio precedente per determinare i primi B che stanno sopra a (p).

La situazione dell'esempio, si presenta anche nel caso dei corpi quadratici o dei corpi ciclotomici principali, e sarebbe facile dare i dettagli in questi casi. Ritorneremo su questi esempi, dopo aver approfondito alcune caratteristiche generali degli anelli di interi di estensioni algebriche.

9. Domini di Dedekind

Cominciamo occupandoci del caso locale: i domini di Dedekind locali sono gli anelli di valutazione discreta.

9.1 Definizione. Un dominio d'integrità A si dice *dominio di valutazione discreta* (DVR) se è principale ed ha un unico ideale primo $\mathfrak{p}$. Ogni generatore π del primo $\mathfrak{p}$ è detto un *uniformizzante* per A.

Osserviamo che, come facile conseguenza del Lemma di Nakayama, per un DVR A, si ha

$$\bigcap_{n \geq 0} \mathfrak{p}^n = (0). \tag{9.2}$$

Infatti, posto $I = \bigcap_{n \geq 0} \mathfrak{p}^n$ e ricordato che $\mathfrak{p}$ è un ideale principale, è immediato verificare che $\mathfrak{p}I = I$; quindi, essendo $\mathfrak{p}$ l'unico massimale di A, si conclude che $I = (0)$ per il citato Lemma.

Siano A un DVR, $K = Frac\,A$ e sia fissato un uniformizzante π di A. Ogni elemento $x \in A$, si può scrivere (in modo unico) come $x = \pi^n u$, ove $u \in A^\times$ è invertibile e quindi n è l'unico intero non negativo tale che $x \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$. Dunque, l'intero n non dipende dalla scelta di π e si può estendere la decomposizione $x = \pi^n u$, con $u \in A^\times$ ed $n \in \mathbb{Z}$ ad ogni elemento $0 \neq x \in K$. Sai definisce così la *valutazione discreta* associata ad A, ovvero l'applicazione $v : K^\times \to \mathbb{Z}$, definita da $v(x) = n$, ove n è determinato dalla decomposizione $x + \pi^n u$ descritta sopra. Si verifica immediatamente che v è un omomorfismo suriettivo di gruppi, ovvero che $v(xy) = v(x) + v(y)$ e $v(\pi) = 1$ ed inoltre che vale la proprietà $v(x + y) \geq \min\{\, v(x), v(y)\,\}$. Spesso l'applicazione v si estende a K ponendo $v(0) = +\infty$, mantenendo valide le proprietà dette.

A partire dall'applicazione v, si può ricostruire l'anello A osservando che

$$A = \{\, x \in K \mid v(x) \geq 0 \,\}.$$

In particolare, tramite v, si verifica facilmente che *ogni ideale* $J \neq (0)$ *di* A *è del tipo* $\pi^m A$, ove $m = \min_{x \in I} v(x)$.

Osserviamo infine che, a partire da v, si può definire un *valore assoluto* (ultrametrico) su K, fissando un numero reale $c \in (0, 1)$ e ponendo $|x| = c^{v(x)}$. Tramite questo valore assoluto, si definisce una topologia su K (che è indipendente dalla scelta di c) e si può considerare il completamento di K rispetto alla metrica data, che è ancora un corpo con una valutazione discreta.

Esempi di DVR sono: il localizzato $\mathbb{Z}_{(p)}$ dell'anello degli interi ad un suo ideale primo $(p) \neq (0)$; l'anello $k[\![X]\!]$ delle serie di potenze a coefficienti in un campo k; l'anello locale di un punto semplice P di una curva algebrica (ad esempio, se la curva è contenuta nel piano, si può prendere come uniformizzante, l'equazione di una qualsiasi retta non tangente alla curva nel punto P).

Diamo ora alcune caratterizzazioni dei DVR che ci saranno utili nel seguito

9.3 Proposizione. *Sia A un dominio noetheriano. Le seguenti affermazioni sono equivalenti:*
(i) A è un DVR;
(ii) A è un anello locale con il massimale $\mathfrak{p}$ principale;
(iii) A è integralmente chiuso ed ammette un unico ideale primo $\mathfrak{p} \neq (0)$.

dim. È immediato verificare che *(i)* $\Rightarrow$ *(ii)*; viceversa, basta osservare che, essendo A locale e $\mathfrak{p}$ principale, si dimostra con il Lemma di Nakayama che vale (I.9.2) e si può così definire una valutazione sul corpo $K = Frac\, A$.

Per verificare che *(i)* $\Rightarrow$ *(iii)*, è sufficiente ricordare che un DVR è un anello ad ideali principali e quindi un dominio fattoriale, che è integralmente chiuso in base alla *Proposizione I.3.6*.

Il resto della dimostrazione è dedicato alla verifica che *(iii)* $\Rightarrow$ *(ii)*, ovvero che, sotto le ipotesi di *(iii)*, $\mathfrak{p}$ è un ideale principale. Sia dunque $K = Frac\, A$ e si consideri

$$\mathfrak{p}' = \{\, x \in K \mid x\mathfrak{p} \subseteq A \,\},$$

ed osserviamo che $\mathfrak{p}'$ è un ideale frazionario (cf. *Definizione I.9.6*) in K, perchè, per ogni $y \in \mathfrak{p} \setminus \{0\}$, si ha $y\mathfrak{p}' \subseteq A$, ovvero $\mathfrak{p}' \subseteq \frac{1}{y}A$, ed A è noetheriano. Dunque, si ha che $\mathfrak{p}\mathfrak{p}'$ è un ideale di A che contiene $\mathfrak{p}$ ($1 \in \mathfrak{p}'$), dunque, essndo $\mathfrak{p}$ massimale, si conclude che

$$\mathfrak{p}\mathfrak{p}' = \mathfrak{p} \qquad \text{oppure} \qquad \mathfrak{p}\mathfrak{p}' = A.$$

Se fosse $\mathfrak{p}\mathfrak{p}' = A$, potremmo scrivere $1 = \sum_{i=1}^{n} x_i y_i$, con $x_i \in \mathfrak{p}'$ ed $y_i \in \mathfrak{p}$, e poichè tutti gli addendi sono in A, deve esistere un indice i per cui $x_i y_i = u \in A^\times$. Possiamo dunque supporre che, si abbia $xy = 1$ per qualche $x \in \mathfrak{p}'$ ed $y \in \mathfrak{p}$ e possiamo perciò concludere che y è un generatore di $\mathfrak{p}$, avendosi $z = (zx)y$ per ogni $z \in \mathfrak{p}$, con $zx \in A$, perchè $x \in \mathfrak{p}'$.

Siamo quindi in grado di concludere se dimostriamo che non può aversi $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$. Se così fosse, dato $x \in \mathfrak{p}'$, si avrebbe $x\mathfrak{p} \subseteq \mathfrak{p}$ e quindi che x è intero su A e quindi, poichè A è integralmente chiuso, si concluderebbe che $\mathfrak{p}' = A$. Si osservi poi che, dato un elemento $x \neq 0$ di $\mathfrak{p}$, si ha che l'anello $A_x = A[\frac{1}{x}]$ è uguale al compo K, perchè $\mathfrak{p}$ è l'unico ideale primo di A. Dunque, fissato un elemento non nullo $z \in \mathfrak{p}$, in corrispondenza ad ogni $x \in \mathfrak{p} \setminus \{0\}$, esiste un intero non negativo n, tale che $\frac{1}{z} = \frac{a}{x^n}$, ovvero che $x^n \in (z)$. Poichè A è noetheriano, si conclude che esiste un esponente $N \geq 1$ tale che $\mathfrak{p}^N \subseteq (z)$, ma $\mathfrak{p}^{N-1} \not\subseteq (z)$. Ciò significa che esiste un elemento $y \in \mathfrak{p}^{N-1}$ tale che $y \notin (z)$ ovvero che $y/z \notin A$, ma ciò è assurdo, perchè $y/z \in \mathfrak{p}' = A$. **CVD** □

Possiamo quindi dare la definizione di dominio di Dedekind.

9.4 Definizione. Un dominio noetheriano A è un *dominio di Dedekind* se è soddisfatta una delle seguenti proprietà, tra loro equivalenti:
(i) per ogni ideale primo $\mathfrak{p}$ di A, il localizzato $A_\mathfrak{p}$ è un DVR;
(ii) A è integralmente chiuso e di dimensione ≤ 1[(†)].

dim. (dell'equivalenza delle due condizioni.)
(i) $\Rightarrow$ *(ii)* Siano dati due primi di A, $(0) \subset \mathfrak{p} \subset \mathfrak{q}$, considerando il DVR $A_\mathfrak{q}$, si avrebbe $\mathfrak{p}A_\mathfrak{q} = (0)$, oppure $\mathfrak{p}A_\mathfrak{q} = \mathfrak{q}A_\mathfrak{q}$. La prima possibilità non può darsi perchè A è un dominio. Dalla seconda uguaglianza, si ottiene $\mathfrak{p} = \mathfrak{q}$, perchè, per ogni $x \in \mathfrak{q}$, si ha $x = \frac{x'}{y}$ per opportuni $x' \in \mathfrak{p}$ ed $y \in A \setminus \mathfrak{q}$, e da questa uguaglianza, si ottiene $yx = x' \in \mathfrak{p}$ e quindi $x \in \mathfrak{p}$.
(ii) $\Rightarrow$ *(i)* In base alla *Proposizione I.9.3* è sufficiente mostrare che, per ogni primo $\mathfrak{p}$, il localizzato $A_\mathfrak{p}$ è integralmente chiuso. Se $x \in K = Frac\, A$, è intero su $\mathbb{A}_\mathfrak{p}$, si ha la relazione $x^n + c_1 x^{n-1} + \cdots + c_n = 0$,

(†) un dominio A è di dimensione ≤ 1 se, e solo se, ogni ideale primo $\mathfrak{p} \neq (0)$ è massimale in A.

con $c_i = \frac{a_i}{b}$ ed $a_i \in A$, $b \in A \setminus \mathfrak{p}$, per ogni $i = 1, \dots, n$. Moltiplicando per b^n, si ottiene che bx è intero su A e quindi appartiene ad A. Si conclude perciò che $x \in A_\mathfrak{p}$ e quindi che il localizzato è integralmente chiuso$^{(**)}$. **CVD** □

9.5 Osservazione. Sia A un dominio di Dedekind, di corpo di frazioni K, sia L un'estensione finita di K e sia B la chiusura integrale di A in L. Allora B è ancora un dominio di Dedekind. Infatti, per ogni primo $\mathfrak{q}$ di B, il localizzato $B_\mathfrak{q}$ è integralmente chiuso ed ha un unico ideale primo (se ciò non fosse si potrebbe applicare il Teorema di going-down ed ottenere una contraddizione col fatto che A è un dominio di Dedekind). Dunque, $B_\mathfrak{q}$ è un DVR (cf. *Proposizione I.9.3*) e quindi B è un dominio di Dedekind. In particolare osserviamo che $\mathbb{Z}$ è un dominio di Dedekind e quindi, per quanto appena osservato, tutti gli anelli degli interi di corpi di numeri algebrici sono domini di Dedekind.

Il nostro primo obbiettivo è lo studio degli ideali frazionari di un anello di Dedekind; nozione che generalizza ai corpi di numeri algebrici la nozione di numero primo nel corpo dei numeri razionali. Cominciamo con la definizione

9.6 Definizione. Sia A un dominio di integrità noetheriano e K il suo corpo delle frazioni. Si chiama *ideale frazionario* ogni sotto-A-modulo finitamente generato di K.

Osserviamo che ogni ideale di A è un ideale frazionario e che, se I è un ideale frazionario, allora $(A : I) = \{ x \in K \mid xI \subseteq A \}$ è un ideale frazionario. Infatti, se $x \in I$ allora $(A : I) \subset \frac{1}{x}A$ ed A è noetheriano.. Un altro facile risultato sugli ideali frazionari è il seguente

9.7 Lemma. *Sia A un dominio di integrità noetheriano e K il suo corpo delle frazioni. Siano I e J ideali frazionari e sia $\mathfrak{p}$ un ideale primo. Allora*

(i) $(IJ)_\mathfrak{p} = I_\mathfrak{p} J_\mathfrak{p}$;
(ii) $(A : I)_\mathfrak{p} = (A_\mathfrak{p}, I_\mathfrak{p})$.

dim. Le inclusioni $(IJ)_\mathfrak{p} \subseteq I_\mathfrak{p} J_\mathfrak{p}$ e $(A : I)_\mathfrak{p} \subseteq (A_\mathfrak{p} : I_\mathfrak{p})$ discendono in modo ovvio dalle definizioni. Le inclusioni inverse sono conseguenza del fatto che I e J sono A-moduli finitamente generati. Ad esempio, se $z \in (A_\mathfrak{p} : I_\mathfrak{p})$, allora, per ogni $x \in I$, si ha che $zx \in A_\mathfrak{p}$, ed essendo I finitamente generato, esiste un elemento $s \in A \setminus \mathfrak{p}$, tale che $szx \in A$ per ogni $x \in I$. Dunque $sz \in (A : I)$ e quindi $z \in (A : I)_\mathfrak{p}$. Ciò conclude la dimostrazione di *(ii)*. La dimostrazione di *(i)* si basa su considerazioni analoghe. **CVD** □

Siamo quindi in grado di dimostrare la seguente

9.8 Proposizione. *Sia A un dominio di Dedekind e K il suo corpo delle frazioni. Gli ideali frazionari formano un gruppo rispetto all'operazione di prodotto.*

dim. È chiaro che il prodotto di ideali frazionari è ancora un ideale frazionario e che l'anello A si comporta da elemento neutro rispetto a questa operazione. Dunque, è sufficiente dimostrare che ogni ideale frazionario è invertibile. Mostreremo che, dato un ideale frazionario I, l'ideale frazionario $I' = (A : I)$ è il suo inverso. Infatti, per ogni ideale primo $\mathfrak{p}$ di A si ha

$$(I\,I')_\mathfrak{p} = I_\mathfrak{p}\,(A : I)_\mathfrak{p} = I_\mathfrak{p}\,(A_\mathfrak{p} : I_\mathfrak{p}) = A_\mathfrak{p}$$

ove l'ultima uguaglianza è ovvia nel DVR $A_\mathfrak{p}$. Poichè l'uguaglianza $(I\,I')_\mathfrak{p} = A_\mathfrak{p}$ vale per ogni primo $\mathfrak{p}$, si conclude che $I\,I' = A$. **CVD** □

Il nostro prossimo obbiettivo è dimostrare che per gli ideali di un dominio di Dedekind vale l'analogo della decomposizione in fattori primi degli interi razionali, ovvero che ogni ideale si scrive in modo unico come prodotto di ideali primi.

$^{(**)}$ Più in generale, è vero per ogni dominio noetheriano A che *A è integralmente chiuso se, e solo se, $A_\mathfrak{p}$ è integralmente chiuso, per ogni primo $\mathfrak{p}$ di A*. In un verso l'affermazione è stata appena dimostrata; nell'altro verso, si osservi che, se $x \in K$ è intero su A allora x è intero su ogni localizzato $A_\mathfrak{p}$, e dunque $x \in \bigcap_\mathfrak{p} A_\mathfrak{p} = A$. L'ultima uguaglianza, si ottiene facilmente osservando che, dato un elemento $y \in \bigcap_\mathfrak{p} A_\mathfrak{p}$, l'insieme $\{ s \in A \mid sy \in A \}$ è un ideale di A diverso da zero e non contenuto in nessun primo di A. Dunque $\{ s \in A \mid sy \in A \} = A$ e ciò permette di concludere.

9.9 Lemma. *Sia A un dominio di Dedekind. Ogni ideale $I \neq (0)$ di A contiene un prodotto finito di ideali primi non-nulli.*

dim. Se l'insieme degli ideali che non verificano la tesi è diverso dal vuoto allora tale insieme contiene un elemento massimale J, perchè A è noetheriano. Allora, J non è un ideale primo e perciò esistono $a, b \in A \setminus J$ tali che $ab \in J$. I due ideali $J + (a)$ e $J + (b)$, contengono propriamente J e quindi per essi vale la tesi, ma allora $J \supseteq (J + (a))(J + (b))$ e quindi contiene un prodotto non nullo di ideali primi, il che è assurdo. **CVD** □

Come conseguenza, possiamo osservare che ogni ideale $I \neq (0)$ di un dominio di Dedekind è contenuto in un numero finito di ideali primi. Infatti, in base al Lemma precedente, dalla relazione $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I \subseteq \mathfrak{p}$ si deduce che $\mathfrak{p}$ deve essere uno degli ideali $\mathfrak{p}_j$. Possiamo quindi concludere con il risultato a cui si faceva cenno in precedenza

9.10 Proposizione. *Sia A un dominio di Dedekind e K il suo corpo delle frazioni. Ogni ideale $I \neq (0)$ di A si scrive in modo unico come prodotto di ideali primi.*

dim. Sia dunque I un ideale di A e sia $\mathfrak{p}$ un ideale primo. Localizzando al primo $\mathfrak{p}$, ed indicando con $v_\mathfrak{p}$ la valutazione di K relativa al primo $\mathfrak{p}$, si ottiene

$$I_\mathfrak{p} = \mathfrak{p}^{e_\mathfrak{p}} A_\mathfrak{p} \qquad \text{ove} \qquad 0 \leq e_\mathfrak{p} = v_\mathfrak{p}(I) = \min \{ v_\mathfrak{p}(x) \mid x \in I \}.$$

Inoltre, per quanto visto sopra, $v_\mathfrak{p}(I) > 0$ solo per un numero finito di primi. Dunque, si conclude che

$$I = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(I)},$$

perchè tale uguaglianza vale in $A_\mathfrak{p}$ per ogni ideale primo $\mathfrak{p}$. **CVD** □

Il nostro ultimo obbiettivo è lo studio della fattorizzazione unica (degli elementi e non solo degli ideali) nei domini di Dedekind. Il primo risultato in tale direzione è un Lemma di approssimazione simultanea rispetto a varie valutazioni.

9.11 Proposizione. [Teorema Cinese] *Siano A un dominio di Dedekind e K il suo corpo delle frazioni. Siano $v_1, \dots, v_n$ valutazioni discrete di K corrispondenti a primi distinti $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Siano $x_1, \dots, x_n$ degli elementi di A ed $h_1, \dots, h_n$ degli interi positivi. Allora esiste un elemento $x \in A$ tale che*

$$v_i(x - x_i) \geq h_i \qquad \text{per } i = 1, \dots, n.$$

dim. Non è restrittivo supporre $x_1 = 1$ ed $x_2 = \cdots = x_n = 0$, perchè se sappiamo risolvere questo problema per ogni indice $i = 1, \dots, n$ ed indichiamo con y_i la soluzione, allora l'elemento $x = y_1 x_1 + \cdots + y_n x_n$ soddisfa alle condizioni dell'enunciato. Dunque si tratta di mostrare che esiste un elemento $y \in A$ tale che

$$v_1(y - 1) \geq h_1, \qquad \text{e} \qquad v_i(y) \geq h_i, i = 2, \dots, n.$$

Per ogni $j > 1$, si ha $\mathfrak{p}_1 + \mathfrak{p}_j = A$ e quindi, per ogni $H > 0$, si ha $\mathfrak{p}_1^H + \mathfrak{p}_j^H = A$. Fissato un intero $H \geq \max_i(h_i)$, per ogni $j \geq 2$, esistono degli elementi $z_j \in \mathfrak{p}_1^H$ e $y_j \in \mathfrak{p}_j^H$ tali che $z_j + y_j = 1$ e si ha

$$1 = \prod_{2 \leq j \leq n} (z_j + y_j) = z + y \qquad \text{ove} \qquad z \in \mathfrak{p}_1^H, y = y_2 \cdots y_n \in \prod_{2 \leq j \leq n} \mathfrak{p}_j^H.$$

Si conclude che y è l'elemento cercato. **CVD** □

Osserviamo a margine che, con una scelta più accurata degli elementi y_i si può fare in modo che si abbia $v_i(x - x_i) = h_i$ per ogni i. Siamo quindi in grado di dimostrare il seguente

9.12 Teorema. *Sia A un dominio di Dedekind. Allora A è fattoriale se, e solo se, A è un dominio ad ideali principali.*

dim. È ben noto che A $PID \Rightarrow A$ UFD, e quindi si tratta di dimostrare l'implicazione nel verso opposto. Sia $\mathfrak{p} \neq (0)$ un ideale primo di A e sia $\pi \in \mathfrak{p}$ un elemento tale che $v_{\mathfrak{p}}(\pi) = 1$ e supponiamo che π sia irriducibile. Allora $(\pi) = \mathfrak{p}_1 \cdots \mathfrak{p}_h$ con $\mathfrak{p}_1 = \mathfrak{p} \neq \mathfrak{p}_j$ per $j \geq 2$. Se effettivamente apparisse un ideale $\mathfrak{p}_h \neq \mathfrak{p}$ nella fattorizzazione dell'ideale (π), allora, per il Teorema Cinese, esisterebbe un elemento $y \in A$ tale che $y \in \mathfrak{p}_j$ per $j \geq 2$, ma $y \notin \mathfrak{p}$. Allora $(y) = \mathfrak{p}_2 \cdots \mathfrak{p}_h \mathfrak{q}$ e $\mathfrak{q} \not\subset \mathfrak{p}$ e, preso un elemento $z \in \mathfrak{p}$ tale che $z \notin \mathfrak{p}_j$ per $j \geq 2$, si ha $yz \in (\pi)$ e quindi $yz = a\pi$ per qualche $a \in A$ senza che π divida né y né z, contro l'ipotesi che A sia un anello fattoriale. **CVD** □

Dunque, per sapere se l'anello degli interi di un corpo di numeri è un anello fattoriale, basta studiare il suo gruppo di classi di ideali.

9.13 Definizione. Sia A un dominio di Dedekind e sia K il suo corpo dei quozienti. Due ideali frazionari I e J si dicono *equivalenti*, e si scrive $I \sim J$, se esiste una costante $\alpha \in K^\times$ tale che $I = \alpha J$. Si verifica facilmente che si tratta di una relazione di equivalenza e che è compatibile col prodotto di ideali frazionari. Il *gruppo di classi di ideali* è il quoziente del gruppo degli ideali frazionari modulo questa relazione di equivalenza e si denota col simbolo $\mathrm{Cl}(A)$ o $\mathrm{Pic}\, A$.

Possiamo quindi concludere osservando che un dominio di Dedekind A è un anello fattoriale se, e solo se, $\mathrm{Cl}\, A = \{1\}$. Useremo tale criterio per decidere se gli interi di un dato un corpo di numeri formano o meno un anello fattoriale. Prima di occuparci di questo problema, diamo un ultimo risultato generale sulle relazioni tra ideali primi di estensioni intere; precisamente, dimostriamo il seguente

9.14 Teorema. *Sia A un dominio di Dedekind con corpo delle frazioni K e siano L un'estensione finita e separabile di K e B la chiusura integrale di A in L. Dato un ideale primo $\mathfrak{p}$ di A, sia $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$, e si indichi con f_i il grado su $A/\mathfrak{p}$ dell'estensione $B/\mathfrak{q}_i$, per $i = 1, \dots, r$(*). Nelle ipotesi che tutte le estensioni $B/\mathfrak{q}_i$ siano separabili su $A/\mathfrak{p}$, si ha*

$$[L : K] = \sum_{i=1}^{r} e_i f_i.$$

dim. Si consideri l'algebra $B/\mathfrak{p}B$ sul corpo $A/\mathfrak{p}$. Allora

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = [L : K],$$

Infatti, se si sostituisce A con il suo localizzato $A_{\mathfrak{p}}$, non cambia il corpo residuo $A/\mathfrak{p} = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ e, posto $B_{\mathfrak{p}} = B \otimes_A A_{\mathfrak{p}}$, si ha $B/\mathfrak{p}B = B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$. Basta quindi osservare che $B_{\mathfrak{p}}$ è un modulo libero su $A_{\mathfrak{p}}$, di rango uguale ad $[L : K]$ (cf. *Corollario I.3.9*).

In base al Teorema Cinese (cf. *Proposizione I.9.11*), si ha

$$B/\mathfrak{p}B = \prod_{i=1}^{r} B/\mathfrak{q}_i^{e_i}.$$

Considerando la catena discendente di $A/\mathfrak{p}$-spazi vettoriali

$$B/\mathfrak{q}_i^{e_i} \supset \mathfrak{q}_i/\mathfrak{q}_i^{e_i} \supset \mathfrak{q}_i^2/\mathfrak{q}_i^{e_i} \supset \cdots \supset \mathfrak{q}_i^{e_i-1}/\mathfrak{q}_i^{e_i},$$

ed osservando che $\mathfrak{q}_i^h/\mathfrak{q}_i^{h+1} \cong B/\mathfrak{q}_i$, per ogni intero positivo h, si ottiene la tesi. **CVD** □

(*) L'intero e_i è detto l'*indice di ramificazione* del primo $\mathfrak{q}_i$ su $\mathfrak{p}$, mentre l'intero f_i è detto il *grado residuo* di $\mathfrak{q}_i$ su $\mathfrak{p}$.

Poniamoci nelle ipotesi dell'*Esempio I.8.4*, e siano $B = A[\alpha]$, ed $f(X) \in A[X]$ il polinomio minimo di α. Dato un ideale $\mathfrak{p}$ di A, si consideri la decomposizione in fattori irriducibili nell'anello $A/\mathfrak{p}[X]$:

$$\bar{f}(X) = \bar{f}_1(X)^{e'_1} \cdots \bar{f}_r(X)^{e'_r}, \tag{9.15}$$

con i polinomi $f_i(X) \in A[X]$ monici, a due a due distinti (mod $\mathfrak{p}$). Come abbiamo già osservato nell'esempio citato, gli ideali primi di B contenenti $\mathfrak{p}$, sono della forma $\mathfrak{q}_i = \mathfrak{p}B + f_i(\alpha)B$, e si ha

$$B/\mathfrak{q}_i \cong \frac{A/\mathfrak{p}[X]}{(\bar{f}_i(X))} \qquad \text{e quindi} \qquad f_i = \dim_{A/\mathfrak{p}} B/\mathfrak{q}_i = \deg f_i(X).$$

Vogliamo mostrare che si ha $e_i = e'_i$. Dalla decomposizione (I.9.15), si ottiene che

$$\sum_{i=1}^{r} e'_i f_i = \deg f(X) = [L : K] = \sum_{i=1}^{r} e_i f_i$$

ed inoltre, essendo

$$\prod_{i=1}^{r} \mathfrak{q}_i^{e'_i} \subseteq \mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i},$$

si conclude che $e_i \leq e'_i$ per ogni $i = 1, \ldots, r$, da cui si ottiene l'uguaglianza voluta.

10. Applicazioni.

In questa sezione vogliamo esporre alcune applicazioni dei risultati sin qui ottenuti allo studio dei corpi di numeri e dei loro anelli di interi. Sia dunque A l'anello degli interi di un corpo di numeri K, di grado n su $\mathbb{Q}$, ed introduciamo una funzione degli ideali di A che generalizza la norma degli elementi.

10.1 Lemma. *Notazioni come sopra.*
(i) Preso comunque un ideale $I \neq (0)$ di A, $N(I) := \sharp(A/I)$ è un numero intero positivo.
(ii) Per ogni coppia di ideali non-nulli I e J si ha $N(IJ) = N(I)\,N(J)$.
(iii) Per ogni ideale principale $(\alpha) \neq (0)$, si ha $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.

dim. (i). È sufficiente osservare che $I \cap \mathbb{Z}$ è un ideale non-nullo di $\mathbb{Z}$ e che A è uno $\mathbb{Z}$-modulo libero finito, per concludere che $\sharp(A/I)$ è un numero intero positivo.
(ii). Se I e J sono coprimi, allora $A/IJ \cong A/I \times A/J$ e quindi la tesi è vera. Per dimostrarla in generale, ricordando che ogni ideale di A si decompone in un prodotto di ideali primi, è sufficiente verificare la tesi quando $I = \mathfrak{p}^r$ e $J = \mathfrak{p}^s$ per un qualche ideale primo $\mathfrak{p}$, e la verifica di viene immediata se si localizza in $\mathfrak{p}$ e si osserva che $A/\mathfrak{p}^n \cong A_\mathfrak{p}/(\mathfrak{p}A_\mathfrak{p})^n$ per ogni intero $n \geq 0$. *(iii).* La moltiplicazione per $\alpha \in A$ è un endomorfismo iniettivo dello $\mathbb{Z}$-modulo libero finito A e sia $M_\alpha \in M_{n \times n}(\mathbb{Z})$ la matrice di tale endomorfismo rispetto ad una base intera di A. Per il teorema dei divisori elementari, si ha $\sharp(A/(\alpha)) = |\det M_\alpha|$ e quindi la tesi (cf. I.2.10). **CVD** □

10.2 Osservazione. Osserviamo che, dalla definizione discende che $N(I)x \in I$ per ogni $x \in A$ e quindi che $N(I)\mathbb{Z} \subset I$. Dunque, i primi di A che dividono I sono da cercarsi tra i primi di A al di sopra dei primi razionali che dividono $N(I)$. Vogliamo mostrare che all'interno di ogni classe in $\mathrm{Cl}\,A$ esiste un ideale I con $N(I) < C_A$, ove C_A è una costante dipendente solo da A. Da ciò si conclude che gli ideali primi di A che stanno al di sopra dei primi razionali (positivi e) minori di C_A sono sufficienti a generare tutti gli elementi del gruppo $\mathrm{Cl}\,A$. In particolare, ciò significa che è sufficiente conoscere questa famiglia finita di primi per decidere se $\mathrm{Cl}\,A = (0)$ e quindi se A è o meno fattoriale.

Sia quindi $\{\omega_1, \ldots, \omega_n\}$ una base intera di A su $\mathbb{Z}$ (cf. *Definizione I.3.10*), e si consideri un ideale $I \neq (0)$. Allora, esiste un elemento $\alpha = x_1\omega_1 + \cdots + x_n\omega_n \neq 0$ di I per cui $|x_i| < N(I)^{1/n}$ per ogni

$i = 1, \dots, n$. Infatti, vi sono $[N(I)^{1/n}] + 1$ numeri interi compresi tra 0 ed $N(I)^{1/n}$, ed $[N(I)^{1/n}] + 1 > N(I)^{1/n}$. Considerando questi interi come coefficienti degli elementi della base intera $\{\omega_1, \dots, \omega_n\}$ di A, si ottengono $([N(I)^{1/n}] + 1)^n > N(I)$ elementi di A soddisfacenti alla condizione richiesta. Ciò significa che almeno due tali elementi stanno nella stessa classe in A/I e quindi la loro differenza è un elemento $\alpha = x_1\omega_1 + \dots + x_n\omega_n \neq 0$ di I per cui $|x_i| < N(I)^{1/n}$ per ogni $i = 1, \dots, n$.

Sia quindi I un ideale di A ed $\alpha \in I$ soddisfacente alle condizioni dette; allora I divide (α) per cui esiste un ideale J tale che $(\alpha) = IJ$. In base al Lemma precedente, da ciò si deduce che

$$|N_{K/\mathbb{Q}}(\alpha)| = N(\alpha) = N(I)N(J).$$

Ora, se $\alpha = x_1\omega_1 + \dots + x_n\omega_n$, con $|x_i| < N(I)^{1/n}$ per $i = 1, \dots, n$, i coniugati di α (in una chiusura algebrica $\bar{\mathbb{Q}}$ di $\mathbb{Q}$) sono tutti del tipo $\alpha^{(\mu)} = x_1\omega_1^{(\mu)} + \dots + x_n\omega_n^{(\mu)}$, al variare di μ tra le $\mathbb{Q}$-immersioni di K in $\bar{\mathbb{Q}}$. Da ciò si ottiene la disuguaglianza

$$|\alpha^{(\mu)}| \leq N(I)^{1/n} \sum_{i=1}^{n} |\omega_i^{(\mu)}|$$

e, facendo il prodotto al variare di μ, si deduce la disuguaglianza

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(I)C_A, \qquad \text{ove} \qquad C_A = \prod_{\mu} \left(\sum_{i=1}^{n} |\omega_i^{(\mu)}| \right). \tag{10.3}$$

Ciò permette di concludere che $N(J) \leq C_A$ ed essendo I scelto ad arbitrio e J un rappresentante della classe di I^{-1} in $\mathrm{Cl}\, A$, si conclude che *in ogni classe di ideali di A c'è un rappresentante J con $N(J) \leq C_A$*.

Da questa osservazione discende che è sufficiente considerare tutti i primi razionali minori di C_A e le loro fattorizzazioni in A per ottenere un numero finito di ideali che genera tutto $\mathrm{Cl}\, A$. In particolare, ciò costituisce un test effettivo per decidere se A è o meno un anello a fattorizzazione unica. Useremo questo criterio per discutere la fattorizzazione unica nei corpi quadratici immaginari.

10.4 Esempio. [*Corpi quadratici immaginari*] Sia quindi $d > 0$ un intero square-free e consideriamo il corpo quadratico immaginario $\mathbb{Q}(\sqrt{-d})$ ed il suo anello degli interi A. Se supponiamo che $-d \equiv 2, 3 \pmod 4$, allora $A = \mathbb{Z}[\sqrt{-d}]$ e $\{1, \sqrt{-d}\}$ è una base intera di A (cf. *Proposizione I.4.2*). Il polinomio minimo di $\sqrt{-d}$ è $X^2 + d$ e, ragionando come nell'*Esempio I.8.4*, se p è un primo razionale, si ha

- l'ideale pA è primo in A se il polinomio $X^2 = d$ è irriducubile in $\mathbb{Z}/p\mathbb{Z}[X]$ e quindi se, e solo se, $\left(\frac{-d}{p}\right) = -1$.
- l'ideale pA si spezza nel prodotto di due primi distinti in A se, e solo se, $\left(\frac{-d}{p}\right) = 1$.
- l'ideale pA è il quadrato di un ideale primo di A se p divide il discriminante di A, ovvero se, e solo se, $\left(\frac{-d}{p}\right) = 0$.

La costante C_A è uguale ad $(1 + \sqrt{d})^2 = 1 + d + 2\sqrt{d}$ ed osserviamo che, se d non è un primo, allora $A = \mathbb{Z}[\sqrt{-d}]$ non è un anello a fattorizzazione unica. Infatti, se $d = pd_1$ con $d_1 > 1$ e p un primo razionale, allora $pA = \mathfrak{p}^2$ ed $\mathfrak{p}$ non può essere un ideale principale di A. Se fosse $\mathfrak{p} = (\beta)$, con $\beta = x + y\sqrt{-d} \in A$, si avrebbe $pA = \beta^2 A$ e quindi $p = \pm\beta^2$ (perchè in A non vi sono invertibili diversi da ± 1). Da ciò si dedurrebbe $p^2 = N_{K/\mathbb{Q}}(\beta)^2 = (x^2 + dy^2)^2$ e quindi $p = x^2 + dy^2 > d$ e ciò è assurdo.

Si può mettere un'ulteriore restrizione ai primi d per cui $A = \mathbb{Z}[\sqrt{-d}]$ può essere un anello fattoriale. Infatti, se $d + 1 = 2pd_1$, e quindi $-d \equiv 1 \pmod p$, allora il primo p si spezza in A, ovvero $pA = \mathfrak{p}_1\mathfrak{p}_2$ con fp_1 e $\mathfrak{p}_2$ primi distinti di A, tra loro coniugati. Allora, se i due ideali fossero principali, si avrebbe $fp_1 = (\beta)$, $fp_2 = (\beta')$, e $p = \pm\beta\beta' = \pm N_{K/\mathbb{Q}}(\beta)$. Dunque, si avrebbe $p = x^2 + dy^2$, che è assurdo perchè $p \leq \frac{d+1}{2}$.

Supponiamo ora che $d \equiv -1 \pmod 4$, allora $A = \mathbb{Z}[\omega]$, ove $\omega = \frac{1+\sqrt{-d}}{2}$ e quindi $\{1, \omega\}$ è una base intera (cf. *Proposizione I.4.2*) e, posto $\Delta = \omega\omega' = \frac{1+d}{4}$, il polinomio minimo di ω è $f(X) = X^2 - X + \Delta$. Allora, ragionando come nell'*Esempio I.8.4*, si verifica facilmente che

- l'ideale $2A$ è primo se il polinomio $d \equiv 3 \pmod 8$, mentre è prodotto di due primi distinti se $d \equiv -1 \pmod 8$.

  Per quanto riguarda i primi $p > 2$ si ha, analogamente al caso precedente,
- l'ideale pA si spezza nel prodotto di due primi distinti in A se, e solo se, $\left(\frac{-d}{p}\right) = 1$.
- l'ideale pA ramifica se, e solo se, $\left(\frac{-d}{p}\right) = 0$.

  Vogliamo mostrare che, se d è sufficientemente grande,

$$\mathrm{Cl}(\mathbb{Z}[\omega]) = \{1\} \qquad \Longleftrightarrow \qquad f(x) \text{ è un numero primo se } 0 \leq x \leq \Delta - 1. \tag{10.5}$$

Supponiamo quindi che A sia un anello fattoriale ed osserviamo che, se per qualche primo p si ha $f(x) = x(x-1) + \Delta = pq$ con $p < q$ ed $x \leq \Delta - 1$, si ricava la disuguaglianza $p^2 < pq \leq (\Delta - 1)(\Delta - 2) + \Delta$. Inoltre, poichè $f(X)$ ha una radice modulo p, allora p è un primo che si spezza in A, si ha $p = \alpha\alpha'$ ove $\alpha = a - b\omega$ ed α' è il coniugato di α. Da ciò si deduce la relazione $p = a^2 - ab + b^2\Delta$ e quindi $4p = (a+b)^2 + db^2 > d$. Con un calcolo diretto, si verifica che le due disuguaglianze sono incompatibili e quindi $f(x)$ deve essere un numero primo.

Viceversa, supponiamo che per $0 < x \leq \Delta - 1$, $f(x) = p$ sia un primo razionale. In particolare, ciò significa che p è un primo che si spezza in $A = \mathbb{Z}[\omega]$ e supponiamo che si abbia $p \leq C_A = 1 + \Delta + 2\sqrt{\Delta}$, perchè sono questi i primi che ci interessano per conoscere $\mathrm{Cl}\,A$. Osservando che per ogni intero y, si ha $f(y) \equiv 0 \pmod p \quad \Leftrightarrow \quad f(p+1-y) \equiv 0 \pmod p$, possiamo supporre che si abbia $f(y) \equiv 0 \pmod p$ con $0 \leq y \leq \frac{p+1}{2}$. Si deduce quindi che deve aversi $y \leq \frac{\Delta}{2} + 1 + \sqrt{\delta}$ e, per d sufficientemente elevato (ad esempio $d > 40$), ciò implica $y \leq \Delta - 1$. Quindi deve aversi $f(y) = p$, ovvero $p = (y - \omega)(y - \omega')$ e quindi pA si spezza nel prodotto di due primi principali, che è quanto ci serviva per concludere la dimostrazione di (I.10.5).

Osserviamo che, la condizione precedente si può migliorare, per d elevato, nel modo seguente

$$f(x) \text{ è un numero primo se } 0 \leq x \leq \Delta - 1 \qquad \Longleftrightarrow \qquad f(x) \text{ è un numero primo se } 0 \leq x \leq \sqrt{\frac{4}{3}\Delta}.$$

Se d è elevato (ad esempio $d > 11$ e quindi $\Delta > 3$), allora $\sqrt{\frac{4}{3}\Delta} \leq \Delta - 1$ ed una delle implicazioni è ovvia. Sia quindi $f(x)$ un primo per $0 \leq x \leq \sqrt{\frac{4}{3}\Delta}$ e sia

$$x_0 = \min\{\, y \in \mathbb{Z}_{\geq 0} \,|\, f(y) \text{ non è primo} \,\}.$$

Si avrà dunque $p^2 \leq pq = x_0^2 - x_0 + \Delta$, ove p è un primo e $q \geq p$. Scelto un minimo intero $z \leq \frac{p+1}{2}$ tale che $f(z) \equiv 0 \pmod p$, si avrà $z = x_0$, oppure $\Delta \leq f(z) = p$. In quest'ultimo caso, si conclude che $\Delta^2 \leq p^2 \leq f(x_0)$, e quindi che $x_0 \geq \Delta$; se invece, $z = x_0$, allora si ottiene

$$p^2 \leq x_0^2 - x_0 + \Delta \leq \frac{p^2 - 1}{4} + \Delta$$

e quindi $p^2 \leq \frac{4}{3}\Delta - \frac{1}{4}$.

Non ci occuperemo del gruppo di classi di ideali nel caso di corpi quadratici reali, ma mostreremo come si possa migliorare la stima della costante C_A che permetteva di determinare un insieme finito di generatori per $\mathrm{Cl}\,A$ (cf. I.10.3). Ricordiamo che un *reticolo* (lattice) in uno spazio vettoriale reale

V è il sotto-$\mathbb{Z}$-modulo libero Λ generato da una base di V. Fissato un sistema di generatori liberi $\mathcal{V} = \{v_1, \dots, v_n\}$ di Λ, si chiama *dominio fondamentale* del reticolo Λ il sottoinsieme chiuso di V

$$\mathcal{F} = \left\{ \sum_{i=1}^{n} x_i v_i \mid 0 \leq x_i \leq 1, \text{ per } i = 1, \dots, n \right\}.$$

10.6 Teorema. [Teorema di Minkowski] *Sia Λ un reticolo in $\mathbb{R}^n$ con dominio fondamentale di volume M. Se $\mathcal{C}$ è una regione compatta, convessa, simmetrica rispetto all'origine, e di volume maggiore o uguale a $2^n M$, allora esiste un vettore $0 \neq x \in \Lambda \cap \mathcal{C}$.*

La dimostrazione discenderà dal seguente

10.7 Lemma. *Se $\mathcal{D}$ è una regione misurabile di volume maggiore di M, allora esistono due punti distinti $x, y \in \mathcal{D}$ con $x - y \in \Lambda$.*

dim. Sia $\mathcal{F}$ il dominio fondamentale di Λ e si considerino i sottoinsiemi del tipo $x + \mathcal{F}$, al variare di $x \in \Lambda$. Posto $\mathcal{D}_x = (x + \mathcal{F}) \cap \mathcal{D}$, allora si ha

$$\mathrm{Vol}(\mathcal{F}) = M < \mathrm{Vol}(\mathcal{D}) = \sum_{x \in \Lambda} \mathrm{Vol}(\mathcal{D}_x) = \sum_{x \in \Lambda} \mathrm{Vol}(\mathcal{F} \cap (\mathcal{D} - x)).$$

Dunque devono esistere $u, v \in \mathcal{D}$ ed $x \neq y$ in Λ tali che $u - x = v - y$, e quindi $u - v = x - y \in \Lambda \setminus \{0\}$. **CVD** □

Possiamo quindi dedurre da ciò la dimostrazione del *Teorema I.10.6*

dim. [del Teorema di Minkowski]. Se $\mathrm{Vol}(\mathcal{C}) > 2^n M$, siano α e β in $\frac{1}{2}\mathcal{C}$ con $\alpha - \beta \in \Lambda \setminus \{0\}$. Dunque, se scriviamo $\alpha = \frac{\alpha'}{2}$ e $\beta = \frac{-\beta'}{2}$ con $\alpha', \beta' \in \mathcal{C}$, poichè $\mathcal{C}$ è simmetrico rispetto all'origine e convesso, si conclude che $\alpha - \beta = \frac{\alpha' + \beta'}{2} \in \Lambda \cap \mathcal{C}$. Per concludere nel caso in cui sia $\mathrm{Vol}(\mathcal{C}) = 2^n M$, si possono considerare gli insiemi $\mathcal{C}_n = (1 + \frac{1}{n})\mathcal{C}$ ed ottenere degli elementi $0 \neq x_n \in \Lambda \cap \mathcal{C}_n$ ed osservare che tali elementi stanno in un insieme compatto, discreto e contenuto in una regione limitata. Dunque esiste una sottosuccessione costante che perciò, converge ad un elemento di $\Lambda \cap \mathcal{C}$. **CVD** □

Applichiamo il Teorema di Minkovski ai corpi quadratici immaginari allo scopo di migliorare la stima della costante C_A che compare in (I.10.3). Sia quindi $K = \mathbb{Q}(\sqrt{-d})$ con $d > 0$, square-free e $d \not\equiv 3 \pmod 4$. In tal caso l'anello degli interi di K è $A = \mathbb{Z}[\sqrt{-d}]$, ed un ideale $I \subseteq A$ corrisponde ad un reticolo in $\mathbb{C}$, il cui dominio fondamentale ha area uguale a $N(I)$. Dato un elemento $z = a + b\sqrt{-d} \in A$, si ha $N_{K/\mathbb{Q}}(x) = a^2 + db^2$, e quindi usiamo il teorema di Minkowski per determinare un valore minimo di λ affinchè l'insieme

$$C_\lambda = \left\{ z \in \mathbb{C} \,|\, z = x + y\sqrt{-d}, \quad (x, y) \in \mathbb{R}^2, \quad x^2 + dy^2 \leq \lambda \right\}$$

intersechi I in un elemento non nullo α, ed ottenere così una stima della norma di α in funzione di $N(I)$. In base al Teorema di Minkovski, è sufficiente che si abbia $\mathrm{Vol}\, C_\lambda \geq 4N(I)$ affinché vi sia $0 \neq \alpha \in I$, di norma $N_{K/\mathbb{Q}}(\alpha) = \lambda$. Essendo $\mathrm{Vol}\, C_\lambda = \frac{\lambda\pi}{\sqrt{d}}$, si deduce la relazione

$$N_{K/\mathbb{Q}}(\alpha) = \frac{4\sqrt{d}}{\pi} N(I), \tag{10.8}$$

che migliora la stima (I.10.3).

Osserviamo infine che quest'ultima osservazione non si può applicare nel caso dei corpi quadratici reali perchè, in tal caso, gli insiemi C_λ non sono convessi.

Concludiamo questa sezione ricordando due importanti stime per la costante C, per cui si abbia $N_{K/\mathbb{Q}}(\alpha) \leq C\, N(I)$, ove I è un qualsiasi ideale dell'anello degli interi del corpo di numeri K.

- Si può prendere
$$C = |\sqrt{\Delta}|\,\frac{2^{2t}\,d!}{\pi^t\,d^d}, \qquad \text{[\textit{stima di Minkovski}]}$$
ove Δ è il discriminante di K, $d = [K : \mathbb{Q}]$ e $2t$ è il numero di immersioni non-reali di K in $\mathbb{C}$. Come si vede facilmente, questa stima si riduce a (I.10.8) nel caso dei corpi quadratici immaginari.
- Si può prendere
$$C = |\Delta| \left(\frac{r}{d}\right)^d, \qquad \text{[\textit{stima di Siegel}]}$$
nel caso di un corpo totalmente reale, ove r è la parte intera di $d/6$ se $d \equiv 1 \pmod 6$, mentre $r = \left[\frac{d}{6}\right] + 1$ altrimenti.

II
Il Teorema di Hasse e Minkowski

1. Valori assoluti

In questa sezione ci occuperemo dei valori assoluti –detti anche valutazioni di rango 1– sul corpo $\mathbb{Q}$ dei numeri razionali e della loro classificazione.

1.1 Definizioni. Un *valore assoluto* sul corpo K è un omomorfismo di gruppi moltiplicativi $f : K^\times \to \mathbb{R}^\times_{>0}$, soddisfacente alla condizione $f(x + y) \geq f(x) + f(y)$. Tale omomorfismo si estende a tutto K ponendo $f(0) = 0$.

Ad un valore assoluto f su K resta associata una *metrica*, definita ponendo

$$d_f(x, y) := f(x - y) \qquad \text{per ogni } x, y \in K,$$

ed è facile verificare che tale metrica rende K un corpo topologico.

Infine, diremo che due valori assoluti sono *equivalenti* se le metriche associate inducono la stessa topologia.

Si chiama *valore assoluto banale* il valore assoluto definito ponendo $f(x) = 1$ per ogni $x \in K^\times$. Si verifica facilmente che tale valore assoluto induce la topologia discreta su K.

Vogliamo dare una facile caratterizzazione di valori assoluti tra loro equivalenti.

1.2 Proposizione. *Siano f e g due valori assoluti sul corpo K. Allora f e g sono equivalenti se, e solo se, esiste una costante positiva $c \in \mathbb{R}$ tale che $f(x) = g(x)^c$ per ogni $x \in K$.*

dim. Si osservi che, se f e g sono due valori assoluti ed $f(x) = g(x)^c$ per ogni $x \in K$ allora è facile verificare che inducono la stessa topologia, considerando ad esempio delle sfere centrate nell'origine ed osservando che $B_f(0, r^c) = B_g(0, r)$ per ogni raggio positivo r.

Dimostriamo quindi l'implicazione nel verso contrario e cominciamo con il caso in cui uno dei valori assoluti, sia g, è banale. Si osservi che, se f induce la topologia discreta su K, non può esistere un elemento $x \in K^\times$ con $f(x) \neq 1$, perchè, in tal caso una delle due successioni $(x^n)_{n\in\mathbb{N}}$ ed $(x^{-n})_{n\in\mathbb{N}}$ convergerebbe a zero senza annullarsi mai. Il che dimostra la tesi nel caso di valori assoluti banali.

Sia quindi f non banale e si fissi un elemento $x_0 \in K$ con $0 < f(x_0) < 1$ e si osservi che allora si ha $\lim_{k\to\infty} x_0^k = 0$ e quindi $g(x_0) < 1$. Inoltre, fissato comunque $x \in K$ esiste un esponente $r \in \mathbb{R}$ tale che $f(x) = f(x_0)^r$ e, a meno di sostituire x con x^{-1}, possiamo supporre che sia $r \geq 0$. Analogamente, si avrà $g(x) = g(x_0)^s$, per qualche $s \in \mathbb{R}_{\geq 0}$. Allora, se $r < \frac{m}{n} \in \mathbb{Q}$, si ha $f(x_0)^{m/n} < f(x_0)^r = f(x)$ e quindi $f(x_0^m) < f(x^n)$, ovvero $f(x_0^m/x^n) < 1$, da cui si deduce che la successione $((x_0^m/x^n)^k)_{k\in\mathbb{N}}$ converge a zero in K e deve quindi aversi $g(x_0^m/x^n) < 1$, ovvero $g(x_0)^{m/n} < g(x)$. Dunque si ha $s < \frac{m}{n}$, e poichè un risultato analogo vale per ogni approssimazione razionale di r, si conclude che $r = s$. Si conclude quindi che

$$r = \frac{\log f(x)}{\log f(x_0)} = \frac{\log g(x)}{\log g(x_0)} \qquad \text{e quindi} \qquad \log f(x) = c \log g(x), \text{ ove } c = \frac{\log f(x_0)}{\log g(x_0)},$$

che, data l'arbitrarietà di x, è ciò che dovevamo dimostrare. **CVD** □

Mettiamo in evidenza una classe importante di valori assoluti

1.3 Definizione. Un valore assoluto $f : K \to \mathbb{R}$ si dice *non-archimedeo* se vale la condizione ulteriore $f(x+y) \leq \sup(f(x), f(y))$, per ogni $x, y \in K$.

Sia f un valore assoluto ed osserviamo che, usualmente la propietà archimedea, che vale ad esempio per l'usuale valore assoluto dei numeri reali, si esprime nella forma seguente:

$$\text{dati comunque } a, b \in K^\times \text{ esiste } n \in \mathbb{N} \text{ tale che } f(na) > f(b). \tag{1.4}$$

In realtà le due formulazioni sono equivalenti e, più in generale, vale la seguente

1.5 Proposizione. *Sia $f : K \to \mathbb{R}$ un valore assoluto non banale sul corpo K. Le seguenti condizioni sono equivalenti:*

(a) f è non-archimedeo;
(b) $f(n) \leq 1$ per ogni intero positivo n;
(c) $f(n) \leq B$ per ogni intero positivo n;
(d) non vale la (II.1.4).

dim. La verifica che $(a) \Leftarrow (b) \Leftarrow (c)$ è immediata. Per vedere che $(c) \Leftarrow (d)$, si può ragionare così: se vale la proprietà (II.1.4), preso comunque un elemento $b \in K$, esiste un numero naturale n tale che $f(b) < f(n)$ e quindi $f(b) \leq B$ per ogni $b \in K$ e quindi f è imitato e perciò banale. Ma il valore assoluto banale non può soddisfare ad (II.1.4) e ciò permette di concludere. D'altra parte, è facile vedere che $(d) \Leftarrow (c)$; infatti, se non vale la (II.1.4) devono esistere due elementi $a, b \in K^\times$, tali che $f(na) \leq f(b)$ per ogni $n \in \mathbb{N}$ e perciò si conclude che $f(n) \leq B = \frac{f(b)}{f(a)}$ per ogni $n \in \mathbb{N}$.

Dunque, per concludere è sufficiente mostrare che $(c) \Leftarrow (a)$. Infatti, dati $x, y \in K$ e posto $M = \sup(f(x), f(y))$, si ha

$$f(x+y)^n = f\left(\sum_{h=0}^{n} \binom{n}{h} x^h y^{n-h}\right) \leq \sum_{h=0}^{n} f(\binom{n}{h})\, M^n \leq BM^n(n+1).$$

Se ne deduce quindi che, per ogni intero positivo n, vale la disuguaglianza $f(x+y) \leq (B(n+1))^{1/n} M$ che, passando al limite per $n \to \infty$, permette di concludere. **CVD** □

Vogliamo occuparci ora specificamente dei valori assoluti sul corpo $\mathbb{Q}$ dei numeri razionali. Ricordiamo che su $\mathbb{Q}$, si possono porre il valore assoluto banale, l'usuale valore assoluto archimedeo, indotto dall'ordinamento naturale, che indicheremo con $|x|_\infty$ per ogni $x \in \mathbb{Q}$ ed inoltre, per ogni numero primo p, il valore assoluto p-adico, definito dalla posizione $|x|_p = p^{-v}$, ove l'intero v soddisfa alla condizione $x = p^v \frac{r}{s}$ con r ed s entrambi primi con p. Si può verificare che i valori assoluti p-adici sono tutti non-archimedei.

Vogliamo mostrare che quelli appena descritti sono, a meno di equivalenza, tutti i possibili valori assoluti sul corpo $\mathbb{Q}$.

1.6 Teorema. [Ostrowski] *Ogni valore assoluto non banale su $\mathbb{Q}$ è equivalente al valore assoluto archimedeo oppure ad uno dei valori assoluti p-adici.*

dim. Sia dunque $f : \mathbb{Q} \to \mathbb{R}$ un valore assoluto non banale e siano dati due numeri naturali $m \geq n > 1$. Scriviamo m in base n, nella forma

$$m = a_0 + a_1 n + \cdots + a_r n^r, \qquad \text{con } 0 \leq a_i \leq n-1, \text{ per } i = 0, \ldots, r \text{ e } a_r \neq 0.$$

Applicando f si ottiene

$$f(m) \leq \sum_{i=0}^{r} f(a_i) f(n)^i \leq B \sum_{i=0}^{r} f(n)^i \leq B(r+1)\sup(1, f(n)^r),$$

ove $B = \max_{j=0,\dots,n-1} f(j)$.

Dalla disuguaglianza $n^r < m$, si deduce $r \leq \frac{\log m}{\log n}$ e quindi

$$f(m) \leq B\left(\frac{\log m}{\log n} + 1\right) \sup(1, f(n)^{\frac{\log m}{\log n}}).$$

Fissato un intero M e prendendo $m = M^k$, si ottiene quindi

$$f(M) \leq B^{1/k}\left(k\frac{\log M}{\log n} + 1\right) 1/k \sup(1, f(n)^{\frac{\log M}{\log n}}), \tag{1.7}$$

da cui, passando al limite per $k \to \infty$, si ottiene la disuguaglianza

$$f(M) \leq \sup(1, f(n)^{\frac{\log M}{\log n}}).$$

Se f è archimedea, esiste un intero M con $f(M) > 1$ (cf. *Proposizione II.1.5*) e dalla disuguaglianza si deduce che $f(n) > 1$ per ogni $n > 1$ e dunque, che si ha $f(M)^{1/\log M} \leq f(n)^{1/\log n}$ e quindi, scambiando i ruoli di M ed n, si ottiene

$$f(M)^{1/\log M} = f(n)^{1/\log n} \qquad \text{per ogni coppia di interi } M, n.$$

Si conclude perciò che il rapporto $\alpha = \dfrac{\log f(n)}{\log n}$ è indipendente da n e quindi che $f(x) = |x|_\infty^\alpha$, per ogni $x \in \mathbb{Q}$.

Supponiamo ora che f sia non-archimedea. Allora, l'insieme

$$\mathcal{M} = \{\, n \in \mathbb{Z} \mid f(n) < 1 \,\}$$

è un ideale primo, non banale, di $\mathbb{Z}$ e si deduce dalla formula (II.1.7) che f è equivalente a $|\ |_p$, ove p è un generatore di $\mathcal{M}$. **CVD** □

Indichiamo con $\mathcal{V} = \{\, p \in \mathbb{Z} \mid p \text{ è primo} \,\} \cup \{\infty\}$ l'insieme delle classi di equivalenza dei valori assoluti su $\mathbb{Q}$ (i *posti* di $\mathbb{Q}$) e scegliamo per ogni $v \in \mathcal{V}$ il valore assoluto $|\ |_v$, opportunamente normalizzato, ovvero l'usuale valore assoluto se $v = \infty$ (per cui si ha $|n|_\infty = n$ per ogni $n \in \mathbb{N}$) ed il valore assoluto p-adico se $v = p$ (per cui si ha $|p|_p = p^{-1}$). Con queste normalizzazioni vale la seguente

$$[\textit{formula del prodotto}] \qquad \prod_{v \in \mathcal{V}} |x|_v = 1 \quad \text{per ogni } x \in \mathbb{Q}^\times. \tag{1.8}$$

Il corpo $\mathbb{Q}$ può essere completato rispetto a ciascuna delle metriche indotte dai valori assoluti $|\ |_v$ e si ha $\mathbb{Q}_\infty = \mathbb{R}$, mentre si indica con $\mathbb{Q}_p$ il completamento rispetto al valore assoluto p-adico. Si verifica facilmente che, trattandosi di valori assoluti non-archimedei, le sfere

$$B(0, 1^+) = \{\, x \in \mathbb{Q}_p \mid |x|_p \leq 1 \,\} =: \mathbb{Z}_p \qquad \text{e} \qquad B(0, 1^-) = \{\, x \in \mathbb{Q}_p \mid |x|_p < 1 \,\} =: \mathfrak{m}_p$$

sono rispettivamente un sottoanello di $\mathbb{Q}_p$ ed un ideale massimale di tale anello; inoltre si ha $\mathbb{Q}_p = Frac\,\mathbb{Z}_p$(*). L'ideale $\mathfrak{m}_p$ contiene tutti gli elementi non-invertibili di $\mathbb{Z}_p$ ed è generato dal primo p, si conclude che $\mathbb{Z}_p$ è un DVR (cf. *Proposizione I.9.3*) e la relazione tra la valutazione discreta $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ ed il valore assoluto p-adico è data dall'identità

$$|x|_p = p^{-v_p(x)} \qquad \text{per ogni } x \in \mathbb{Q}_p.$$

Vogliamo illustrare ora alcune proprietà topologiche dei completamenti p-adici di $\mathbb{Q}$.

(*) Si potrebbe mostrare che $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, ove le freccie di connessione sono le proiezioni naturali tra i quozienti.

1.9 Proposizione. *L'anello $\mathbb{Z}_p$ è compatto e totalmente sconnesso. Dunque $\mathbb{Q}_p$ è localmente compatto e totalmente sconnesso.*

dim. Si osservi che, ogni sfera di $\mathbb{Q}_p$ è simultaneamente aperta e chiusa ed è omeomorfa a $\mathbb{Z}_p$, essendo

$$B(x, p^{-m,+}) = \{\, y \in \mathbb{Q}_p \,|\, |y-x|_p \leq p^{-m} \,\} = \{\, x+u \,|\, v_p(u) \geq m \,\} = x + p^m\mathbb{Z}_p = B(x, p^{-m+1,-}).$$

Da ciò discende che $\mathbb{Q}_p$ è totalmente sconnesso e che è sufficiente dimostrare che $\mathbb{Z}_p$ è compatto per concludere. Per fare ciò mostriamo che vale il criterio di Bolzano-Weierstrass, ovvero che da ogni successione in $\mathbb{Z}_p$ si può estrarre una sottosuccessione convergente. Sia quindi $(x_n)_{n\in\mathbb{N}}$ una successione in $\mathbb{Z}_p$ e sia $S = \{\, x_n \,|\, n \in \mathbb{N} \,\}$ un insieme infinito. Poichè il quoziente $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ è finito, esiste un elemento $x_{n(1)}$ di S tale che l'insieme $S_1 = \{\, x_n \,|\, n \geq n(1),\ v_p(x_n - x_{n(1)}) \geq 1 \,\}$ contenga infiniti elementi. Considerando l'immagine di S_1 nel quoziente finito $\mathbb{Z}_p/p^2\mathbb{Z}_p \cong \mathbb{Z}/p^2\mathbb{Z}$, ottengo che esiste un elemento $x_{n(2)}$ di S_1 tale che l'insieme $S_2 = \{\, x_n \,|\, n \geq n(2),\ v_p(x_n - x_{n(1)}) \geq 2 \,\}$ contenga infiniti elementi. Ragionando analogamente, si costruisce una sottosuccessione $(x_{n(k)})_{k\in\mathbb{N}}$, che soddisfa alla condizione di Cauchy, perchè $|\ |_p$ è un valore assoluto non-archimedeo e si ha $v_p(x_{n(k)} - x_{n(k+1)}) \geq k$, ovvero $|x_{n(k)} - x_{n(k+1)}|_p \leq p^{-k}$ per ogni $k \in \mathbb{N}$. **CVD** □

Si osservi che, per costruzione, l'anello degli interi $\mathbb{Z}$ è denso in $\mathbb{Z}_p$ e $\mathbb{Q}$ è denso nel suo completamento $\mathbb{Q}_p$. Ciò si estende al prodotto finito di completamenti di $\mathbb{Q}$ nel modo seguente.

1.10 Proposizione. [Principio di approssimazione debole] *Per ogni sottoinsieme finito $S \subset \mathcal{V}$, l'immagine di $\mathbb{Q}$ tramite l'immersione diagonale $\mathbb{Q} \to \prod_{v\in S} \mathbb{Q}_v$ è densa.*

dim. Osserviamo che, se $\infty \notin S$, allora il risultato discende dall'usuale teorema cinese del resto. Si scriva quindi $S = \{\infty\} \cup S'$, con $S' = \{p_1, \dots, p_n\}$ e indichiamo con $(x_\infty, x_1, \dots, x_n)$ un generico elemento di $\prod \mathbb{Q}_v$. Dobbiamo quindi mostrare che fissati comunque un tale elemento ed un numero reale positivo ε,

esiste un numero razionale $x \in \mathbb{Q}$ tale che $|x - x_\infty|_\infty < \varepsilon$ e $|x - x_i|_{p_i} < \varepsilon$ per $i = 1, \dots, n$. A meno di moltiplicare per un prodotto del tipo $p_1^{m_1} \cdots p_n^{m_n}$, si può supporre che $x_i \in \mathbb{Z}_{p_i}$ per ogni $i = 1, \dots, n$ e quindi, per il Teorema citato, in corrispondenza ad un qualunque numero reale positivo δ, esiste un intero $y \in \mathbb{Z}$ tale che $|y - x_i|_{p_i} < \varepsilon$ per $i = 1, \dots, n$; inoltre la condizione resta vera se sostituisco ad y numeri razionali del tipo $y + (p_1 \cdots p_n)^M u$, per M sufficientemente elevato ed $|u|_{p_i} \leq 1$ per ogni $i = 1, \dots, n$. Si tratta quindi di determinare u affinché si abbia

$$|y + (p_1 \cdots p_n)^M u - x_\infty|_\infty < \varepsilon \qquad \text{ovvero} \qquad \left| \frac{y - x_\infty}{(p_1 \cdots p_n)^M} + u \right| < \frac{\varepsilon}{(p_1 \cdots p_n)^M}.$$

È chiaro che si possono trovare dei numeri razionali soddisfacenti a questa condizione, che non contengano nessuno dei p_i al denominatore. **CVD** □

Da ultimo, diamo qualche cenno ai prolungamenti dei valori assoluti p-adici di $\mathbb{Q}$ alle sue estensioni finite. Se L è un'estensione di $\mathbb{Q}$ di grado n, per il Teorema dell'elemento primitivo (cf. *Proposizione I.2.2*), possiamo supporre che sia $L = \mathbb{Q}(\alpha)$ ed indicare con $F(X) = a_0 + a_1 X = \dots + X^n \in \mathbb{Q}[X]$ il polinomio minimo di α. Indicato con $\mathcal{O}_L$ l'anello degli interi di L (ovvero la chiusura integrale di $\mathbb{Z}$ in L), si avrà $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, ove gli $\mathfrak{p}_j$ sono primi distinti di $\mathcal{O}_L$ e si ha $n = \sum_{i=1}^r e_i f_i$, ove $f_i = [\mathcal{O}_L/\mathfrak{p}_i : \mathbb{F}_p]$ per $i = 1, \dots, r$ (cf. *Teorema I.9.14*). Allora si può dimostrare che *esistono esattamente r estensioni $g_1, \dots, g_r$ del valore assoluto $|\ |_p$ ad L, rispettivamente con indici di ramificazione $e_1, \dots, e_r$ e tali che per ogni $i = 1, \dots, r$ si abbia $\{\, x \in L \,|\, g_i(x) \leq 1 \,\} = \mathcal{O}_{L,\mathfrak{p}_i}$.*

In particolare, si può osservare che $L \otimes_{\mathbb{Q}} \mathbb{Q}_p$ è somma diretta di r corpi $L_1, \dots, L_r$, di grado $[L_i : \mathbb{Q}_p] = f_i e_i$, determinati in corrispondenza alla decomposizione in fattori irriducibili di $F(X)$ in $\mathbb{Q}_p[X]$. Uno studio ulteriore potrebbe determinare la ramificazione di p nelle singole estensioni.

Non dimostriamo queste asserzioni[(*)], ci limitiamo invece ad illustrare l'esempio di un'estensione quadratica di $\mathbb{Q}$. Sia quindi $L = \mathbb{Q}(\sqrt{d})$ ove d è un intero square-free e sia p un primo tale che $p \nmid 2d$. Se $\left(\frac{d}{p}\right) = 1$, ovvero se d è un quadrato modulo p, allora esiste un elemento $\alpha \in \mathbb{Q}_p$ tale che $\alpha^2 = d$ (si veda il successivo *Corollario II.2.4*), e quindi vi sono due immersioni distinte di L in $\mathbb{Q}_p$ (che mandano $\sqrt{d}$ in α e $-\alpha$ rispettivamente) e le restrizioni di $|\ |_p$ all'immagine forniscono le due estensioni del valore assoluto p-adico da $\mathbb{Q}$ ad L. In particolare, dall'esistenza di α, si deduce $\mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \oplus \mathbb{Q}_p$.

D'altro canto, se $\left(\frac{d}{p}\right) = -1$, allora d non è un quadrato in $\mathbb{Q}_p$ e perciò $\mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p(\sqrt{d})$. In particolare, vi è un'unica estensione $|\ |$ del valore assoluto $|\ |_p$, che può essere determinata in questo modo: se $\beta \in \bar{\mathbb{Q}}_p$ è una radice quadrata di d ($\beta^2 = d$), allora posto $c = |a + b\beta| = |a - b\beta|$ (due elementi coniugati hanno la stessa valutazione), si ha $c^2 = |a + b\beta|\,|a - b\beta| = |a^2 + db^2|_p$, e quindi deve essere $|x| = |N_{L/\mathbb{Q}}(x)|_p^{1/2}$ per ogni $x \in L$.

2. Equazioni polinomiali p-adiche

Dato un polinomio $f(X) \in \mathbb{Z}_p[X_1, \dots, X_n]$ indicheremo con $f_m(X)$ il polinomio che si ottiene riducendo modulo p_m i coefficienti di $f(X)$.

2.1 Proposizione. *Sia $f(X) \in \mathbb{Z}_p[X_1, \dots, X_n]$. Le seguenti affermazioni sono equivalenti*
(i) esiste $a = (a_1, \dots, a_n) \in \mathbb{Z}_p^n$ tale che $f(a) = 0$;
(ii) la congruenza $f(X) \equiv 0 \pmod{p}^m$ ha soluzione per ogni $m \geq 0$.

dim. È chiaro che $(i) \Rightarrow (ii)$. Viceversa se, per ogni m, si indica con $a^{(m)} = (a_1^{(m)}, \dots, a_n^{(m)}) \in \mathbb{Z}_p^n$ una soluzione della congruenza $f(X) \equiv 0 \pmod{p}^m$, ricordando che $\mathbb{Z}_p$ è compatto (cf. *Proposizione II.1.9*), si conclude che esiste una sottosuccessione convergente di soluzioni delle congruenze che converge quindi ad uno zero di $f(X)$. **CVD** □

Per i polinomi omogenei, il risultato si può rafforzare introducendo il concetto di n-upla *primitiva*, ovvero di un n-upla $(x_1, \dots, x_n) \in \mathbb{Z}_p^n$, tale che $\sup |x_i|_p = 1$. Possiamo quindi enunciare la seguente Proposizione la cui dimostrazione si ottiene da un facile adattamento degli argomenti della dimostrazione precedente.

2.2 Proposizione. *Sia $f(X) \in \mathbb{Z}_p[X_1, \dots, X_n]$ un polinomio omogeneo. Le seguenti affermazioni sono equivalenti*
(i) esiste $a = (a_1, \dots, a_n) \in \mathbb{Q}_p^n \setminus \{(0, \dots, 0)\}$ tale che $f(a) = 0$;
(ii) esiste un n-upla primitiva $a = (a_1, \dots, a_n) \in \mathbb{Z}_p^n$ tale che $f(a) = 0$;
(iii) la congruenza $f(X) \equiv 0 \pmod{p}^m$ ha soluzioni primitive per ogni $m \geq 0$.

In base alle osservazioni fatte, possiamo enunciare il metodo di approssimazione di Newton delle soluzioni di un'equazione (cf. *Lemma I.6.9*) nel modo seguente.

2.3 Proposizione. *Siano dati $f(X) \in \mathbb{Z}_p[X_1, \dots, X_n]$ e due interi k, m con $0 \leq 2k < m$. Dato $a = (a_1, \dots, a_n) \in \mathbb{Z}_p^n$ tale che*

$$f(a) \equiv 0 \pmod{p}^m \qquad e \qquad v_p\left(\frac{\partial f}{\partial x_j}\right) = k \text{ per qualche } j = 1, \dots, n,$$

allora esiste $x = (x_1, \dots, x_n) \in \mathbb{Z}_p^n$ tale che $f(x) = 0$ e $v_p(x_i - a_i) \geq m - k$ per $i = 1, \dots, n$.

Questo risultato ha interessanti conseguenze che andiamo ad enunciare per le equazioni polinomiali in $\mathbb{Q}_p$ ed in particolare per le forme quadratiche.

(*) Il lettore interessato può trovare una dimostrazione di queste affermazioni nei §§. 2 e 3 del Capitolo II di J.-P. Serre, *Corps Locaux*, Hermann 1962.

2.4 Corollario. *Sia $f(X) \in \mathbb{Z}_p[X_1, \dots, X_n]$ un polinomio. Ogni zero semplice*[†] *di f_1 in $(\mathbb{Z}/p\mathbb{Z})^n$ si rialza ad uno zero di f in $\mathbb{Z}_p^n$.*

2.5 Corollario. *Sia $p \neq 2$ e si consideri una forma quadratica*

$$f(X) = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_n]$$

con $a_{ij} = a_{ji}$ e $\det(a_{ij}) \in \mathbb{Z}_p^\times$. Dato $a \in \mathbb{Z}_p$, ogni soluzione primitiva della congruenza $f(x) \equiv a \pmod p$ si rialza ad una soluzione (primitiva) di $f(x) = a$.

dim. Sia y una soluzione primitiva della congruenza. In base al risultato precedente è sufficiente verificare che una almeno tra le derivate parziali di f non si annulla, modulo p, in y. e ciò è vero perchè

$$\frac{\partial f}{\partial X_j} = 2 \sum_{i=1}^{n} a_{ij} X_i, \qquad \det(a_{ij}) \not\equiv 0 \pmod p, \qquad y \text{ è primitiva.}$$

In tal modo si conclude. **CVD** □

Consideriamo infine il caso in cui $p = 2$, che richiede una qualche cautela.

2.6 Corollario. *Sia $p = 2$ e si consideri una forma quadratica*

$$f(X) = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j \in \mathbb{Z}_2[X_1, \dots, X_n]$$

con $a_{ij} = a_{ji}$. Dato $a \in \mathbb{Z}_2$, Se y è una soluzione primitiva della congruenza $f(x) \equiv a \pmod 8$, y si rialza ad una soluzione (primitiva) dell'equazione $f(x) = a$ se una almeno tra le derivate parziali di f non si annulla in y modulo 4. In particolare, quest'ultima condizione è soddisfatta se $\det(a_{ij}) \in \mathbb{Z}_2^\times$.

L'asserzione si dimostra applicando la Proposizione nel caso in cui $m = 3$ e $k = 1$ e ragionando poi come nel caso in cui $p \neq 2$.

Nel seguito di questo numero applicheremo i risultati precedenti allo studio dei gruppi $\mathbb{Z}_p^\times$ e $\mathbb{Q}_p^\times$. Prima di fare ciò, vogliamo generalizzare ai completamenti p-adici un risultato ben noto per i numeri reali (completamento archimedeo di $\mathbb{Q}$).

2.7 Proposizione. *Il corpo $\mathbb{Q}_p$ non ha automorfismi diversi dall'identità.*

dim. Osserviamo che ogni automorfismo induce l'identità sul sottocorpo fondamentale $\mathbb{Q}$, che è denso in $\mathbb{Q}_p$ e quindi è sufficiente dimostrare che ogni automorfismo di $\mathbb{Q}_p$ è continuo[*]. Si consideri il sottogruppo moltiplicativo

$$U_1 = \left\{ x \in \mathbb{Q}_p^\times \mid \forall m \in \mathbb{N},\, (m,p) = 1,\ x = y^m\ \exists y \in \mathbb{Q}_p \right\}.$$

È chiaro che, per ogni automorfismo σ di $\mathbb{Q}_p$, deve aversi $\sigma(U_1) \subseteq U_1$, quindi, se mostriamo che $U_1 = 1 + p\mathbb{Z}_p$, si conclude che $\sigma(p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$, che è sufficiente per verificare che σ è continuo. Dunque, se $x \in U_1$ allora deve aversi $v_p(x) = m v_p(y)$ per infiniti interi m e quindi $v_p(x) = 0$. Inoltre, deve aversi $x \equiv y^{p-1} \equiv 1 \pmod p$, perchè il gruppo moltiplicativo di $\mathbb{F}_p$ è ciclico, di periodo $p - 1$. Dunque $U_1 \subseteq 1 + p\mathbb{Z}_p$. D'altra parte, se $u \in 1 + p\mathbb{Z}_p$, la congruenza $X^m \equiv u \pmod p$ ha una soluzione non

---

(†) Se $F(X_1, \dots, X_n)$ è un polinomio a coefficienti in un corpo, uno zero x di F si dice *semplice* se una almeno tra le derivate $\frac{\partial F}{\partial X_i}$ non si annulla in x.

(*) Nel caso del corpo reale, ciò si vede osservando che i positivi sono quadrati in $\mathbb{R}$, e perciò ogni automorfismo conserva l'ordinamento dei numeri reali ed è quindi continuo per il valore assoluto archimedeo.

nulla che non annulla la derivata se $(m,p)=1$. Dunque, per il *Corollario II.2.4*, possiamo concludere che $u \in U_1$. **CVD** □

2.8 Remarks. *(a).* Dato un elemento $u \in 1+p\mathbb{Z}_p$ si poteva verificare l'esistenza di radici m-esime di u in $\mathbb{Q}_p$, osservando che la serie binomiale

$$(1+X)^{1/m} = \sum_{h\geq 0} \binom{1/m}{h} X^h$$

ha i coefficienti in $\mathbb{Z}_p$ se $(m,p)=1$ e perciò converge (assolutamente) per ogni $x \in p\mathbb{Z}_p$[†] e la sua somma è una radice m-esima di $1+x$ per il principio di identità. Un modo semplice per vedere che per $\alpha \in \mathbb{Z}_p$ ed $h \in \mathbb{N}$ i coefficienti binomiali $\binom{\alpha}{h} = \frac{\alpha(\alpha-1)\cdots(\alpha-h+1)}{h!}$ appartengono a $\mathbb{Z}_p$ è osservare che ogni elemento di $\mathbb{Z}_p$ è limite di una successione di interi razionali[‡] $(\alpha_n)_{n\in\mathbb{N}}$ e che il coefficiente binomiale, è una funzione di tipo polinomiale, e quindi continua nell'argomento α. Si conclude che

$$\left|\binom{\alpha}{h}\right| = \lim_{n\to\infty}\left|\binom{\alpha_n}{h}\right| \leq 1, \qquad \text{perchè } \binom{\alpha_n}{h} \in \mathbb{Z}.$$

Una stima più precisa del raggio di convergenza delle serie binomiali, si può avere ricordando che tali serie si possono ottenere a partire dalle serie esponenziale e logaritmica ponendo

$$(1+X)^\alpha = \exp[\alpha \log(1+X)], \qquad \text{per } \alpha \in \mathbb{Z}_p;$$

ricordando che

$$\log(1+x) = \sum_{n\geq 1}(-1)^{n-1}\frac{x^n}{n}, \qquad \text{converge per } \begin{cases} |x|<1 & \text{se } p\neq 2 \\ |x|<\frac{1}{2} & \text{altrimenti} \end{cases},$$

ed

$$\exp y = \sum_{h\geq 0}\frac{y^n}{n!}, \qquad \text{converge per } \begin{cases} |y|<p^{1/(1-p)} & \text{se } p\neq 2 \\ |y|<\frac{1}{4} & \text{altrimenti} \end{cases}.$$

La stima del raggio di convergenza di queste ultime due serie, si ottiene facilmente dall'osservazione che $v_p(n) \leq \log_p(n)$ (logaritmo reale in base p) e $v_p(n!) = \frac{n-S(n)}{p-1} \leq \frac{n-1}{p-1}$, ove $S(n)$ è la somma delle cifre della scrittura in base p del numero naturale n.

(b). Il contenuto della Proposizione precedente resta valido per le estensioni finite di $\mathbb{Q}_p$, ma è chiaramente falso per le estensioni di $\mathbb{R}$ (il coniugio di $\mathbb{C}$ è un automorfismo diverso dall'identità e, più in generale, esistono infiniti $\mathbb{Q}$-automorfismi non-continui di $\mathbb{C}$.). Una conseguenza di quanto dimostrato è che non vi sono sottocorpi di indice finito in $\mathbb{Q}_p$; infatti, se L fosse un tale sottocorpo, sarebbe un sottocorpo chiuso nella sua chiusura normale, in quanto stabile rispetto agli automorfismi del gruppo di Galois. Poichè L è chiuso e contiene $\mathbb{Q}$, deve necessariamente aversi $L=\mathbb{Q}_p$, perchè $\mathbb{Q}$ è denso in $\mathbb{Q}_p$.

Concludiamo questa sezione occupandoci della struttura del gruppo delle unità di $\mathbb{Z}_p$ e di $\mathbb{Q}_p$. Sia quindi

$$U = \mathbb{Z}_p^\times = \{\, x \in \mathbb{Q}_p \,|\, |x|_p = 1 \,\},$$

[†] In un corpo completo per un valore assoluto non-archimedeo, una serie $\sum_{n=0}^{\infty} a_n$ converge assolutamente se, e solo se, $\lim_{n\to\infty} a_n = 0$.

[‡] Ad esempio, se $(m,p)=1$, si può approssimare $\frac{1}{m}$ nel modo seguente. Essendo $am+bp=1$ per opportuni interi a e b, si può scrivere

$$\frac{1}{m} = \frac{a}{am} = a\,\frac{1}{1-bp} = a\sum_{n\geq 0}(bp)^n;$$

la serie geometrica converge perche $|bp|_p < 1$ e fornisce così una successione di interi che converge ad $\frac{1}{m}$.

e si osservi che in U vi è la filtrazione discendente di sottogruppi

$$U \supset U_1 \supset U_2 \supset \cdots \qquad \text{ove } U_n = 1 + p^n\mathbb{Z}_p, \text{ per } n \geq 1. \tag{2.9}$$

Considerando la restrizione ad U della riduzione modulo p, e l'applicazione $1 + p^n x \mapsto x \pmod p$, per $n \geq 1$, si conclude che i quozienti successivi della filtrazione sono

$$U/U_1 \cong \mathbb{F}_p^\times \qquad \text{ed} \qquad U_n/U_{n+1} \cong \mathbb{F}_p \text{ se } n \geq 1.$$

In particolare, per ogni $n \geq 1$, si ha la sequenza esatta (spezzante(*))

$$0 \longrightarrow U_1/U_n \longrightarrow U/U_n \longrightarrow U/U_1 \longrightarrow 0$$

Dunque, $U/U_n \cong V \oplus U_1/U_n$, ove V è un sottogruppo ciclico di ordine $p-1$ di U/U_n. Considerando il limite proiettivo di queste sequenze, si può scrivere

$$U = V \oplus U_1,$$

ove V è un sottogruppo ciclico, finito, di ordine $p-1$ di U, ovvero il gruppo delle radici p^n-esime di 1 in $\mathbb{Q}_p$(**). Per quanto riguarda la struttura del gruppo U_1, dobbiamo distinguere il caso in cui $p = 2$ dagli altri primi; precisamente vale il seguente risultato.

2.10 Proposizione. *Notazioni come in (II.2.9). Allora*
(i) se $p \neq 2$, si ha $U_1 \cong \mathbb{Z}_p$;
(ii) se $p = 2$, $U_1 \cong \{\pm 1\} \oplus U_2$ ed $U_2 \cong \mathbb{Z}_2$.

dim. (i). Si osservi che, *per $n \geq 1$, se $x \in U_n \setminus U_{n+1}$, allora $x^p \in U_{n+1} \setminus U_{n+2}$*. Infatti, se $x = 1 + p^n y$, con $y \in \mathbb{Z}_p^\times$, allora applicando la formula del binomio di Newton, si ottiene $x^p = 1 + p^{n+1}y + p^{n+2}t$, ove $p^{n+2}t = \sum_{j \geq 2} \binom{p}{j} p^{nj} y^j$ e quindi $x^p \in U_{n+1} \setminus U_{n+2}$. Da questa osservazione, si ricava che, se $\alpha \in U_1 \setminus U_2$, allora l'immagine di α nel quoziente $U_1/U_n \cong \mathbb{Z}/p^n\mathbb{Z}$ è un generatore di questo gruppo ciclico. Dunque, dato $u \in U_1$, in corrispondenza ad ogni $n \geq 1$, esiste un intero a_n, determinato, a meno di addendi in $p^n\mathbb{Z}$, tale che $u \equiv \alpha^{a_n} \pmod{U_n}$. Poichè $a_{n+1} \equiv a_n \pmod{p^n}$, si conclude che esiste $\lim_{n\to\infty} a_n = a \in \mathbb{Z}_p$ e che $u = \alpha^a := \lim_{n\to\infty} \alpha^{a_n}$. La corrispondenza $u \mapsto a$ è l'isomorfismo cercato.

(ii). Se $p = 2$, non è più vera l'osservazione iniziale, ma è vero che *per $n \geq 2$, se $x \in U_n \setminus U_{n+1}$, allora $x^2 \in U_{n+1} \setminus U_{n+2}$*. Allora, ragionando come nel caso precedente si conclude che $U_2 \cong \mathbb{Z}_2$. Poichè U_1 contiene il sottogruppo di 2-torsione $\{\pm 1\}$, mentre U_2 è privo di torsione si conclude che la sequenza esatta

$$0 \longrightarrow U_2 \longrightarrow U_1 \longrightarrow U_1/U_2 \longrightarrow 0$$

si spezza, dando luogo alla decomposizione dell'enunciato. **CVD** $\square$

(*) Una sequenza esatta di gruppi abeliani finiti

$$0 \longrightarrow A \xrightarrow[\alpha]{} C \xrightarrow[\beta]{} B \longrightarrow 0$$

si spezza se gli ordini di A e B sono coprimi. Infatti, se $\sharp(A) = a$ e $\sharp(B) = b$, con $(a, b) = 1$, allora $B' = \{\, x \in C \mid bx = 0 \,\}$, è un sottogruppo di C, isomorfo a B tramite β e tale che $C = A \oplus B'$.

(**) Si può osservare che, essendo $a^p \equiv a \pmod p$ per ogni intero a (piccolo teorema di Fermat), se ne deduce in particolare che, per $1 \leq a \leq p-1$, si ha $a^{p^{n+1}} \equiv a^{p^n} \pmod{p^n}$ e quindi esiste $\omega_a = \lim_{n\to\infty} a^{p^n} \in \mathbb{Z}_p$. Osservando che la riduzione modulo p di ω_a coincide con la riduzione di a, si conclude che, $\omega_a^p = \omega_a \neq 0$ e quindi che $\omega_a^{p-1} = 1$. In questo modo si ha una costruzione esplicita degli elementi del gruppo V.

Possiamo quindi concludere, osservando che, ogni elemento di $z \in \mathbb{Q}_p^\times$ si può decomporre in modo unico nel prodotto $z = p^n u$, ove $v_p(x) = n \in \mathbb{Z}$ ed $u \in \mathbb{Z}_p^\times$, e dedurre da ciò la struttura del gruppo $\mathbb{Q}_p^\times$, ovvero

$$\mathbb{Q}_p^\times \cong \begin{cases} \mathbb{Z} \oplus \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z} & \text{se } p \neq 2 \\ \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z} & \text{se } p = 2 \end{cases}. \tag{2.11}$$

In particolare, indicato con $\mathbb{Q}_p^2$ il sottogruppo di $\mathbb{Q}_p^\times$ formato dai quadrati degli elementi non nulli, da (II.2.11) si deduce

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^2 \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{se } p \neq 2 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{se } p = 2 \end{cases}. \tag{2.12}$$

3. Il simbolo di Hilbert

In questa sezione ci occuperemo di studiare una generalizzazione della legge di reciprocità quadratica che, in questa forma potrà essere generalizzata alle estensioni finite di $\mathbb{Q}$. Sia K un corpo (che supporremo nel seguito essere uguale ad uno dei completamenti $\mathbb{Q}_v$ al variare di v nell'insieme $\mathcal{V}$ dei posti di $\mathbb{Q}$) Si definisce l'applicazione $(\ ,\ ) : K^\times \times K^\times \to \{\pm 1\}$, ponendo

$$(a, b) = \begin{cases} 1 & \text{se } Z^2 - aX^2 - bY^2 \text{ ha uno zero non banale in } K \times K \times K \\ -1 & \text{altrimenti} \end{cases}$$

Cominciamo ad elencare alcune proprietà elementari di questa operazione, valide su qualsiasi corpo K.

(*i*) $(a, b) = (b, a)$;
(*ii*) $(a, -a) = 1 = (a, 1 - a)$;
(*iii*) $(a, c^2) = 1$;
(*iv*) $(a, b) = 1 \ \Rightarrow\ (aa', b) = (a', b)$;
(*v*) $(a, b) = (a, -ab) = (a, (1 - a)b)$;

Le prime tre proprietà sono di verifica immediata: la (*i*) discende dalla definizione stessa mentre la (*ii*) e la (*iii*) si verificano osservando che nei rispettivi casi le terne $(0, 1, 1)$, $(1, 1, 1)$ e $(0, 1, c)$ sono zeri non banali della forma quadratica in questione. Per quanto riguarda (*iv*) (e rispettivamente (*v*)), è chiaro che l'affermazione si deduce da (*iii*) se b (risp. a) è un quadrato. In caso contrario, possiamo dedurre il risultato dal seguente

3.1 Lemma. *Se b non è un quadrato in K, allora $(a, b) = 1$ se, e solo se, $a = N_{K(\sqrt{b})/K}(x)$ per qualche $x \in K(\sqrt{b})$.*

dim. Se $(\alpha, \beta, \gamma) \in K^3$ è uno zero non banale di $Z^2 - aX^2 - bY^2$, e b non è un quadrato in K, deve aversi $\gamma^2 - a\alpha^2 - b\beta^2 = 0$, con $\alpha \neq 0$. Si conclude che

$$a = \frac{\gamma^2}{\alpha^2} - b\frac{\beta^2}{\alpha^2} = N_{K(\sqrt{b})/K}\left(\frac{\gamma}{\alpha} + \frac{\beta}{\alpha}\sqrt{b}\right).$$

D'altra parte se $a = N_{K(\sqrt{b})/K}(t + u\sqrt{b}) = t^2 - bu^2$, allora $(1, u, t)$ è uno zero di $Z^2 - aX^2 - bY^2$. **CVD** □

In base a questa osservazione, (*iv*) discende banalmente dalla moltiplicatività della norma (cf. *Proposizione I.2.11* (*i*)) e (*v*) si deduce da (*ii*) e (*iv*).

In base alle proprietà appena dimostrate, resta ben definita un'applicazione simmetrica di $\mathbb{F}_2$-spazi vettoriali

[*simbolo di Hilbert*] $\qquad (\ ,\ ) : K^\times/K^2 \times K^\times/K^2 \to \{\pm 1\}.$

Nel caso in cui K sia uno dei completamenti di $\mathbb{Q}$, mostreremo che il simbolo di Hilbert è un'applicazione bilineare (simmetrica) non-degenere di spazi vettoriali su $\mathbb{F}_2$. Ciò discenderà da una descrizione esplicita del simbolo di Hilbert e, perciò richiamiamo alcuni simboli. Nella sezione *I.7* è stato definito il simbolo di Legendre $\left(\frac{a}{p}\right)$ per ogni intero a ed ogni primo p; poichè il simbolo dipende solo dalla riduzione modulo p di a, è chiaro cosa si intende per $\left(\frac{\alpha}{p}\right)$ per $\alpha \in \mathbb{Z}_p$. Inoltre, se $u \in 1 + \mathbb{Z}_2$, allora si pone

$$\varepsilon(u) \equiv \frac{u-1}{2} \pmod 2 = \begin{cases} 0 & \text{se } u \equiv 1 \pmod 4 \\ 1 & \text{se } u \equiv 3 \pmod 4 \end{cases}, \quad \omega(u) \equiv \frac{u^2-1}{8} \pmod 2 = \begin{cases} 0 & \text{se } u \equiv \pm 1 \pmod 8 \\ 1 & \text{se } u \equiv \pm 3 \pmod 8 \end{cases}.$$

Osserviamo, in particolare che in $\mathbb{Z}_2$ l'applicazione $U_1/U_3 \to \mathbb{F}_2 \times \mathbb{F}_2$ definita da $u \mapsto (\varepsilon(u), \omega(u))$ è un isomorfismo di gruppi, ovvero che un'unità $u \in \mathbb{Z}_2^\times$ è un quadrato se, e solo se, $\varepsilon(u) = 0 = \omega(u)$.

Possiamo quindi enunciare il seguente

3.2 Teorema. *Notazioni come sopra.*
(i) Se $K = \mathbb{R}$, allora si ha

$$(a,b)_\infty = \begin{cases} -1 & \textit{se } a < 0,\ b < 0 \\ 1 & \textit{altrimenti} \end{cases}.$$

(ii) Se $K = \mathbb{Q}_p$, allora, posto $a = p^\alpha u$, $b = p^\beta v$, con $\alpha, \beta \in \mathbb{Z}$ ed $u, v \in \mathbb{Z}_p^\times$, si ha

$$(a,b)_p = \begin{cases} (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha & \textit{se } p \neq 2 \\ (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)} & \textit{se } p = 2 \end{cases}.$$

dim. (i). È chiaro che la forma quadratica $Z^2 - aX^2 - bY^2$ è priva di zeri non banali in $\mathbb{R}$ se, e solo se, è definita positiva, e ciò permette di concludere.

(ii). Otterremo il risultato con calcoli diretti e perciò, dobbiamo distinguere vari casi. Cominciamo quindi supponendo

$p \neq 2$. In tal caso $\mathbb{Q}_p^\times/\mathbb{Q}_p^2$ è uno spazio vettoriale di dimensione 2 su $\mathbb{F}_2$, generato da (le classi di) p e u, ove $u \in \mathbb{Z}_p^\times \setminus U_1$. Dobbiamo quindi verificare la formula dell'enunciato sulle coppie di elementi non nulli.

- Se $u, v \in \mathbb{Z}_p^\times$, allora $(u,v)_p = 1$, perchè la forma quadratica $Z^2 - uX^2 - vY^2$ ha uno zero non banale se, e solo se, la sua ridotta modulo p ha uno zero non banale (cf. *Corollario II.2.5*) e questo si verifica facilmente, ad esempio prendendo $Z = 1$ ed osservando che vi sono $\frac{p+1}{2}$ elementi distinti del tipo $1 - ux^2$ e $\frac{p+1}{2}$ elementi distinti del tipo vy^2, al variare di $x, y \in \mathbb{F}_p$ e perciò due fra questi elementi devono coincidere dando luogo ad uno zero non-banale della forma quadratica ridotta.
- Se $u, v \in \mathbb{Z}_p^\times$, allora $(pu, v)_p = \left(\frac{v}{p}\right)$. Infatti, essendo $(u,v)_p = 1$, in base alla proprietà (iv) del simbolo di Hilbert, si ricava che $(pu, v)_p = (p, v)_p$ e si verifica facilmente che $(p, v)_p = 1$ se, e solo se, v è un quadrato modulo p.
- Se $u, v \in \mathbb{Z}_p^\times$, allora $(pu, pv)_p = (-1)^{\varepsilon(p)} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. Infatti, per la proprietà (v) del simbolo di Hilbert, si ha $(pu, pv)_p = (pu, -p^2uv)_p = (pu, -uv)_p$ e quindi, per quanto visto nel punto precedente si conclude che $(pu, pv)_p = \left(\frac{-uv}{p}\right)$ da cui si deduce la tesi (cf. (I.7.6)).

$p = 2$. In tal caso $\mathbb{Q}_2^\times/\mathbb{Q}_2^2$ è uno spazio vettoriale di dimensione 3 su $\mathbb{F}_2$, ed anche in questo caso discuteremo varie possibilità separatamente.

- Se $u, v \in \mathbb{Z}_2^\times$, allora dobbiamo mostrare che

$$(u,v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)},$$

ovvero che $(u,v)_2 = 1$ se uno almeno tra u e v appartiene ad U_2, mentre $(u,v)_2 = -1$ in caso contrario. Supponiamo quindi che si abbia $u \in U_2 \setminus U_3$, perchè se $u \in U_3$ è un quadrato e si ha $(u,v)_2 = 1$. Dunque $u + 4v \equiv 1 \pmod 8$ e quindi, esiste $w \in \mathbb{Z}_2$ tale che $u + 4v = w^2$, ovvero $(1,2,w)$ è uno zero della forma quadratica $Z^2 - uX^2 - vY^2$ e perciò $(u,v)_2 = 1$. Supponiamo quindi che si abbia $u \equiv v \equiv -1 \pmod 4$, allora, se esistesse una soluzione primitiva (x,y,z) della forma $Z^2 - uX^2 - vY^2$, allora si avrebbe, in particolare, $z^2 + x^2 + y^2 \equiv 0 \pmod 4$ che implica $x \equiv y \equiv z \equiv 0 \pmod 2$ contro l'ipotesi che si tratti di una soluzione primitiva, dunque deve aversi $(u,v)_2 = -1$.

- Dobbiamo ora mostrare che, se $u, v \in \mathbb{Z}_2^\times$, allora

$$(2u, v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}.$$

Mostriamo per prima cosa che $(2,v)_2 = (-1)^{\omega(v)}$, ovvero che $(2,v)_2 = 1$ se, e solo se, $v \equiv \pm 1 \pmod 8$. Infatti, se $v \equiv 1 \pmod 8$, allora v è un quadrato e quindi $(2,v)_2 = 1$; mentre, se $v \equiv -1 \pmod 8$, allora la forma quadratica $Z^2 - 2x^2 - vY^2$, ridotta modulo 8, ha la soluzione $(1,1,1)$ e quindi $(2,v)_2 = 1$ (cf. *Corollario II.2.6*). D'altra parte, se esistesse una terna primitiva (x,y,z), per cui $z^2 - 2x^2 - vy^2 = 0$, e quindi con $y \equiv z \equiv 1 \pmod 2$, riducendo modulo 8, dovrebbe aversi $1 - 2x^2 - v \equiv 0 \pmod 8$; ed osservando che gli unici quadrati in $\mathbb{Z}/8\mathbb{Z}$ sono 0, 1 e 4 si conclude che $v \equiv \pm 1 \pmod 8$.

Per concludere questa parte, dobbiamo mostrare che $(2u,v)_2 = (2,v)_2(u,v)_2$. Ciò è vero se $(2,v) = 1$, oppure se $(u,v) = 1$ per la proprietà (iv) del simbolo di Hilbert. Resta quindi da dimostrare che $(2,v)_2 = -1 = (u,v)_2 \quad \Rightarrow \quad (2u,v)_2 = 1$. Le condizioni in ipotesi sono equivalenti alle congruenze $u \equiv v \equiv -1 \pmod{()4}$ e $v \equiv 3 \mod 8$; quindi è sufficiente osservare che le equazioni $Z^2 2X^2 - 3Y^2 = 0$ e $Z^2 - 6X^2 + 5Y^2 = 0$ ammettono la soluzione $(1,1,1)$ per concludere che $(2u,v)_2 = 1$ (cf. *Corollario II.2.6*).

- L'ultimo punto consiste nel verificare che, se $u, v \in \mathbb{Z}_2^\times$, allora

$$(2u, 2v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)}.$$

Per la proprietà (v) del simbolo di Hilbert, si ha $(2u,2v) = (2u,-4uv) = (2u,-uv)$ e quindi, dal caso discusso nel punto precedente si deduce

$$(2u,2v)_2 = (2u,-uv)_2 = (-1)^{\varepsilon(u)\varepsilon(-uv)+\omega(-uv)} = (-1)^{\varepsilon(u)(\varepsilon(-1)+\varepsilon(u)+\varepsilon(v))+\omega(-1)+\omega(u)+\omega(v)}.$$

Si può quindi concludere ricordando che $\varepsilon(-1) = 1$, $\omega(-1) = 0$ e $\varepsilon(u)(1+\varepsilon(u)) = 0$, come si ricava direttamente dalle definizioni. **CVD** □

Una conseguenza di questa descrizione esplicita del simbolo di Hilbert è contenuta nel seguente

3.3 Teorema. *Per ogni posto v di $\mathbb{Q}$ il simbolo di Hilbert è un'applicazione bilineare simmetrica non-degenere di $\mathbb{Q}_v/\mathbb{Q}_v^2$ a valori in $\mathbb{F}_2$.*

L'unica cosa che non sia stata dimostrata in modo esplicito è la verifica che il simbolo di Hilbert sia non-degenere e ciò si può dedurre facilmente dalla matrice del simbolo di Hilbert nei vari casi. Scriviamo quindi la matrice di questa applicazione bilineare di $\mathbb{F}_2$-spazi vettoriali, usando –come in tutta la discussione precedente– la notazione moltiplicativa (± 1) per gli elementi di $\mathbb{F}_2$.

- se $K = \mathbb{R}$ la matrice è (-1).
- se $K = \mathbb{Q}_p$ con $p \neq 2$, consideriamo la base $\{p, u\}$ di $\mathbb{Q}_p/\mathbb{Q}_p^2$, con $u \in \mathbb{Z}_p^\times$ ed $\left(\frac{u}{p}\right) = -1$. Allora la matrice del simbolo di Hilbert è

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \quad \text{se } p \equiv 1 \pmod 4, \qquad \text{e} \qquad \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \quad \text{se } p \equiv -1 \pmod 4.$$

- se $K = \mathbb{Q}_2$, rispetto alla base $\{2, -1, 5\}$, la matrice del simbolo di Hilbert è

$$\begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}.$$

Il corpo $\mathbb{Q}$ può essere immerso come sottocorpo denso in ciascuno dei suoi completamenti $\mathbb{Q}_v$ ed anche in ogni loro prodotto finito (cf. *Proposizione II.1.10*). Il Teorema che segue, mostra quale relazione vi sia tra i vari simboli di Hilbert di una coppia di numeri razionali.

3.4 Teorema. [Hilbert] *Siano $a, b \in \mathbb{Q}^\times$; allora si ha $(a,b)_v = 1$ per tutti i posti v di $\mathbb{Q}$, eccetto al più un numero finito, e inoltre*

$$\prod_{v \in \mathcal{V}} (a,b)_v = 1.$$

dim. Il quoziente $\mathbb{Q}^\times/\mathbb{Q}^2$ è uno spazio vettoriale di dimensione infinita su $\mathbb{F}_2$, che ha come base l'insieme $\{\pm 1\} \cup \{\, p \in \mathbb{N} \mid p \text{ primo } \}$. Si tratta quindi di verificare gli asserti dell'enunciato nei casi in cui a e b sono uguali a -1 oppure ad un primo razionale. Distinguiamo i vari casi ed effettuiamo i calcoli servendoci del *Teorema II.3.2*.

- Se $a = -1 = b$, allora $(-1,-1)_\infty = -1 = (-1,-1)_2$, e $(-1,-1)_p = 1$, per $p \neq 2$ e quindi la tesi è verificata.
- Se $a = -1$ e $b = \ell$ (ℓ primo). Se $\ell = 2$, si ha $(-1,2)_v = 1$, per ogni $v \in V$. Se $\ell \neq 2$, allora $(-1,\ell)_v = 1$ per $v \neq 2, \ell$ e $(-1,\ell)_2 = (-1,\ell)_\ell = (-1)^{\varepsilon(\ell)}$. Anche in questo caso la tesi è verificata.
- Se $a = \ell$ e $b = \ell'$ (ℓ, ℓ' primi). Se fosse $\ell = \ell'$, in base alla proprietà (v) del simbolo di Hilbert, si ha $(\ell,\ell)_v = (-1,\ell)_v$ e questo caso l'abbiamo già trattato nel punto precedente. Sia quindi $\ell \neq \ell'$ ed osserviamo che, nel caso in cui $\ell' = 2$, si ha $(\ell,2)_v = 1$ per $v \neq 2, \ell$ e $(\ell,2)_2 = (-1)^{\omega(\ell)} = (\ell,2)_\ell$. Infine se ℓ ed ℓ' sono distinti tra loro e da 2, si ha $(\ell,\ell')_v = 1$ se $v \neq 2, \ell, \ell'$ ed inoltre, $(\ell,\ell')_2 = (-1)^{\epsilon(\ell)\epsilon(\ell')}$, $(\ell,\ell')_\ell = \left(\frac{\ell'}{\ell}\right)$ ed $(\ell,\ell')_{\ell'} = \left(\frac{\ell}{\ell'}\right)$. Grazie alla legge di reciprocità quadratica, si conclude che

$$(-1)^{\epsilon(\ell)\epsilon(\ell')} \left(\frac{\ell'}{\ell}\right) \left(\frac{\ell}{\ell'}\right) = 1$$

(cf. *Teorema I.7.8*) il che conclude la dimostrazione. **CVD** □

Concludiamo questa sezione con un risultato di esistenza di numeri razionali con valori prefissati del simbolo di Hilbert. Faremo uso di questo risultato nella dimostrazione del Teorema di Hasse e Minkowski (cf. *Teorema II.5.1*).

3.5 Teorema. *Siano $\{a_1, \dots, a_m\}$ dei numeri razionali non nulli e siano dati, per ogni $i = 1, \dots, m$ e per ogni posto v di $\mathbb{Q}$, i numeri $\varepsilon_{i,v} \in \{\pm 1\}$, soggetti alle seguenti condizioni*

(i) *ad eccezione di un numero finito di coppie di indici (i, v), si ha $\varepsilon_{i,v} = 1$;*

(ii) *per ogni $i = 1, \dots, m$, si ha $\prod_v \varepsilon_{i,v} = 1$;*

(iii) *per ogni posto v, esiste $x_v \in \mathbb{Q}_v^\times$ tale che $(x_v, a_i)_v = \varepsilon_{i,v}$ per $i = 1, \dots, m$. Allora esiste $x \in \mathbb{Q}^\times$ tale che $(x, a_i)_v = \varepsilon_{i,v}$ per ogni coppia di indici (i, v).*

dim. È pressochè immediato verificare che le condizioni date sono necessarie per l'esistenza di un tale $x \in \mathbb{Q}^\times$. Per verificare che sono anche sufficienti avremo bisogno di appellarci al

Teorema. [Dirichlet] *Dati due interi positivi e coprimi a e b; allora esistono infiniti numeri primi p che soddisfano alla congruenza $p \equiv a \pmod{b}$.*

Di questo teorema non daremo la dimostrazione e rimandiamo il lettore interessato al Capitolo VII di A. W. Knapp, *Elliptic Curves*, Princeton Univ. Press 1992.

Cominciamo quindi la dimostrazione del Teorema osservando che, a meno di moltiplicare gli a_i per un quadrato, possiamo supporre che si tratti di numeri interi e consideriamo quindi il sottoinsieme S di posti di $\mathbb{Q}$, formato da ∞, 2 e dai primi che compaiono nella fattorizzazione degli a_i. Oltre ad S, consideriamo anche l'insieme T dei posti v per cui qualcuno degli $\varepsilon_{i,v}$ è uguale a -1. Entrambi sono sottoinsiemi finiti dell'insieme dei posti di $\mathbb{Q}$ e supponiamo dapprima che si abbia $S \cap T = \emptyset$ rimandando il caso generale ad una successiva discussione. Allora, sotto l'ipotesi $S \cap T = \emptyset$, si ponga

$$a = \prod_{\substack{\ell \in T \\ \ell \neq \infty}} \ell \qquad \text{e} \qquad b = 8 \prod_{\substack{\ell \in S \\ \ell \neq 2,\infty}} \ell.$$

Gli interi a e b sono coprimi e, per il teorema di Dirichlet citato sopra, esiste un numero primo $p \notin S \cup T$ tale che $p \equiv a \pmod{b}$. Mostriamo che, in tal caso, il numero $x = ap$ soddisfa alle condizioni del Teorema.

Se $v = \infty$, allora $v \in S$ e quindi $\varepsilon_{i,\infty} = 1$ perchè $S \cap T = \emptyset$, d'altra parte $(a_i, x)_\infty = 1$ perchè $x > 0$. Se consideriamo ora un numero primo $\ell \in S$, essendo $x = pa \equiv a^2 \pmod{m}$, si deduce che x è congruo ad un quadrato, sia modulo ℓ che modulo 8, e quindi, poichè sia a che x sono unità in $\mathbb{Q}_\ell$, si conclude che x è un quadrato in $\mathbb{Q}_\ell$ (cf. *Corollario II.2.5* e *Corollario II.2.6*) e quindi si ha $(a_i, x)_\ell = 1 = \varepsilon_{i,\ell}$, ove l'ultima uguaglianza discende sempre dal fatto che $\ell \in S$ ed $S \cap T = \emptyset$.

Se si considera un numero primo $\ell \notin S$, allora, ciascuno degli a_i è un'unità in $\mathbb{Q}_\ell$ e si ha $(a_i, b)_\ell = \left(\frac{a_i}{\ell}\right)^{v_\ell(b)}$, per ogni $b \in \mathbb{Q}_\ell^\times$ (cf. *Teorema II.3.2*). Se $\ell \notin T \cup \{p\}$, allora $v_\ell(x) = 0$ e quindi $(a_i, x)_\ell = 1 = \varepsilon_{i,\ell}$. Se $\ell \in T$, allora $v_\ell(x) = 1$ e inoltre, esiste un elemento $x_\ell \in \mathbb{Q}_\ell^\times$, tale che $(a_i, x_\ell) = \varepsilon_{i,\ell}$ per ogni i, ed uno almeno degli $\varepsilon_{i,\ell} = -1$, per cui si conclude che $v_\ell(x_\ell)$ è un numero dispari e quindi

$$(a_i, x)_\ell = \left(\frac{a_i}{\ell}\right) = (a_i, x_\ell) = \varepsilon_{i,\ell}, \qquad \text{per ogni } i = 1, \dots, m.$$

Da ultimo il caso $\ell = p$ è necessariamente verificato perchè, per ogni i, sia i simboli di Hilbert $(a_i, x)_v$ che i vari $\varepsilon_{i,v}$ soddisfano alla formula del prodotto (cf. *Teorema II.3.4* e l'ipotesi *(ii)*).

Ciò dimostra completamente il teorema nell'ipotesi che $S \cap T = \emptyset$ e passiamo quindi a discutere il caso generale. Si osservi che, qualunque sia il posto v di $\mathbb{Q}$, se $|x - 1|_v < \frac{1}{8}$, allora x è un quadrato in $\mathbb{Q}_v$ (cf. *Corollario II.2.5* e *Corollario II.2.6*); dunque, per il principio di approssimazione debole (cf. *Proposizione II.1.10*), esiste un'elemento $x' \in \mathbb{Q}^\times$ tale che x'/x_v sia un quadrato in $\mathbb{Q}_v$ per ogni $v \in S$. Quindi, in particolare, si ha $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$ per ogni $v \in S$ e quindi, posto

$$\varepsilon'_{i,v} = \varepsilon'_{i,v}(a_i, x')_v \qquad \text{per ogni posto } v,$$

si ottiene una famiglia che soddisfa alle ipotesi del Teorema con l'ulteriore condizione che $\varepsilon'_{i,v} = 1$ se $v \in S$ e quindi, per le considerazioni fatte in precedenza esiste un elemento $y \in \mathbb{Q}^\times$ tale che $(a_i, y)_v = \varepsilon'_{i,v}$ per ogni indice i e per ogni posto v. Per la bilinearità del simbolo di Hilbert, si conclude che $x = yx'$ è l'elemento che soddisfa alle condizioni del Teorema. **CVD** □

4. Forme quadratiche

In questa sezione ci occuperemo di forme quadratiche su corpi di caratteristica diversa da 2.

4.1 Definizione. Siano K un corpo e V uno spazio vettoriale di dimensione finita su K. Una applicazione $q : V \to K$ è una *forma quadratica* se, e solo se, l'applicazione $(x, y) \mapsto q(x + y) - q(x) - q(y)$ è un'applicazione bilineare.

Si chiama *modulo quadratico* la coppia (V, q), ove V è uno spazio vettoriale di dimensione finita su K e $q : V \to K$ è una forma quadratica.

Dati due moduli quadratici (V, q) e (V', q'), un'applicazione lineare $\phi : V \to V'$ è un'*isometria* se $q = q' \circ \phi$.

Due moduli quadratici (V, q) e (V', q') si dicono *isometrici* se hanno la stessa dimensione ed esiste un'isometria $\phi : V \to V'$.

La definizione precedente resta valida anche su corpi di caratteristica 2. D'ora in poi però supporremo che K abbia caratteristica diversa da 2 e, dato un modulo quadratico (V, q), indicheremo con

$$x \cdot y := \frac{1}{2}[q(x + y) - q(x) - q(y)]$$

l'applicazione bilineare (simmetrica) su V, associata a q, ed applicheremo a (V, q), la terminologia in uso per gli spazi dotati di un 'prodotto scalare': parleremo quindi del *nucleo* dell'applicazione bilineare ($N_q = \{\, v \in V \mid v \cdot x = 0 \ \forall x \in V \,\}$) e di forma *non-degenere* ($N_q = \{0\}$), di sottospazi mutuamente *ortogonali* ($U \subseteq W^\perp$ se $u \cdot w = 0$ per ogni $u \in U$ ed ogni $w \in W$) e di *somma diretta ortogonale* ($U \hat{\oplus} W$, ovvero la somma diretta di U e W con i due sottospazi mutuamente ortogonali) ed infine, chiameremo *isotropi* i sottospazi U contenuti nel proprio ortogonale ($U \subseteq U^\perp$) e *piano iperbolico* un modulo quadratico di dimensione 2, ove la matrice dell'applicazione bilineare sia $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Raccogliamo brevemente nella proposizione successiva alcune proprietà elementari delle applicazioni bilineari.

4.2 Proposizione. *Sia K un corpo di caratteristica diversa da 2.*

(i) *Sia (V, q) un modulo quadratico su K ed $N = N_q$ il nucleo dell'applicazione bilineare associata; allora $(V/N, q)$ è un modulo quadratico non-degenere.*

(ii) *Sia (V, q) un modulo quadratico su K ed U un sottospazio vettoriale di V. Allora la restrizione ad U di q è non degenere se, e solo se, $U \cap U^\perp = \{0\}$. In tal caso $V = U \hat{\oplus} U^\perp$.*

(iii) *Sia (V, q) un modulo quadratico non-degenere su K, allora esiste una base ortogonale di V.*

(iv) *Siano (V, q) un modulo quadratico non-degenere, (V', q') un modulo quadratico su ed $s : V \to V'$ un'isometria. Allora s è iniettiva.*

(v) *Sia (V, q) un modulo quadratico non-degenere su K; allora, dati due vettori $v, w \in V$ tali che $v \cdot v = w \cdot w \neq 0$, allora esiste un'isometria $\sigma : V \to V$, tale che $\sigma(v) = w$.*

(vi) *Sia (V, q) un modulo quadratico non-degenere su K allora ogni vettore isotropo è contenuto in un piano iperbolico.*

(vii) *Sia (V, q) un modulo quadratico non-degenere su K, se vi sono in V vettori isotropi non-nulli, allora q rappresenta ogni elemento di K (ovvero $q : V \to K$ è suriettiva).*

dim. *(i)* Dalla definizione discende che $x \in N$ se, e solo se, $q(y + x) = q(y)$, per ogni $y \in V$ e quindi è ben definita la funzione q su V/N ed è ovviamente una forma quadratica non-degenere.

(ii) È una conseguenza diretta delle definizioni.

(iii) Dobbiamo dimostrare che esiste una base $\mathcal{V} = \{v_1, \dots, v_n\}$ di V tale che $v_i \cdot v_j \neq 0$ se, e solo se, $i = j$. Ciò è banalmente vero se $\dim V = 1$, si può quindi fare induzione sulla dimensione di V, osservando che, se q è non-degenere, esiste almeno un vettore non isotropo ($\operatorname{char} K \neq 2$), sia v_1, ed allora $V = \langle v_1 \rangle \hat{\oplus} \langle v_1 \rangle^\perp$. Essendo $\dim \langle v_1 \rangle^\perp = \dim V - 1$, esiste una base ortogonale $\{v_2, \dots, v_n\}$ di tale sottospazio e quindi $\mathcal{V} = \{v_1, \dots, v_n\}$ è la base cercata.

(iv) Se $s(v) = 0$, allora, per ogni $x \in V$, si ha

$$x \cdot v = \frac{1}{2}[q(x+v) - q(x) - q(v)] = \frac{1}{2}[q'(s(x+v)) - q'(s(x)) - q'(s(v))] = 0$$

perchè s è un'applicazione lineare e $q'(0) = 0$. Dunque $v \in N_q = \{0\}$, perchè q è non-degenere.

(v) Si considerino i vettori $x = v + w$ ed $y = v - w$ e si osservi che si ha $x \cdot x = 2(v \cdot v + v \cdot w)$ ed $y \cdot y = 2(v \cdot v - v \cdot w)$ quindi, essendo $v \cdot v \neq 0$, uno almeno tra x ed y non è un vettore isotropo. Sia y, allora l'applicazione $\sigma_y : V \to V$ definita ponendo $\sigma_y(z) := z - 2\frac{z \cdot y}{y \cdot y}y$, è l'isometria richiesta(*), come si verifica con calcoli diretti. Se invece y è isotropo, allora l'analoga applicazione $\sigma_x : V \to V$ è un'isometria per cui $\sigma_x(v) = -w$. È quindi sufficiente considerare $-\sigma_x$ per concludere.

(vi) Sia $u \neq 0$ un vettore isotropo. Poichè V è non-degenere, esiste un vettore w, tale che $u \cdot w \neq 0$ e, a meno di dividere w per una costante possiamo supporre $u \cdot w = 1$. Allora il sottospazio $\langle u, w \rangle$ è un piano iperbolico. Infatti, se fosse $w \cdot w = a \neq 0$, basta considerare i vettori u e $v = w - \frac{a}{2}u$ per avere una base di $\langle u, w \rangle$ rispetto a cui la restrizione dell'applicazione bilineare ha matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(vii) È sufficiente mostrare che se (U, q) è un piano iperbolico, allora q rappresenta ogni elemento di K. Infatti se $\{u, v\}$ è una base di U rispetto a cui l'applicazione bilineare ha matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, allora si ha $q(u + av) = (u + av) \cdot (u + av) = 2a$ per ogni $a \in K$ e poichè 2 è invertibile in K ciò permette di concludere. **CVD** □

Possiamo quindi dimostrare il risultato fondamentale per la classificazione delle forme quadratiche su di un corpo di caratteristica diversa da 2, ovvero il *Teorema di cancellazione* (o *Teorema di estensione delle isometrie*) di Ernst Witt.

4.3 Teorema. [Witt] *Siano (V, q) e (V', q') due moduli quadratici, non-degeneri ed isometrici, definiti su un corpo K di caratteristica diversa da 2. Se $U \subset V$ è un sottospazio vettoriale ed $s : U \to V'$ è un'isometria iniettiva ($q'(s(u)) = q(u)$ per ogni $u \in U$), allora s si estende ad una isometria di tutto V su V'.*

dim. Osserviamo che l'ipotesi che l'isometria $s : U \to V'$ sia iniettiva non è ridondante perchè può ben accadere che la restrizione di q ad U sia degenere. Infatti, dimostriamo dapprima che in tal caso, s si estende ad un sottospazio U_1, contenente U, tale che la restrizione di q ad U_1 sia non-degenere.

Supponiamo quindi che vi sia un vettore $u \neq 0$ nel nucleo N della restrizione di q ad U. Se W è un sottospazio di U tale che $U = \langle u \rangle \oplus W$ allora esiste un vettore $y \in W^\perp \setminus U^\perp$, e, a meno di sostituirlo con un vettore del tipo $\beta y + \alpha u$ (con $\beta \neq 0$), possiamo supporre che si abbia $y \cdot u = 1$ e $y \cdot y = 0$. Analogamente, considerando in V' il vettore $s(u)$ ed il sottospazio $U' = \operatorname{im} s = \langle s(u) \rangle \oplus s(W)$, si può determinare un vettore $y' \in s(W)^\perp$, per cui si abbia $y' \cdot s(u) = 1$ e $y' \cdot y' = 0$. Allora, presi il sottospazio $T = U \oplus \langle y \rangle$ e l'applicazione $s' : T \to V'$ definita ponendo $s'(x + \alpha y) := s(x) + \alpha y'$ per ogni $x \in U$, si ha che s' estende s e che il nucleo della restrizione di q a T è contenuto in N ed ha dimensione strettamente più piccola, perchè non contiene u.

Procedendo in tal modo, si può determinare un sottospazio $U_1 \supset U$ ed un'isometria iniettiva $s_1 : U_1 \to V'$, con l'ulteriore proprietà che la restrizione di q ad U_1 sia non degenere. Per concludere la dimostrazione del Teorema di Witt, dobbiamo estendere s_1 a tutto V. Fissiamo una base ortogonale $\{x_1, \dots, x_r\}$ di U_1 (cf. *Proposizione II.4.2 (iii)*) ed osserviamo che si hanno le decomposizioni

$$V = \langle x_1 \rangle \hat{\oplus} \cdots \hat{\oplus} \langle x_r \rangle \hat{\oplus} U_1^\perp \qquad \text{e} \qquad V' = \langle s_1(x_1) \rangle \hat{\oplus} \cdots \hat{\oplus} \langle s_1(x_r) \rangle \hat{\oplus} s_1(U_1)^\perp.$$

(*) Si osservi che l'applicazione σ_y altri non è che la 'riflessione' rispetto al sottospazio $\langle y \rangle^\perp$ ovvero, scritto $z = u + \alpha y$, con $u \in \langle y \rangle^\perp$ ed $\alpha \in K$, si ha $\sigma_y(z) = u - \alpha y$.

Fissata inoltre un'isometria $f : V \to V'$, i vettori $f(x_1)$ ed $s_1(x_1)$ di V' soddisfano alle ipotesi della *Proposizione II.4.2 (v)* e quindi esiste un'isometria $\sigma_1 : V' \to V'$, tale che $\sigma_1(f(x_1)) = s_1(x_1)$. Dunque $\sigma_1 \circ f$ è un'isometria di V su V' e coincide con s_1 sul sottospazio $\langle x_1 \rangle$; in particolare, l'immagine di $\langle x_1 \rangle^\perp = \langle x_2 \rangle \hat{\oplus} \cdots \hat{\oplus} \langle x_r \rangle \hat{\oplus} U_1^\perp$ è contenuta in $\langle s_1(x_1) \rangle^\perp = \langle s_1(x_2) \rangle \hat{\oplus} \cdots \hat{\oplus} \langle s_1(x_r) \rangle \hat{\oplus} s_1(U_1)^\perp$. Quindi questi due sottospazi sono isometrici e si può quindi costruire un'isometria $\sigma_2 : V' \to V'$ che mandi $\sigma_1(f(x_2))$ su $s_1(x_2)$ ed induca l'identità su $s_1(x_1)$. Proseguendo in tal modo, si costruisce un'isometria $\sigma_r \circ \cdots \circ \sigma_1 \circ f : V \to V'$ che estende s_1 e quindi s. **CVD** □

4.4 Remark. Prima di trarre le conseguenze del Teorema di Witt, vogliamo mostrare con un esempio come tale risultato non si possa estendere a forme quadratiche su campi di caratteristica 2. Sia dunque K un corpo di caratteristica 2 e siano V e W due spazi vettoriali di dimensione 3 su K. Siano $\{v_1, v_2, v_3\}$ una base di V e $\{w_1, w_2, w_3\}$ una base di W e si considerino le applicazioni bilineari che, rispetto alle basi date, hanno rispettivamente matrice

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{e} \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

I due moduli quadratici così ottenuti sono isometrici, perchè l'applicazione

$$v_1 \mapsto w_1 + w_2 + w_3, \quad v_2 \mapsto w_1 + w_2, \quad v_3 \mapsto w_1 + w_3$$

si verifica essere un'isometria. D'altra parte l'applicazione $v_1 \mapsto w_1$ è un'isometria iniettiva di $\langle v_1 \rangle$ su W, ma non si può estendere a tutto V, perchè una tale estensione, dovrebbe mandare il sottospazio $\langle v_1 \rangle^\perp = \langle v_2, v_3 \rangle$, sul sottospazio $\langle w_1 \rangle^\perp = \langle w_2, w_3 \rangle$, ma questi sopttospazi non sono isometrici, come si vede facilmente osservando che il secondo non contiene alcun vettore non isotropo.

Andiamo quindi ad enunciare alcune conseguenze del Teorema di Witt, cominciando da quella che gli vale il nome di Teorema di cancellazione e la cui dimostrazione è immediata applicazione del Teorema.

4.5 Corollario. *Sia (V, q) un modulo quadratico non-degenere sul corpo K di caratteristica diversa da 2. Se U_1 ed U_2 sono sottospazi di V, allora U_1 è isometrico ad U_2 se, e solo se, $U_1^\perp$ è isometrico ad $U_2^\perp$.*

Il teorema si applica inoltre alla classificazione (a meno di isometria) dei moduli quadratici nel modo seguente.

4.6 Proposizione. *Sia (V, q) un modulo quadratico non-degenere sul corpo K di caratteristica diversa da 2. Allora V si decompone nella somma ortogonale*

$$V = U_1 \hat{\oplus} \ldots \hat{\oplus} U_r \hat{\oplus} W,$$

ove $U_1, \ldots, U_r$ sono piani iperbolici, mentre W è privo di vettori isotropi diversi da zero. Il numero $r \geq 0$ dei piani iperbolici e la classe di isometria di W non dipendono dalla decomposizione, ma sono univocamente determinati da (V, q).

dim. Se V non contiene vettori isotropi (diversi da zero), allora $V = W$ ed il risultato è banalmente vero. Altrimenti, se V contiene un vettore isotropo diverso da zero, per la *Proposizione II.4.2 (vi)*, V contiene un piano iperbolico U_1 e si può quindi decomporre $V = U_1 \hat{\oplus} U_1^\perp$ (cf. la Proposizione citata *(ii)*). Ora, se $U_1^\perp$ non contiene vettori isotropi non banali si pone $U_1^\perp = W$, altrimenti, $U_1^\perp$ contiene un piano iperbolico U_2 e si prosegue analogamente fino ad ottenere la decomposizione dell'enunciato.

Infine, se $V = U_1 \hat{\oplus} \ldots \hat{\oplus} U_r \hat{\oplus} W = U_1' \hat{\oplus} \ldots \hat{\oplus} U_s' \hat{\oplus} W'$ sono due decomposizioni di V del tipo descritto con $r \geq s$, allora l'isometria naturale di $U_1 \hat{\oplus} \ldots \hat{\oplus} U_s$ su $U_1' \hat{\oplus} \ldots \hat{\oplus} U_s'$ induce un'isometria tra i rispettivi ortogonali e quindi deve aversi sia $r = s$, perchè W' non contiene vettori isotropi diversi da zero, che indurre un isometria di W su W'. **CVD** □

Da ciò si conclude che la classificazione delle forme quadratiche su un corpo K di caratteristica diversa da 2 si riduce alla classificazione dei moduli quadratici (V, q) privi di vettori isotropi non-nulli (talvolta detti moduli quadratici *ellittici*) e lo strumento utilizzato in questo ambito è il gruppo di Witt. Diamo qualche cenno alla costruzione del *gruppo di Witt* $\mathbb{W}(K)$, associato al corpo K (di caratteristica diversa da 2).

Due moduli quadratici (V,q) e (V',q') si dicono *equivalenti secondo Witt* se $(V,q)\hat{\oplus}(V',-q')$ è una somma ortogonale di piani iperbolici. Si può mostrare che le classi di equivalenza secondo Witt dei moduli quadratici formano un gruppo rispetto all'operazione di somma ortogonale e questi è il gruppo di Witt. Si può dedurre facilmente dal Teorema di estensione delle isometrie che due moduli quadratici su K sono isometrici se, e solo se, hanno la stessa dimensione e sono equivalenti secondo Witt. Ciò mostra la relazione tra il gruppo di Witt e la classificazione dei moduli quadratici. Inoltre, si può dimostrare che per qualsiasi corpo K, il gruppo $\mathbb{W}(K)$ è generato dalle classi $[a]$ al variare di $a \in K$, soggette alle relazioni $[a] = [ax^2]$ $\forall x \in K$, $[a] + [-a] = 0$, $[a] + [b] = [a+b] + [ab(a+b)]$ se $a + b \neq 0$ (cf. ad esempio J. Milnor, D. Husemoller, *Symmetric Bilinear Forms*, Springer 1973, Ch. III, per un'esauriente trattazione dell'argomento). Lo studio del gruppo di Witt sui corpi finiti $\mathbb{F}_q$, di caratteristica diversa da 2, risulta semplice se si osserva che ogni modulo quadratico di dimensione ≥ 3 su $\mathbb{F}_q$ contiene un vettore isotropo non nullo (ciò perchè la forma quadratica $aX_1^2 + bX_2^2$, con $ab \neq 0$, rappresenta ogni elemento di $\mathbb{F}_q$). Quindi utilizzando le relazioni scritte sopra, si deduce che

$$\text{se } 2 \nmid q, \qquad \mathbb{W}(\mathbb{F}_q) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{se } -1 \text{ è un quadrato in } \mathbb{F}_q \\ \mathbb{Z}/4\mathbb{Z} & \text{altrimenti} \end{cases}.$$

Non diamo altri dettagli sullo studio del gruppo di Witt e torniamo alla discussione iniziale sulle forme quadratiche.

Dato un polinomio omogeneo di grado 2 (forma quadratica) a coefficienti in K, sia $g(X_1,\dots,X_n)$, possiamo associare a questi il modulo quadratico (K^n, g), e quindi, date due forme quadratiche g_1 e g_2, scriveremo $g_1 \sim g_2$ per indicare che i corrispondenti moduli quadratici sono isometrici. Date due forme quadratiche $g(X_1,\dots,X_n)$ ed $h(X_1,\dots,X_m)$ indicheremo con $g\dot{+}h$ (risp. $g\dot{-}h$) la somma ortogonale (risp. differenza ortogonale) delle due forme, ovvero il modulo quadratico (K^{n+m}, f), ove $f(X_1,\dots,X_{n+m}) = g(X_1,\dots,X_n) + h(X_{n+1},\dots,X_{n+m})$ (risp. $f(X_1,\dots,X_{n+m}) = g(X_1,\dots,X_n) - h(X_{n+1},\dots,X_{n+m})$) ovvero $(K^{n+m}, f) = (K^n, g)\hat{\oplus}(K^m, h)$ (risp. $(K^{n+m}, f) = (K^n, g)\hat{\oplus}(K^m, -h)$).

In queste notazioni, i risultati già mostrati per i moduli quadratici possono essere enunciati nel modo seguente.

- Se f è non-degenere e rappresenta zero (cioè $f(\xi) = 0$ per qualche $\xi \neq (0,\dots,0)$), allora $f \sim f_1\dot{+}g$ con $g(X_1,X_2) = X_1X_2$ (ovvero g è la forma quadratica associata ad un piano iperbolico). Inoltre f rappresenta ogni elemento di K.
- L'esistenza di una base ortogonale per i moduli quadratici è equivalente al fatto che ogni forma quadratica è equivalente ad una 'somma di quadrati'; ovvero, per ogni forma quadratica f in n indeterminate, esistono delle costanti $a_1,\dots,a_n$ in K tali che $f \sim a_1X_1^2 + \cdots + a_nX_n^2$.
- Il Teorema di cancellazione di Witt è quindi equivalente a

$$g_1\dot{+}h_1 \sim g_2\dot{+}h_2, \quad g_1 \sim g_2 \qquad \Longrightarrow \qquad h_1 \sim h_2. \tag{4.7}$$

- Se f è una forma quadratica non-degenere, allora $f = g_1\dot{+}\cdots\dot{+}g_r\dot{+}h$ con $g_1,\dots,g_r$ piani iperbolici ed h forma quadratica che non rappresenta zero (cioè $h(\xi) = 0 \Rightarrow \xi = (0,\dots,0)$). Inoltre, l'intero $r \geq 0$ e la classe di isometria di h sono univocamente determinati da f.

Sempre nel linguaggio delle forme quadratiche, possiamo enunciare i seguenti

4.8 Corollario. *Siano $g(X_1,\dots,X_{n-1})$ una forma quadratica non-degenere ed $a \in K^\times$. Sono equivalenti:*

(i) g rappresenta a;

(ii) $g \sim h\dot{+}aZ^2$ per un'opportuna forma quadratica $h(X_1,\dots,X_{n-2})$;

(iii) *La forma* $f = g \dot{-} aZ^2$ *rappresenta* 0.

dim. È immediato verificare che *(ii)* $\Rightarrow$ *(i)* $\Rightarrow$ *(iii)*. Se vale *(iii)*, allora esiste $\xi = (x_1, \dots, x_n) \neq (0, \dots, 0)$ tale che $f(\xi) = 0$. Se $x_n = 0$, allora g rappresenta 0 e quindi ogni elemento di K, altrimenti $g(x_1/x_n, \dots, x_{n-1}/x_n) = a$ e quindi *(iii)* $\Rightarrow$ *(i)*. Infine, se vale *(i)*, esiste $v \in K^{n-1}$ tale che $v \cdot v = g(v) = a \neq 0$, allora $K^{n-1} = \langle v \rangle \hat{\oplus} \langle v \rangle^{\perp}$ (cf. *Proposizione II.4.2 (ii)*) e quindi, indicata con h la forma quadratica indotta su $\langle v \rangle^{\perp}$ si ottiene quanto affermato in *(ii)*. **CVD** □

4.9 Corollario. *Siano* g *ed* h *due forme quadratiche non-degeneri e sia* $f = g \dot{-} h$. *Sono equivalenti:*
(i) f *rappresenta* 0*;*
(ii) *esiste* $a \in K^{\times}$ *rappresentato sia da* g *che da* h*;*
(iii) *esiste* $a \in K^{\times}$ *tale che* $g \dot{-} aZ^2$ *ed* $h \dot{-} aZ^2$ *rappresentino entrambe lo* 0.

dim. È immediato verificare che *(ii)* $\Leftrightarrow$ *(iii)* e che *(ii)* $\Rightarrow$ *(i)*. Infine, se vale *(i)*, sia $0 = g(\xi) - h(\eta)$ e si ponga $a = g(\xi) = h(\eta)$. Se $a \neq 0$ è verificata la *(ii)*; se fosse $a = 0$, allora una almeno tra le due forme quadratiche, sia g, avrebbe un vettore isotropo non-nullo e quindi potrebbe rappresentare qualsiasi valore non-nullo di h. **CVD** □

Sia $p \neq 2$ un primo razionale ed interessiamoci della classificazione, a meno di isometria, delle forme quadratiche su $\mathbb{Q}_p$ e cominciamo la discussione introducendo due importanti invarianti da associare ad una forma quadratica.

Sia (V, q) un modulo quadratico non-degenere su $K = \mathbb{Q}_p$. Fissata una base ortogonale $\mathcal{V} = \{v_1, \dots, v_n\}$ di V $(p \neq 2)$, consideriamo le due grandezze

$$d(q, \mathcal{V}) = q(v_1) \cdots q(v_n), \qquad \text{e} \qquad \varepsilon(q, \mathcal{V}) = \prod_{1 \leq i < j \leq n} (q(v_i), q(v_j))_p, \tag{4.10}$$

ove $(\ ,\ )_p$ indica il Simbolo di Hilbert. Vogliamo mostrare che sia la classe di $d(q, \mathcal{V})$ in $K^{\times}/K^2$ che $\varepsilon(q, \mathcal{V})$ sono indipendenti dalla scelta della base ortogonale e sono perciò invarianti della forma quadratica q. Tali invarianti saranno detti, rispettivamente, il *discriminante* $d(q)$ ed il *simbolo* $\varepsilon(q)$ della forma quadratica q. Mostreremo poi che due moduli quadratici (V, q) e (V', q') sono isometrici se, e solo se, hanno la stessa dimensione, lo stesso discriminante e lo stesso simbolo.

Nelle notazioni precedenti, osserviamo che $d(q, \mathcal{V}) = q(v_1) \cdots q(v_n)$ è il determinante della matrice della forma bilineare associata a q, scritta rispetto alla base ortogonale $\mathcal{V}$. Poichè due matrici simmetriche A eB rappresentano la stessa applicazione bilineare se, e solo se, esiste una matrice invertibile P tale che ${}^tPAP = B$; è chiaro che la classe di $d(q, \mathcal{V})$ è determinata modulo quadrati. Scriveremo quindi $d(q) \in K^{\times}/K^2$ per indicare il discriminante di q, ovvero la classe di $d(q, \mathcal{V})$ in $K^{\times}/K^2$. Notiamo a margine che la definizione di discriminante può essere estesa a qualsiasi corpo K (di caratteristica diversa da 2).

La dimostrazione dell'invarianza del simbolo seguirà da un'osservazione e da alcuni calcoli espliciti sul simbolo di Hilbert. Per cominciare, diciamo che due basi di un modulo quadratico (V, q) sono *contigue* se hanno almeno un vettore in comune. Dimostriamo quindi la seguente Proposizione, che resta valida su ogni corpo K di caratteristica diversa da 2.

4.11 Proposizione. *Sia* (V, q) *un modulo quadratico non degenere su* K*, di dimensione* $n \geq 3$*, e siano* $\mathcal{V} = \{v_1, \dots, v_n\}$ *e* $\mathcal{V}' = \{v'_1, \dots, v'_n\}$ *due basi ortogonali di* V*. Allora esiste una successione finita di basi ortogonali,* $\mathcal{V}_0, \dots, \mathcal{V}_r$*, a due a due contigue, tale che* $\mathcal{V} = \mathcal{V}_0, \mathcal{V}_1, \dots, \mathcal{V}_r = \mathcal{V}'$.

dim. Cominciamo supponendo che $(v_1 \cdot v_1)(v'_1 \cdot v'_1) - (v_1 \cdot v'_1)^2 \neq 0$, ovvero che la restrizione di q a $\langle v_1, v'_1 \rangle$ sia non-degenere. In particolare ciò significa che $\langle v_1, v'_1 \rangle$ ha dimensione 2 e che $V = \langle v_1, v'_1 \rangle \oplus \langle v_1, v'_1 \rangle^{\perp}$. Allora si può considerare una base ortogonale $v''_3, \dots, v''_n$ di $\langle v_1, v'_1 \rangle^{\perp}$ e completarla con le due basi ortogonali v_1, w_1 e v'_1, w'_1 di $\langle v_1, v'_1 \rangle$. Poichè $n \geq 3$, le basi ortogonali

$$\{v_1, w_1, v''_3, \dots, v''_n\} \qquad \text{e} \qquad \{v'_1, w'_1, v''_3, \dots, v''_n\}$$

sono contigue tra loro ed ovviamente, contigue rispettivamente alle basi $\mathcal{V}$ e $\mathcal{V}'$.

Se invece $(v_1 \cdot v_1)(v_i' \cdot v_i') - (v_1 \cdot v_i')^2 \neq 0$ per $i = 1, 2$, allora, poichè la restrizione di q a $\langle v_1', v_2' \rangle$ è non degenere, esiste una costante $\lambda \in K$ tale che $v_0 = \lambda v_1' + v_2'$ è un vettore non isotropo, linearmente indipendente da v_1 e tale che la restrizione di q a $\langle v_1, v_0 \rangle$ sia non degenere. Allora si considera la decomposizione $V = \langle v_1, v_0 \rangle \oplus \langle v_1, v_0 \rangle^\perp$ e si completa una base ortogonale $w_3'', \dots, w_n''$ di $\langle v_1, v_0 \rangle^\perp$, con due basi ortogonali v_1, w_1 e v_0, w_0 di $\langle v_1, v_0 \rangle$. Infine, si osservi che $\langle v_0, v_1' \rangle = \langle v_1', v_2' \rangle$ e perciò la restrizione di q a tale spazio è non-degenere e quindi, ragionando come sopra, si può congiungere la base $\{v_0, w_0, w_3'', \dots, w_n''\}$ con $\mathcal{V}'$ tramite basi contigue. **CVD** □

Passiamo quindi a dimostrare l'indipendenza del simbolo $\varepsilon(q, \mathcal{V})$ dalla scelta della base ortogonale e facciamo induzione sula dimensione dello spazio V. Infatti, se $n = \dim V = 1$ il simbolo vale 1 in quanto è un prodotto su di un insieme vuoto di indici. Se $n = 2$, allora $q(X_1, X_2) = a_1 X_1^2 + a_2 X_2^2$ ed $\varepsilon(q) = (a_1, a_2)$ ed in base al *Corollario II.4.8* $(a_1, a_2) = 1$ se, e solo se, q rappresenta 1 e quindi la condizione non dipende dalla base scelta, ma dalla sola forma q.

Supponiamo ora $n \geq 3$ e supponiamo che $\mathcal{V}$ e $\mathcal{V}'$ siano due basi ortogonali contigue (cf. enuncita-contigue), ovvero siano $\mathcal{V} = \{v_1, \dots, v_n\}$ e $\mathcal{V}' = \{v_1, v_2', \dots, v_n'\}$ e poniamo $a_i = q(v_i)$ ed $a_i' = q(v_i')$, per $i = 1, \dots, n$. Per l'ipotesi induttiva, possiamo supporre

$$\prod_{2 \leq i < j \leq n} (a_i, a_j) = \prod_{2 \leq i < j \leq n} (a_i', a_j')$$

perchè si tratta del simbolo della restrizione di q al sottospazio $\langle v_1 \rangle^\perp$. Indichiamo con ν tale valore ed osserviamo che si ha $\varepsilon(q, \mathcal{V}) = (a_1, a_2 \cdots a_n)\nu$. Inoltre, per la bilinearità e la proprietà *(v)* del simbolo di Hilbert, si ottiene $(a_1, a_2 \cdots a_n) = (a_1, -a_1 a_2 \cdots a_n) = (a_1, -d)$, ove d rappresenta il discriminante della forma q, che è indipendente (a meno di quadrati) dalla scelta della base. Ciò permette di concludere.

Andiamo ora a dimostrare che il discriminante ed il simbolo permettono di classificare le forme quadratiche. Cominciamo dimostrando un Lemma sul simbolo di Hilbert che ci sarà utile nel seguito.

4.12 Lemma. *Siano $K = \mathbb{Q}_p$, $a \in K^\times/K^2$ ed $\varepsilon \in \{\pm 1\}$ e si ponga*

$$H_a^\varepsilon = \left\{\, x \in K^\times/K^2 \,|\, (x, a) = \varepsilon \,\right\}.$$

Allora si ha

(i) $a = 1 \quad \Rightarrow \quad H_a^1 = K^\times/K^2, \quad H_a^{-1} = \emptyset$;
(ii) se $a \neq 1$ allora H_a^ε contiene esattamente due elementi;
(iii) siano $a \neq 1 \neq a'$ ed $\varepsilon, \varepsilon' \in \{\pm 1\}$, allora

$$H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset \qquad \Leftrightarrow \qquad \begin{cases} a = a' \\ \varepsilon \neq \varepsilon' \end{cases}.$$

dim. Per la proprietà *(iii)* del simbolo di Hilbert, si ha $(x, 1) = 1$ per ogni x, mentre se $a \neq 1$, l'applicazione $x \mapsto (x, a)$ è una forma lineare non nulla sul $\mathbb{F}_2$-spazio vettoriale $K^\times/K^2$ che ha dimensione 2 (cf. *Teorema II.3.3* ed anche (II.2.12)). Ciò permette di concludere per quanto riguarda *(i)* e *(ii)*.
(iii) Cominciamo osservando che, se $\varepsilon = \varepsilon'$, allora non può aversi $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$. Dunque, se $\varepsilon \neq \varepsilon'$, si ha $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$ se, e solo se, $(x, a) = (x, a')$ per ogni $x \in K^\times/K^2$ e quindi $a = a'$ (cf. *Teorema II.3.3*).
CVD □

Il passo successivo è dimostrare che è sufficiente classificare i moduli quadratici di dimensione 'piccola'. In particolare, ricordiamo che il *rango* di una forma quadratica $q(X_1, \dots, X_n)$ è la dimensione di uno spazio vettoriale su cu q induce una forma quadratica non-degenere.

4.13 Proposizione. *Sia q una forma quadratica di rango n e siano d il discriminante di q ed ε il suo simbolo. Allora*

(i) q rappresenta zero se, e solo se,
- $n = 2$ *e* $d = -1$;
- $n = 3$ *ed* $\varepsilon = (-1, -d)$;
- $n = 4$ *e* $d \neq 1$ *oppure* $d = 1$ *ed* $\varepsilon = (-1, -1)$;
- $n \geq 5$.

(ii) dato $a \in K^\times/K^2$, q rappresenta a se, e solo se,
- $n = 1$ *e* $d = a$;
- $n = 2$ *ed* $\varepsilon = (a, -d)$;
- $n = 3$ *e* $a \neq -d$ *oppure* $a = -d$ *ed* $\varepsilon = (-1, -d)$;
- $n \geq 4$.

dim. Osserviamo che, punto per punto, *(i)* $\Rightarrow$ *(ii)*, come si deduce facilmente considerando la forma quadratica $aZ^2 - q$, e quindi ci limiteremo a dimostrare il punto *(i)* e ci serviremo delle conseguenze enunciate in *(ii)*.

Cominciamo dal caso $n = 2$; allora $a_1X_1^2 + a_2X_2^2$ rappresenta zero se, e solo se, $-a_1/a_2 \in K^2$ e quindi, se e solo se, $-d = 1$ in $K^\times/K^2$.

Sia ora $n = 3$; allora $a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ rappresenta zero se, e solo se, $\frac{1}{a_3}q$ rappresenta zero; ovvero, per la definizione del simbolo di Hilbert, se, e solo se, $(-\frac{a_1}{a_3}, -\frac{a_2}{a_3}) = 1$. Si ha (cf. *Teorema II.3.3*)

$$(-\frac{a_1}{a_3}, -\frac{a_2}{a_3}) = (-a_1a_3, -a_2a_3) = (-1,-1)(-1,a_2)(-1,a_3)(a_1,-1)(a_1,a_2)(a_1,a_3)(a_3,-1)(a_3,a_2)(a_3,a_3)$$

ed osservando che $(a_3, -1)(a_3, a_3) = (a_3, -a_3) = 1$, si ottiene che il prodotto a secondo membro è uguale a $(-1, -d)\varepsilon$ e ciò permette di concludere.

Sia ora $n = 4$ ed osserviamo che, in base al *Corollario II.4.9*, $a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$ rappresenta zero se, e solo se, esiste un elemento $a \in K^\times$ che sia rappresentato da entrambe le forme quadratiche $a_1X_1^2 + a_2X_2^2$ e $-a_3X_3^2 - a_4X_4^2$. Inoltre, per quanto osservato all'inizio della dimostrazione, dalla verifica del caso $n = 3$ del punto *(i)*, possiamo dedurre il caso $n = 2$ di *(ii)* e quindi concludere che, per un tale a deve aversi

$$(a, -a_1a_2) = (a_1, a_2) \qquad \text{e} \qquad (a, -a_3a_4) = (-a_3, -a_4).$$

Dunque, nelle notazioni del Lemma precedente, q non rappresenta lo zero se, e solo se, $H^{(a_1,a_2)}_{-a_1a_2} \cap H^{(-a_3,-a_4)}_{-a_3a_3} = \emptyset$ e ciò significa che deve aversi $a_1a_2 = a_3a_4$ (in $K^\times/K^2$) ed $(a_1, a_2) = -(-a_3, -a_4)$. Dalla prima relazione si deduce $d = 1$ e quindi, se $d \neq 1$, allora q rappresenta lo zero. Sia $d = 1$ e calcoliamo il simbolo ε. Ricordando che $d = 1$ e la bilinearità del simbolo di Hilbert, si ha

$$\begin{aligned}
\varepsilon &= (a_1, a_2)(a_3, a_4)(a_1a_2, a_3a_4) \\
&= (a_1, a_2)(a_3, a_4)(-a_1a_2a_3a_4, a_3a_4) \\
&= (a_1, a_2)(a_3, a_4)(-1, a_3a_4) \\
&= (a_1, a_2)(-a_3, -a_4)(-1, -1).
\end{aligned}$$

E la condizione $(a_1, a_2) = -(-a_3, -a_4)$ è quindi equivalente ad $\varepsilon \neq (-1, -1)$.

Sia infine $n = 5$. Si osservi che ogni forma di rango 2 rappresenta almeno due elementi di $K^\times/K^2$ perchè, se $d = -1$ allora la forma rappresenta zero e quindi ogni elemento di $K^\times$; altrimenti, (cf. *(ii)* per $n = 2$), q rappresenta a se, e solo se, $a \in H^{\varepsilon}_{-d}$ e, per il Lemma precedente, questo insieme contiene esattamente due elementi. Allora, esiste un elemento $a \neq d \in K^\times/K^2$ rappresentato da q. Possiamo quindi scrivere $q \sim g \dot{+} aZ^2$ ed il discriminante di g è diverso da 1, perchè $d(q) = a\,d(g)$. Quindi g ha rango 4 e rappresenta zero. Ciò conclude la dimostrazione. **CVD** □

Possiamo quindi concludere con il seguente

4.14 Teorema. *Siano q e g due forme quadratiche non-degeneri su $K = \mathbb{Q}_p$. Allora q e g sono isometriche se, e solo se, $d(q) = d(g)$ ed $\varepsilon(q) = \varepsilon(g)$.*

dim. Dimostriamolo per induzione su n. Se $n = 1$ la tesi è ovviamente vera (ed è sufficiente considerare il discriminante). Sia quindi $n \geq 2$ e supponiamo che la tesi sia vera per forme quadratiche di rango $n-1$. Per la *Proposizione II.4.13*, possiamo suppore che q e g rappresentino entrambe uno stesso elemento $a \in K^\times$. Si ha quindi $q \sim aZ^2 \dotplus q'$ e $g \sim aZ^2 \dotplus g'$ e da ciò si deduce $ad(g') = d(g) = d(q) = ad(q')$ e quindi $d(g') = d(q')$ ed inoltre, $(a, d(q'))\varepsilon(q') = \varepsilon(q) = \varepsilon(g) = (a, d(g'))\varepsilon(g')$, da cui si deduce che $\varepsilon(q') = \varepsilon(g')$ e ciò permette di concludere per l'ipotesi induttiva. **CVD** □

5. Il Teorema di Hasse e Minkowski

Il celebre Teorema di Hasse e Minkowski lega la rappresentabilità di un numero razionale tramite una forma quadratica a coefficienti razionali alla possibilità di rappresentare tale numero *localmente*, ovvero in ciascuno dei completamenti del corpo $\mathbb{Q}$. Tale risultato è ricco di conseguenze che cercheremo di illustrare lungo questa sezione.

Cominciamo con l'enunciato del Teorema.

5.1 Teorema. [Hasse-Minkowski] *Sia $f(\underline{X}) \in \mathbb{Q}[X_1, \dots, X_n]$ una forma quadratica. Allora f rappresenta lo zero in $\mathbb{Q}$ se, e solo se, f rappresenta lo zero su $\mathbb{Q}_v$, per ogni posto v di $\mathbb{Q}$.*

La dimostrazione di questo risultato e di alcune sue conseguenze si estenderà lungo tutta la sezione. Osserviamo ora alcuni fatti preliminari: per prima cosa è chiaro che è sufficiente dimostrare l'asserto sulla rappresentabilità dello zero per ottenere un analogo criterio di rappresentabilità per ogni numero razionale (cf. *Corollario II.4.8*); inoltre, è ovvio osservare che l'esistenza di uno zero 'globale' (in $\mathbb{Q}$) per la forma quadratica f implica l'esistenza degli zeri locali, visto che $\mathbb{Q}$ si immerge in ciascuno dei suoi completamenti; infine, come vedremo nel corso della dimostrazione, osserviamo che il criterio di Hasse e Minkowski è un criterio effettivo, perchè, come vedremo, sarà sufficiente conoscere la rappresentabilità dello zero in un numero finito di posti (determinabile a partire da f) per concludere sulla rappresentabilità globale.

Cominciamo la dimostrazione, che si farà discutendo separatamente i vari casi, al crescere del numero n delle variabili coinvolte.

$\boxed{n = 2}$ In tal caso, possiamo ridurci a considerare l'esistenza di soluzioni razionali ad un'equazione del tipo $X^2 = aY^2$, con $a \in \mathbb{Q}^\times$ e quindi, a meno di quadrati (che possono essere 'inglobati nelle soluzioni'), con $a \in \mathbb{Z} \setminus \{0\}$ e square-free (cf. *I* §.4); inoltre, poichè l'equazione è risolubile in $\mathbb{R}$, deve aversi $a > 0$. Sia quindi $a = p_1 \cdots p_r$ con $p_1 < p_2 < \cdots < p_r$, primi distinti e mostriamo che la risolubilità locale ci permette di concludere che $a = 1$ (ovvero che a è un quadrato). Infatti, se comparisse il primo p_1 ed (x_1, y_1) fosse una soluzione primitiva dell'equazione $X^2 = aY^2$ in $\mathbb{Q}_{p_1}$ (cf. *Proposizione II.2.2*), dovrebbe aversi $v_{p_1}(x_1) > 0$ e quindi $v_{p_1}(x_1^2) \geq 2$, da cui si dedurrebbe $v_{p_1}(y_1) \geq 1$, contro l'ipotesi che la soluzione sia primitiva. Ciò conclude la dimostrazione per $n = 2$.

Prima di procedere nella dimostrazione per i successivi valori di n, vogliamo osservare che, in questo caso, si potrebbe dimostrare un'asserto più forte sulla risolubilità locale, ovvero

Osservazione. *Una forma quadratica $f(\underline{X}) \in \mathbb{Q}[X_1, X_2]$ rappresenta lo zero in $\mathbb{Q}$ se, e solo se, rappresenta lo zero su $\mathbb{Q}_v$, per ogni posto v di $\mathbb{Q}$ ad eccezione di un numero finito.*

dim. In base a quanto osservato, si tratta di mostrare che, dato un intero a, il polinomio $X^2 - a$ è irriducibile in $\mathbb{Q}[X]$ se, e solo se, la congruenza $x^2 \equiv a \pmod{p}$ non ha soluzione per infiniti primi, ovvero se, e solo se, il simbolo di Legendre $\left(\frac{a}{p}\right) = -1$ per infiniti primi p. Dividendo per gli eventuali quadrati, si può supporre

$a = (-1)^\alpha 2^\varepsilon p_1 \cdots p_r$ con $2 < p_1 < \cdots < p_r$, primi distinti, ed $\alpha, \varepsilon \in \{0,1\}$ e mostriamo che se compare un primo nella fattorizzazione di a, allora $\left(\frac{a}{p}\right) = -1$ per infiniti primi p. Infatti, per ogni primo p, si ha

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^\alpha \left(\frac{2}{p}\right)^\varepsilon \prod_{i=1}^r \left(\frac{p_i}{p}\right).$$

I primi due fattori sono uguali ad 1 se $p \equiv 1 \pmod 8$ (cf. I.7.7), e sotto tali ipotesi, per reciprocità quadratica, si ha $\left(\frac{a}{p}\right) = \prod_{i=1}^r \left(\frac{p}{p_i}\right)$. Allora, se $r \geq 1$, fissato un elemento u che non sia un residuo quadratico modulo p_1, si ha

$$\left(\frac{a}{p}\right) = -1 \qquad \text{se} \qquad \begin{cases} p \equiv 1 \pmod{p_2 \cdots p_r} \\ p \equiv u \pmod{p_1} \\ p \equiv 1 \mod 8 \end{cases}$$

ovvero se $p \equiv u \pmod{8p_1 \cdots p_r}$. Per il Teorema di Dirichlet, vi sono infiniti primi soddisfacenti a questa condizione.

Infine, se $a = (-1)^\alpha 2$, per ogni primo p, si ha $\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^\alpha \left(\frac{2}{p}\right)$ e questi è certamente uguale a -1 se $p \equiv -3 \pmod 8$ ed anche in questo caso, per il Teorema di Dirichlet, vi sono infiniti primi soddisfacenti a questa condizione. **CVD** □

Torniamo alla dimostrazione del Teorema di Hasse e Minkowski e consideriamo ora il caso successivo.
$\boxed{n=3}$ Consideriamo quindi l'equazione $X^2 - aY^2 - bZ^2$ con $a, b \in \mathbb{Z} \setminus \{0\}$, entrambi square-free e con $|a| \leq |b|$. Facciamo induzione sul numero $|a| + |b|$ chè, per $|a| + |b| = 2$, l'equazione data ha soluzioni razionali se, e solo se, ha soluzioni in $\mathbb{R}$. Sia quindi $|a| + |b| = N > 2$ e supponiamo che la tesi sia vera per valori minori di N. Osserviamo che la risolubilità dell'equazione per ogni posto v, implica l'esistenza di soluzioni non nulle per la congruenza $t^2 \equiv a \pmod b$. Infatti, è sufficiente verificare la risolubilità di questa congruenza per i primi che dividono b e, se $p \mid a$ e $p \mid b$, allora vi è la soluzione $t = 0$, mentre se $p \mid b$ e $p \not| \, a$, allora c'è una soluzione primitiva (x, y, z) all'equazione $X^2 - aY^2 - bZ^2$ e, poichè b è square-free, deve aversi $v_p(y) = 0$, ovvero y è invertibile modulo p e ciò dice come si possa scegliere t. Si fissi quindi un numero intero t, con $|t| \leq \frac{|b|}{2}$, tale che $t^2 = a + bb'$ ed osserviamo che deve aversi

$$|b'| \leq \frac{|t|^2}{|b|} + \frac{|a|}{|b|} \leq \frac{|b|}{4} + 1 < |b|,$$

perchè $|b| \geq 2$. Inoltre, la condizione su t implica che $bb' = t^2 - a = N_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(t + \sqrt{a})$, e quindi b è la norma di un elemento di $\mathbb{Q}(\sqrt{a})$ se, e solo se, b' lo è. Ovvero l'equazione $X^2 - aY^2 - bZ^2$ ha soluzione se, e solo se, ha soluzione l'equazione $X^2 - aY^2 - b'Z^2$ e possiamo concludere in base all'ipotesi induttiva. Infatti, per ogni posto v, si ha $(a, bb')_v = 1$ (cf. *Lemma II.3.1*) e quindi, per la bilinearità del simbolo di Hilbert, deve aversi $(a, b')_v = (a, b)_v = 1$, che è quanto ci serve per concludere.

Ancora una volta interrompiamo il corso della dimostrazione per alcune osservazioni relative al caso appena trattato, che ha un'interessante applicazione geometrica.

Remark. Sia $\mathcal{C}$ una curva piana irriducibile di genere 0, definita sul corpo $\mathbb{Q}$ dei numeri razionali. Vogliamo mostrare che il Teorema di Hasse-Minkowski –e precisamente il caso $n = 3$ appena trattato– può essere usato per decidere dell'esistenza di punti di $\mathcal{C}$ su $\mathbb{Q}$. Siano quindi $f(X, Y) \in \mathbb{Q}[X, Y]$ un polinomio assolutamente irriducibile ed $A = \mathbb{Q}[X, Y]/(f(X, Y))$, di modo che $K = Frac\, A$ sia il corpo delle funzioni razionali su $\mathcal{C}$. Poichè la curva $\mathcal{C}$ ha genere 0, $K \otimes \overline{\mathbb{Q}} \cong \overline{\mathbb{Q}}(t)$ e quindi esistono due funzioni $r(t)$ ed $s(t)$ in $\overline{\mathbb{Q}}(t)$ tali che $f(r(t), s(t)) = 0$ in tale anello.

Osserviamo che *le funzioni $r(t)$ ed $s(t)$ possono essere scelte in $\mathbb{Q}(t)$ se, e solo se, $\mathcal{C}$ ha un punto non-singolare definito su $\mathbb{Q}$.* e quindi che, in tal caso, ha infiniti punti razionali su $\mathbb{Q}$. Infatti, se P è un punto razionale di $\mathcal{C}$, per il Teorema di Riemann-Roch (!precisare per corpi non algebricamente chiusi!), lo spazio vettoriale delle funzioni razionali ϕ (in K) tali che $(\phi)+P$ sia un divisore positivo, ha dimensione (su $\mathbb{Q}$) uguale a 2 e quindi esiste in tale spazio una funzione razionale $\tau(t)$ non costante che ha solo un polo semplice in P e quindi $\mathbb{Q}(\tau)=K=\mathbb{Q}(\mathcal{C})$.

Possiamo quindi rispondere alla domanda sull'esistenza di punti razionali su $\mathcal{C}$ tramite il Teorema di Hasse e Minkowski, mostrando che la curva razionale $\mathcal{C}$ è birazionalmente equivalente ad una curva piana di grado ≤ 2 e perciò deducendo l'esistenza di punti razionali per $\mathcal{C}$ dall'esistenza di punti razionali per tale curva. Consideriamo quindi la curva piana $\mathcal{C}$ ed il differenziale dx. Il divisore D di dx ha grado -2, come si può dedurre dal teorema di Riemann-Roch e quindi, lo spazio vettoriale delle funzioni razionali ϕ su $\mathcal{C}$, tali che $(\phi)-D$ sia un divisore positivo, ha dimensione 3. Sia ϕ una di tali funzioni e si consideri il divisore positivo (e razionale su $\mathbb{Q}$) $\phi-D=(P)+(Q)$, con P e Q non necessariamente distinti. Sia quindi $1,x,y$ una base dello spazio vettoriale delle funzioni razionali tali che $(\phi)+(P)+(Q)$ sia un divisore positivo. Se x, oppure y, ha solo un polo semplice in uno dei due punti, sia P; allora P è un punto razionale di $\mathcal{C}$ e quindi, ragionando come sopra, $\mathbb{Q}(\mathcal{C})=\mathbb{Q}(x)$ ed abbiamo concluso. Altrimenti, il divisore polare di x è $(P)+(Q)$ e considerando le funzioni $1,x,y,x^2,y^2,xy$, si conclude che tutte queste stanno nello spazio delle funzioni con divisore maggiore o uguale a $2(P)+2(Q)$; tale spazio ha dimensione 5 e quindi le funzioni date sono linearmente dipendenti, ovvero c'è una relazione quadratica tra x ed y. Si ha quindi $\mathbb{Q}(x,y)\subseteq\mathbb{Q}(\mathcal{C})$ e se i due corpi fossero distinti, dall'osservazione che $[\mathbb{Q}(\mathcal{C}):\mathbb{Q}(x)]=2$ (x ha due poli su $\mathcal{C}$), si dovrebbe concludere che $y\in\mathbb{Q}(x)$. Poichè y ha gli stessi poli di x, y dovrebbe essere una funzione polinomiale di grado 1 nella x, contro l'ipotesi che $1,x,y$ siano linearmente indipendenti. Ciò conclude la discussione.

5.2 Remark. Proseguiamo nelle nostre osservazioni dando un'altra dimostrazione del Teorema di Hasse-Minkowski nel caso in cui $n=3$, basata sul Teorema di Minkowski (cf. *Teorema I.10.6*). Ci interessiamo quindi degli zeri di una forma quadratica $f(\underline{X})=aX^2+bY^2-cZ^2$ ove possiamo supporre $a,b,c\in\mathbb{Z}_{>0}$, square-free ed a due a due coprimi. In particolare, per quanto riguarda l'ultima condizione sui coefficienti, si osservi che è possibile ottenere una tale forma quadratica con un ragionamento induttivo sul numero di fattori primi del prodotto abc dei coefficienti. Infatti se per un fattore primo p si avesse $a=pa'$ e $b=pb'$, allora, posto $Z=pZ'$, gli zeri della forma quadratica data, sarebbero in ovvia corrispondenza con gli zeri della forma $a'X^2+b'Y^2+pcZ'^2$ si otterrebbe così una forma quadratica con un numero strettamente minore di fattori primi nel prodotto dei coefficienti.

Dati due numeri reali positivi λ,μ, si consideri la regione di $\mathbb{R}^3$ così definita

$$\mathcal{R}_{\lambda,\mu}=\left\{\,(x,y,z)\in\mathbb{R}^3\,|\,ax^2+by^2\leq\lambda,\quad cy^2\leq\mu\,\right\}.$$

È chiaro che si tratta di un cilindro e quindi di una regione chiusa, limitata, convessa e simmetrica rispetto all'origine di $\mathbb{R}^3$, il cui volume è uguale a $\dfrac{2\pi\lambda\sqrt{\mu}}{\sqrt{abc}}$. Inoltre $\max\limits_{\underline{x}\in\mathcal{R}_{\lambda,\mu}}|f(\underline{x})|\leq\max\{\lambda,\mu\}$.

Vediamo ora di determinare un sottoreticolo di $\mathbb{Z}^3$. Sia $p\neq 2$ un primo che divide abc, allora $f(\underline{X})$ è congrua, modulo p, ad una forma in due variabili, che ha uno zero non banale modulo p (cf. *Proposizione II.2.2*), e quindi è prodotto di due forme lineari L_p ed M_p. Consideriamo quindi i reticoli

$$\Lambda_p=\{\,(x,y,z)\in\mathbb{Z}_3\,|\,L_p(x,y,z)\equiv 0 \pmod p\,\}\qquad \text{per } 2\neq p\mid abc,$$

e si osservi che Λ_p ha indice p in $\mathbb{Z}^3$, come si vede facilmente considerando la dimensione del nucleo di una forma lineare su $\mathbb{F}_p^3$. Se $2\nmid abc$, $f(\underline{X})\equiv(aX+bY-cZ)^2 \pmod 2$, e quindi posto $L_2(X,Y,Z)=aX+bY-cZ$, si consideri il sottoreticolo

$$\Lambda_2=\{\,(x,y,z)\in\mathbb{Z}_3\,|\,L_2(x,y,z)\equiv 0 \pmod 2\,\},$$

che ha indice p in $\mathbb{Z}^3$. Se invece $2\mid abc$, si consideri il sottoinsieme

$$\Lambda_2=\{\,(x,y,z)\in\mathbb{Z}_3\,|\,f(x,y,z)\equiv 0 \pmod 4\,\},$$

e verifichiamo che si tratta di un sottoreticolo di indice 4 in $\mathbb{Z}^3$. Per fissare le idee, supponiamo che $2\mid a$ ed osserviamo che, se (x_1,y_1,z_1) ed (x_2,y_2,z_2) appartengono a Λ_2, allora

$$a(x_1+x_2)^2+b(y_1+y_2)^2-c(z_1+z_2)^2\equiv 2(by_1y_2-cz_1z_2) \pmod 4.$$

Inoltre, poichè $(x_1,y_1,z_1)\in\Lambda_2$ e $2\mid a$, si ha che $by_1^2-cz_1^2\equiv 0 \pmod 2$ e quindi $by_1-cz_1\equiv 0 \pmod 2$. Se ne deduce che (y_1,z_1) ed (y_2,z_2) determinano elementi di $\mathbb{F}_2^2$ che sono nel nucleo della stessa forma quadratica e sono quindi proporzionali. Ciò permette di concludere che $by_1y_2-cz_1z_2\equiv 0 \pmod 2$, che è quanto ci serviva per concludere che Λ_2 è un sottoreticolo di $\mathbb{Z}^3$. Per quanto riguarda l'indice del reticolo Λ_2, si osservi che $2\mathbb{Z}^3\subset\Lambda_2$

e che la condizione $by - cz \equiv 0 \pmod 2$ dice che (y, z) varia in un sottospazio 1-dimensionale di $\mathbb{F}_2^2$ e inoltre, per ogni tale scelta di y e z, x è completamente determinato modulo 2 e quindi $\dim_{\mathbb{F}_2}(\Lambda_2/2\mathbb{Z}^3) = 1$ e quindi, Λ_2 ha indice 4 in $\mathbb{Z}^3$.

In ogni caso, si pone

$$\Lambda = \bigcap_{p|2abc} \Lambda_p \qquad \text{e si ha} \qquad \mathbb{Z}^3/\Lambda \cong \bigoplus_{p|2abc} \mathbb{Z}^3/\Lambda_p$$

e quindi Λ è un sottoreticolo di indice $2abc$ di $\mathbb{Z}^3$. Ciò significa che il dominio fondamentale di Λ ha volume $2abc$ e quindi, per il teorema di Minkowski (cf. *Teorema I.10.6*), vi è intersezione tra Λ ed il cilindro $\mathcal{R}_{\lambda,\mu}$ se

$$\frac{2\pi\lambda\sqrt{\mu}}{\sqrt{abc}} \geq 16abc.$$

In particolare, se $\lambda = \mu$, vi è un'intersezione se $\lambda \geq \dfrac{4abc}{\pi^{2/3}}$ e quindi supponiamo che sia $\lambda = \mu = \dfrac{4abc}{\pi^{2/3}}$, da cui si deduce che esiste un elemento $0 \neq \underline{v} \in \Lambda \cap \mathcal{R}_{\lambda,\lambda}$, e quindi si ha

$$f(\underline{v}) \equiv 0 \pmod{2abc} \qquad \text{e} \qquad |f(\underline{v})| \leq \frac{4}{\pi^{2/3}} abc < 2abc,$$

che può aversi se, e solo se, $f(\underline{v}) = 0$ e qundi $\underline{v}$ è la soluzione intera cercata.

Osserviamo che entrambo i metodi utilizzati per la dimostrazione nel caso $n = 3$, permettono di dare una stima del valore assoluto (reale) delle soluzioni in termini del valore assoluto dei coefficienti. La dimostrazione basata sul teorema di Minkowski ha permesso di affermare che, se la forma quadratica $f(\underline{X}) = aX^2 + bY^2 - cZ^2$ con $a, b, c \in \mathbb{Z}_{>0}$, square-free, a due a due coprimi ha una soluzione in $\mathbb{Q}$, allora esiste una soluzione intera $\underline{x} = (x, y, z)$ con $|f(\underline{x})| \leq \dfrac{4}{\pi^{2/3}} abc$, da cui si deducono le disuguaglianze

$$|x| < \frac{2}{\pi^{1/3}}\sqrt{bc} \leq \frac{2}{\pi^{1/3}} M, \qquad |y| < \frac{2}{\pi^{1/3}}\sqrt{ac} \leq \frac{2}{\pi^{1/3}} M, \qquad |z| < \frac{2}{\pi^{1/3}}\sqrt{ab} \leq \frac{2}{\pi^{1/3}} M;$$

ove $M = \max\{|a|, |b|, |c|\}$.

Per determinare un'altra stima del valore assoluto dele soluzioni, ricordiamo che nel metodo delineato nella dimostrazione del Teorema di Hasse-Minkowski nel caso $n = 3$, la forma quadratica era stata posta nella forma $X^2 - aY^2 - bZ^2$ con $a, b \in \mathbb{Z} \setminus \{0\}$, entrambi square-free e con $|a| \leq |b| = m$ ove si supponeva $m > 1$ per escludere il caso banale. Si consideri ora l'intero t, tale che $t^2 = a + bb'$ e $|t| \leq \frac{m}{2}$. Da ciò si deduce che $|b'| \leq \frac{m}{4} + 1 < m$ ed è equivalente considerare l'equazione $x_1^2 - ay_1^2 - b''z_1^2$ in luogo di quella di partenza, ove , b'' è definito dalla condizione di essere square-free e legato a b' dalla relazione $b' = q^2 b''$, per qualche intero q. In particolare, si ha $\max\{|a|, |b''|\} \leq m$, ove vale la disuguaglianza stretta se $|a| < |b| = m$. [.......]

Vogliamo quindi procedere nella dimostrazione del Teorema di Hasse-Minkowski trattando un ulteriore caso.

$\boxed{n = 4}$ Si consideri quindi la forma quadratica $aX^2 + bY^2 - cZ^2 - dW^2$ e si ponga $f(X, Y) = aX^2 + bY^2$ e $g(Z, W) = cZ^2 + dW^2$. Allora, in base al *Corollario II.4.9*, per ogni posto v esiste un elemento $t_v \in \mathbb{Q}_v^\times$ che è rappresentato sia da f che da g. Applicando la *Proposizione II.4.13*, ciò significa che per ogni posto v, deve aversi

$$(t_v, -ab)_v = (a, b)_v \qquad \text{e} \qquad (t_v, -cd)_v = (c, d)_v.$$

Siamo nelle ipotesi del *Teorema II.3.5* e quindi esiste un elemento $x \in \mathbb{Q}^\times$ che può essere posto in luogo di tutti gli elementi t_v e quindi le forme quadratiche $f - xZ^2$ e $g - xT^2$ rappresentano lo 0 in ciascuno dei $\mathbb{Q}_v$ e quindi, essendo forme quadratiche in 3 variabili, rappresentano lo 0 in $\mathbb{Q}$. A questo punto, è sufficiente ricordare il *Corollario II.4.8* per concludere.

$\boxed{n \geq 5}$ Dimostriamo l'asserto per induzione, supponendo che sia vero per forme quadratiche di rango minore di n. Sia $f(\underline{X}) = a_1X_1^2 + \cdots + a_nX_n^2$, con $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ e consideriamo le due forme quadratiche $h(X_1, X_2) = a_1X_1^2 + a_2X_2^2$ e $g(X_3, \ldots, X_n) = -a_3X_3^2 + \cdots - a_nX_n^2$. Dunque si ha $f = h - g$ e, per ogni posto v di $\mathbb{Q}$, esiste un elemento $x_v \in \mathbb{Q}_v^\times$ rappresentato sia da h che da g (cf. *Corollario II.4.9*). Si consideri l'insieme di posti

$$S = \{\infty, 2\} \cap \{\,\ell \,|\, \ell \text{ primo ed } \ell \mid a_i \ \exists i\,\}$$

e, per $v \in S$, indichiamo con $u_{1,v}$ ed $u_{2,v}$ due elementi di $\mathbb{Q}_v^\times$ tali che $h(u_{1,v}, u_{2,v}) = x_v$. Allora, per il principio di approssimazione debole (cf. *Proposizione II.1.10*), esistono $u_1, u_2 \in \mathbb{Q}^\times$ tali che $u_i/u_{i,v}$ sia un quadrato, per $i = 1, 2$ e per ogni $v \in S$. Allora, posto $x = h(u_1, u_2) \in \mathbb{Q}$ si ha che $h \dot{-} xZ^2$ rappresenta lo 0 su $\mathbb{Q}$. Inoltre $xT^2 - g$ rappresenta lo 0 su ogni $\mathbb{Q}_v$ perchè, per $v \in S$ la tesi è vera per x_v ed x/x_v è un quadrato in $\mathbb{Q}_v$, mentre, per $v \notin S$ la forma quadratica g ha rango maggiore o uguale a 3 ed i coefficienti suoi coefficienti sono unità in $\mathbb{Z}_v$. Quindi, per ipotesi induttiva, $xT^2 - g$ rappresenta lo zero in $\mathbb{Q}$ e perciò sia h che g rappresentano x in $\mathbb{Q}$, che è quanto ci basta per concludere (cf. *Corollario II.4.9*). **CVD**
□

5.3 Remark. [*Rappresentazione di interi come somma di quadrati*] Cominciamo cercando di determinare i numeri interi positivi n, per cui si abbia $n = x_1^2 + x_2^2$, con $x_1, x_2 \in \mathbb{Q}$. Ciò equivale a chiedere che la forma quadratica $nx_3^2 - x_1^2 - x_2^2$ rappresenti lo zero in ogni $\mathbb{Q}_p$, e ciò accade se, e solo se, il discriminante d ed il simbolo ε della forma quadratica sono legati dalla relazione $\varepsilon = (-1, -d)_p$, per ogni primo p (cf. *Proposizione II.4.13*). Dunque n è somma di due quadrati in $\mathbb{Q}$ se, e solo se, $1 = (-1, n)_p$ per ogni primo p. Questa condizione è ovviamente soddisfatta se $p \not| \, n$ e $p \neq 2$, mentre se $2 \not| \, n$, deve aversi inoltre, $\varepsilon(n) = 0$, ovvero $n \equiv 1 \pmod 4$ (cf. *Teorema II.3.2*). Se poi $n = p^\alpha u$, con $\alpha > 0$, si ha

$$(-1, n)_p = \begin{cases} \left(\frac{-1}{p}\right)^\alpha & \text{se } p \neq 2 \\ (-1)^{\varepsilon(n)} & \text{se } p = 2 \end{cases} \qquad \text{(cf. } \textit{Teorema II.3.2} \text{ e (I.7.6))}.$$

Possiamo quindi concludere che n si scrive come somma di due quadrati in $\mathbb{Q}$ se i primi dispari che compaiono nella fattorizzazione di n con esponente dispari sono tutti congrui 1 modulo 4.

Consideriamo ora il problema di determinare i numeri interi positivi n, per cui si abbia $n = x_1^2 + x_2^2 + x_3^2$, con $x_1, x_2, x_3 \in \mathbb{Q}$. Si tratta quindi di trovare i valori di n per cui la forma quadratica $nX_4 - x_1^2 - x_2^2 - x_3^2$ rappresenta zero su ogni $\mathbb{Q}_p$. La condizione della *Proposizione II.4.13* è verificata per ogni valore di n se $p \neq 2$. Mentre, per $p = 2$, la forma rappresenta lo zero se, e solo se, il suo discriminante $-n$ non è un quadrato in $\mathbb{Q}_2$; ovvero se n non è della forma $n = 4^\alpha(8k - 1)$.

Osserviamo a margine come si possa ridurre ad una conseguenza di quanto discusso sopra, il problema di determinare se *ogni numero intero n sia somma di tre numeri triangolari*, ovvero se l'equazione

$$n = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2}$$

abbia soluzioni intere non-banali. Infatti, moltiplicando per 8 e sommando 3 ai due membri dell'equazione, si ottiene un'equazione della forma

$$8n + 3 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2,$$

che ci riconduce alla questione di verificare se il numero $8n + 3$ sia rappresentabile in $\mathbb{Z}$ come somma di tre quadrati(*). Come abbiamo visto sopra il problema è risolubile in $\mathbb{Q}$ e vedremo (cf. *Lemma II.5.4*) che ciò è sufficiente per l'esistenza di soluzioni intere.

La questione di determinare soluzioni intere a ciascuno dei problemi precedenti può essere decisa grazie al seguente

(*) Si osservi che il quadrato di un numero intero è congruo a 0, 1 o 4, modulo 8 e quindi una soluzione intera del problema $8n + 3 = X^2 + Y^2 + Z^2$ è necessariamente costituita da tre numeri dispari.

5.4 Lemma. [Davenport-Cassels] *Sia f una forma quadratica di rango n, definita positiva, a coefficienti in $\mathbb{Z}$ e supponiamo che per ogni $x \in \mathbb{Q}^n$ esista $y \in \mathbb{Z}^n$ tale che $f(x-y) < 1$. Allora $m \in \mathbb{Z}$ è rappresentato da f su $\mathbb{Z}$ se, e solo se, m è rappresentato da f su $\mathbb{Q}$.*

dim. Sia $x \in \mathbb{Z}^n$ e $t \in \mathbb{Z}_{\geq 1}$, tale che $f(x/t) = m$ e mostriamo che si può trovare un elemento $v = x'/t'$, tale che $f(x'/t') = m$ e $0 < t' < t$. È chiaro che, in tal modo, dopo un numero finito di passi, si ottiene la soluzione intera (cioè con denominatore $t = 1$). La costruzione di v procede nel modo seguente: se $t > 1$, si considera un elemento $y \in \mathbb{Z}^n$ tale che $\frac{x}{t} = y + z$, con $f(z) < 1$ e si determina il secondo punto di intersezione (dopo $\frac{x}{t}$) tra la retta per y e $\frac{x}{t}$ e la conica $f(X) = m$. Si verifica poi che questo punto di intersezione soddisfa alle condizioni richieste. Si consideri quindi il valore di $\lambda \neq 0$ per cui si ha $(\frac{x}{t} + \lambda z) \cdot (\frac{x}{t} + \lambda z) = m$, ovvero

$$\lambda = -2\,\frac{z \cdot \frac{x}{t}}{z \cdot z},$$

ove si è indicato con un puntino il prodotto scalare associato ad f. E ricordando che $z = \frac{x}{t} - y$ con $y \in \mathbb{Z}^n$, si osservi che si ha

$$v = \frac{x}{t} - 2z\,\frac{z \cdot \frac{x}{t}}{z \cdot z} = \frac{x}{t}\left(1 - 2\,\frac{z \cdot \frac{x}{t}}{z \cdot z}\right) + 2y\,\frac{z \cdot \frac{x}{t}}{z \cdot z} = x\,\frac{z \cdot (z - 2\frac{x}{t})}{t\, z \cdot z} + 2y\,\frac{z \cdot x}{t\, z \cdot z}$$

e inoltre

$$\begin{aligned} z \cdot (z - 2\frac{x}{t}) &= (\frac{x}{t} - y) \cdot (-\frac{x}{t} - y) = y \cdot y - m = a \in \mathbb{Z} \\ z \cdot x &= \frac{x}{t} \cdot x - y \cdot x = tm - y \cdot x = b \in \mathbb{Z} \\ t^2 z \cdot z &= (ty - x) \cdot (ty - x) = t^2 y \cdot y - 2ty \cdot x + 2mt^2 - mt^2 = at^2 + 2bt = t(at + 2b) \end{aligned}$$

e da ciò si deduce che $t' = tz \cdot z = at + 2b \in \mathbb{Z}$ e dalla disuguaglianza $z \cdot z < 1$ si conclude che $v = \frac{ax+2by}{t'}$ soddisfa alla condizione $f(v) = m$ ed ha il denominatore $0 < t' < t$, che è quanto volevamo. **CVD** □

Tornando alle forme quadratiche in questione, ovvero $\sum_{i=1}^{r} X_i^2$, si osservi che per ogni vettore $x \in \mathbb{Q}^r$ esiste un elemento $y \in \mathbb{Z}^r$ tale che $|x_i - y_i| \leq \frac{1}{2}$ per $i = 1, \dots, r$. Allora, se $r \leq 3$, si ha $\sum_{i=1}^{r} (x_i - y_i)^2 \leq \frac{r}{4} < 1$, e quindi sono soddisfatte le ipotesi del Lemma di Davenport e Cassels e perciò le considerazioni fatte in precedenza sulla rappresentabilità in $\mathbb{Q}$ restano valide per decidere della rappresentabilità in $\mathbb{Z}$ di un intero come somma di quadrati. Infine, per quanto riguarda il problema di esprimere un intero positivo n come somma di quattro quadrati di numeri interi, si può ragionare così: si scriva $n = 4^\alpha k$, ove $4 \nmid k$, e si osservi che, per le considerazioni precedenti se $k \not\equiv -1 \pmod 8$, allora n si scrive come somma di tre quadrati di numeri interi. Se poi $k \equiv -1 \pmod 8$, allora esistono tre interi x, y, z tali che $k - 1 = x^2 + y^2 + z^2$ e si conclude quindi che

$$n = 4^\alpha k = (2^\alpha x)^2 + (2^\alpha y)^2 + (2^\alpha z)^2 + (2^\alpha)^2,$$

che è quanto volevamo mostrare$^{(\dagger)}$.

$^{(\dagger)}$ Si osservi che, in base alla *Proposizione II.4.13*, ogni numero intero positivo n, si scrive come $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, con $x_1, x_2, x_3, x_4 \in \mathbb{Q}$: ma in questo caso non è più applicabile il Lemma di Davenport e Cassels e perciò si è preferito un approccio diretto al problema.

6. Punti razionali e punti p-adici per le curve

Il Teorema di Hasse-Minkowski asserisce che, per le forme quadratiche, l'esistenza di zeri razionali è equivalente all'esistenza di zeri sui corpi p-adici, per ogni p; e da ciò avevamo dedotto, in particolare, un criterio per l'esistenza di punti razionali su di una curva di genere 0. Come abbiamo visto, l'esistenza di punti p-adici per una curva è legata all'esistenza di punti non-singolari su $\mathbb{F}_p$ e, nel caso di curve di genere zero, ci si può ricondurre al problema dell'esistenza di zeri non-banali per le coniche. Queste ultime sono definite da equazioni omogenee di grado 2 in 3 variabili e quindi, si può ottenere una risposta dal teorema di Chevalley-Warning (cf. *Teorema I.7.13*).

Il problema analogo per curve di genere superiore, presenta invece un carattere profondamente diverso e mette subito davanti a notevoli difficoltà. Per citare qualche risultato in questa direzione, ricordiamo che Gauss determinò un metodo per studiare le soluzioni in $\mathbb{F}_p$ dell'equazione $x^3+y^3=1$. Circa un secolo dopo, Hasse provò che, indicato con N_p il numero dei punti in $\mathbb{F}_p$ della chiusura proiettiva di una cubica in forma di Weierstrass: $y^2=x^3+ax+b$, è soddisfatta la condizione

$$|N_p-p-1|\le 2\sqrt{p},$$

al variare di p. Questo risultato fu generalizzato da Weil, il quale mostrò che per una curva $\mathcal{C}$, assolutamente irriducibile, di genere g, definita su $\mathbb{F}_p$, vale la condizione

$$|N_p-p-1|\le 2g\sqrt{p},$$

ove, ancora una volta, N_p indica il numero dei punti del modello proiettivo non-singolare di $\mathcal{C}$. Inoltre, Weil congetturò che, per una varietà generica V, non-singolare, di dimensione r, dovesse aversi

$$|N_V-N_{\mathbb{P}}|<cp^{r/2}\qquad \text{per un'opportuna costante } c,$$

ove N_V indica il numero dei punti di V su $\mathbb{F}_p$, mentre $N_{\mathbb{P}}$ indica il numero di punti dello spazio proiettivo di dimensione r sullo stesso campo. La congettura di Weil venne poi dimostrata da P. Deligne, all'inizio degli anni '70.

La dimostrazione di questi risultati va ben al di là dell'ambito di queste note. Qui ci limiteremo a descrivere il metodo utilizzato da Gauss per contare le soluzioni di equazioni cubiche su corpi finiti. Consideriamo quindi il polinomio

$$F(X,Y,Z)=aX^3+bY^3-Z^3,\qquad \text{con } a,b\in\mathbb{F}_p^\times,$$

e cerchiamo di determinare il numero N_p degli elementi dell'insieme $S=\{\,(x,y,z)\in\mathbb{F}_p^3 \mid F(x,y,z)=0\,\}$. Sia ζ una radice p-esima primitiva dell'unità e si osservi che, al variare di h in $\mathbb{F}_p$, si ha

$$\frac{1}{p}\sum_{t\in\mathbb{F}_p}\zeta^{ht}=\begin{cases}1 & \text{se } h=0\\ 0 & \text{altrimenti}\end{cases}\tag{6.1}$$

Dunque, dati arbitrariamente $(x,y,z)\in\mathbb{F}_p^3$, si ha

$$\frac{1}{p}\sum_{t\in\mathbb{F}_p}\zeta^{tF(x,y,z)}=\begin{cases}1 & \text{se } (x,y,z)\in S\\ 0 & \text{altrimenti}\end{cases};$$

da cui si deduce che

$$\sum_{(x,y,z)\in\mathbb{F}_p^3}\frac{1}{p}\sum_{t\in\mathbb{F}_p}\zeta^{tF(x,y,z)}=N_p.$$

Possiamo scambiare l'ordine di somma e mettere in evidenza gli addendi per cui $t = 0$; in tal modo si ottiene

$$N_p = \frac{1}{p} \sum_{t\in\mathbb{F}_p} \sum_{(x,y,z)\in\mathbb{F}_p^3} \zeta^{tF(x,y,z)} = p^2 + \frac{1}{p} \sum_{t\in\mathbb{F}_p^\times} \sum_{(x,y,z)\in\mathbb{F}_p^3} \zeta^{tF(x,y,z)}.$$

Fissato $t \neq 0$, si ha

$$\sum_{(x,y,z)\in\mathbb{F}_p^3} \zeta^{tF(x,y,z)} = \sum_{z\in\mathbb{F}_p} \zeta^{-tz^3} \sum_{x\in\mathbb{F}_p} \zeta^{tax^3} \sum_{y\in\mathbb{F}_p} \zeta^{tby^3};$$

e quindi, posto

$$\sigma_h = \sum_{x\in\mathbb{F}_p} \zeta^{hx^3},$$

si può scrivere

$$N_p = p^2 + \frac{1}{p} \sum_{t\in\mathbb{F}_p^\times} \sigma_{ta}\sigma_{tb}\sigma_{-t}. \tag{6.2}$$

Ricordiamo ora che $\mathbb{F}_p^\times$ è un gruppo ciclico di ordine $p-1$ e quindi:

- se $p \equiv 2 \pmod 3$, allora la corrispondenza $x \mapsto x^3$ è biunivoca in $\mathbb{F}_p$ e perciò $\sigma_h = 0$, non appena $h \neq 0$ (II.6.1). Si conclude perciò che per primi di questo tipo, si ha $N_p = p^2$.
- se invece, $p \equiv 1 \pmod 3$, allora i cubi (degli elementi non-nulli) formano un sottogruppo di $\mathbb{F}_p^\times$ di indice 3 e non si può più applicare il ragionamento del punto precedente. In questo caso, cerchiamo una maggiorazione del numero $|N_p - p^2|$.

Supponiamo quindi $p \equiv 1 \pmod 3$ e sia g un generatore del gruppo ciclico $\mathbb{F}_p^\times$. Fissata una radice cubica primitiva dell'unità, $\varepsilon \in \mathbb{C}$, possiamo considerare il carattere (moltiplicativo) $\chi : \mathbb{F}_p^\times \to \mathbb{C}$ definito ponendo $\chi(g^m) = \varepsilon^m$, per ogni elemento $g^m \in \mathbb{F}_p^\times$. È chiaro che il nucleo di χ è formato dai cubi di $\mathbb{F}_p^\times$. Analogamente a quanto si è fatto per il Simbolo di Legendre (cf. *I*,§.7)), si può estendere il carattere χ ad $\mathbb{F}_p$, ponendo $\chi(0) = 0$.

Vogliamo mostrare un semplice

6.3 Lemma. *Notazioni come sopra. Allora, dato $w \in \mathbb{F}_p$, il numero di soluzioni in $\mathbb{F}_p$ dell'equazione $X^3 = w$ coincide con $1 + \chi(w) + \chi^2(w)$.*

dim. Osserviamo che la formula è vera per $w = 0$. Inoltre, poichè $p \equiv 1 \pmod 3$, esiste in $\mathbb{F}_p$ una radice cubica primitiva di 1 e perciò, se w è un cubo in $\mathbb{F}_p^\times$, allora vi sono esattamente 3 soluzioni all'equazione data e, in questo caso $3 = 1 + \chi(w) + \chi^2(w)$. Infine, se w non è un cubo in $\mathbb{F}_p^\times$, non vi sono soluzioni per l'equazione data e, d'altra parte, si ha $1 + \chi(w) + \chi^2(w) = 0$. **CVD** □

Dunque, dal lemma precedente, si deduce che, per $h \neq 0$, si ha

$$\sigma_h = \sum_{x\in\mathbb{F}_p} \zeta^{hx^3} = \sum_{w\in\mathbb{F}_p} \zeta^{hw}(1 + \chi(w) + \chi^2(w)) = \sum_{w\in\mathbb{F}_p} \zeta^{hw} + \sum_{w\in\mathbb{F}_p} \chi(w)\zeta^{hw} + \sum_{w\in\mathbb{F}_p} \chi^2(w)\zeta^{hw}, \tag{6.4}$$

ove il primo addendo è nullo (cf. (II.6.1)) ed il secondo ed il terzo sono le somme di Gauss relative ai caratteri χ e $\chi^2 = \overline{\chi}$, rispettivamente.

Ci siamo quindi ricondotti al problema di stimare il valore delle somme di Gauss, ed infatti, si ha

6.5 Lemma. *Sia $\chi : \mathbb{F}_p^\times \to \mathbb{C}$ un carattere, esteso ad $\mathbb{F}_p$ ponendo $\chi(0) = 0$. Siano $\zeta \in \mathbb{C}$ una radice p-esima primitiva di 1, ed $h \in \mathbb{F}_p^\times$. Allora*

$$\left| \sum_{w\in\mathbb{F}_p} \chi(w)\zeta^{hw} \right| = \sqrt{p}.$$

dim. Infatti, si ha

$$\left|\sum_{w\in\mathbb{F}_p}\chi(w)\zeta^{hw}\right|^2 = \left(\sum_{w_1\in\mathbb{F}_p^\times}\chi(w_1)\zeta^{hw_1}\right)\left(\sum_{w_2\in\mathbb{F}_p^\times}\chi(w_2^{-1})\zeta^{-hw_2}\right) = \sum_{w_1,w_2\in\mathbb{F}_p^\times}\chi(w_1/w_2)\zeta^{h(w_1-w_2)}.$$

Posto quindi $y = w_1/w_2$, la somma si può scrivere nella forma

$$\sum_{y,w_2\in\mathbb{F}_p^\times}\chi(y)\zeta^{hw_2(y-1)} = \sum_{y\in\mathbb{F}_p^\times}\chi(y)\sum_{w_2\in\mathbb{F}_p^\times}\zeta^{hw_2(y-1)}$$

e si ha

$$\sum_{w_2\in\mathbb{F}_p^\times}\zeta^{hw_2(y-1)} = \begin{cases} -1 & \text{se } y\neq 1 \\ p-1 & \text{se } y=1 \end{cases}.$$

Possiamo quindi riassumere le osservazioni precedenti e scrivere

$$\left|\sum_{w\in\mathbb{F}_p}\chi(w)\zeta^{hw}\right|^2 = -\sum_{y\in\mathbb{F}_p\setminus\{0,1\}}\chi(y) + (p-1)\chi(1) = p - \sum_{y\in\mathbb{F}_p^\times}\chi(y).$$

Infine, ricordando che $p \equiv 1 \pmod 3$, si conclude che la somma a destra è nulla ed è così verificata la tesi. **CVD** □

Dunque, in base al lemma precedente ed a (II.6.4)), si ottiene, $|\sigma_h| \leq 2\sqrt{p}$ per ogni $h\neq 0$ e quindi, applicando questa disuguaglianza a (II.6.2)), si ottiene, per ogni primo p, la stima

$$|N_p - p^2| \leq 8(p-1)\sqrt{p}. \tag{6.6}$$

Per p sufficientemente grande, $8(p-1)\sqrt{p} < p^2$, e quindi questa stima permette di concludere che esistono punti in $\mathbb{F}_p$ per la cubica data.

Sommario del contenuto