ALGEBRA I — TEOREMI DI FATTORIZZAZIONE UNICA

1. La nozione di anello

Un anello è una struttura algebrica con due operazioni, che giocano il ruolo della somma e del prodotto tra numeri interi nell'insieme $\mathbb{Z}$.

Definizione 1.1. Un *anello* è un insieme A dotato di due operazioni $+$, detta *somma*, e $\cdot$, detta *prodotto* o *moltiplicazione*, dotate delle seguenti proprietà

- La somma $+$ costituisce una struttura di gruppo abeliano, la cui identità è indicata con 0;
- La moltiplicazione $\cdot$ è un'operazione associativa;
- la moltiplicazione è *distributiva* rispetto alla somma, cioè $a\cdot(b+c) = a\cdot b+a\cdot c$, $(a+b)\cdot c = a\cdot c+b\cdot c$, per ogni scelta di $a, b, c \in A$.

L'anello A si dice *commutativo* se la moltiplicazione è commutativa[1], *unitario* o *con unità* se ammette un elemento neutro 1 rispetto al prodotto; è un *dominio di integrità* se è commutativo con unità e $ab = 0$ implica $a = 0$ oppure $b = 0$, cioè se vale la legge di annullamento del prodotto. E' un *corpo* se è unitario ed ogni elemento $a \neq 0$ ammette un inverso moltiplicativo. E' un *campo* se è un corpo commutativo.

Osservazione: Se D è un dominio d'integrità, allora $da = db, d \neq 0$ implica $a = b$. Per convincersi di ciò, scriviamo $da - db = 0 \Rightarrow d(a - b) = 0$. Poiché D è un dominio, e $d \neq 0$, allora $a - b = 0$, da cui $a = b$. Utilizzeremo questo fatto più volte nel seguito.

1.1. **Esempi.**

— $\mathbb{Z}$ è ovviamente un anello, essendo il nostro modello per la definizione. $\mathbb{Z}$ è un anello commutativo con unità, ed è anche un dominio di integrità.

— Sia $A = \mathbb{Z}/(n), n > 0$ l'insieme delle classi di resto modulo n, con le ovvie operazioni di somma e prodotto. Allora A è un anello commutativo con unità. A è un dominio di integrità solo se n è un numero primo, nel qual caso è anche un campo.

— $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi, e sono quindi anelli commutativi con unità, nonché domini. Ogni campo è infatti ovviamente un dominio d'integrità.

— L'insieme $M_n(\mathbf{k})$ delle matrici n per n a coefficienti in un campo $\mathbf{k}$ è un anello rispetto alla somma e al prodotto righe per colonne di matrici. E' un anello non commutativo, se $n > 1$, ma possiede un'unità: è la matrice identità. Vale la pena di notare che non vale la legge di annullamento del prodotto, a meno che $n = 1$. Infatti

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

— Sia $\mathbb{H}$ l'insieme dei simboli $a + bi + cj + dk$, dove a, b, c, d sono numeri reali. Definiamo un'operazione di somma sommando i coefficienti di simboli corrispondenti:

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k.$$

Questa operazione fornisce chiaramente una struttura di gruppo abeliano su $\mathbb{H}$.

Definiamo ora un prodotto su $\mathbb{H}$ imponendo che $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, ed estendendo per distributività. Allora $\mathbb{H}$ è un anello non commutativo, con unità $1 = 1 + 0i + 0j + 0k$, e gli elementi di $\mathbb{H}$ si dicono *quaternioni*. $\mathbb{H}$ è un corpo, infatti ogni elemento $a + bi + cj + dk$ in cui a, b, c, d non sono tutti nulli ha un inverso $(a - bi - cj - dk)/(a^2 + b^2 + c^2 + d^2)$.

— Sia A un anello. Definiamo un nuovo anello $A[x]$ detto l'*anello dei polinomi nell'indeterminata x a coefficienti in A*, o più semplicemente *anello dei polinomi in A*. I suoi elementi sono simboli, detti polinomi, della forma $a_0 + a_1x + a_2x^2 + ... + a_nx^n$, dove i coefficienti $a_0, a_1, ..., a_n$ sono elementi di A. La somma tra polinomi è definita coefficiente per coefficiente, con la convenzione che il coefficiente di x^n sia 0 se non scritto. Quindi

$$(a_0 + a_1x + ...a_mx^m)+(b_0 + b_1x + ... + b_nx^n) = \\ (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n + a_{n+1}x^{n+1} + ... + a_mx^m,$$

Date: 29 marzo 2023.

[1]La somma lo è sempre...

se ad esempio $m > n$. Il prodotto si ottiene invece distribuendo rispetto alla somma il prodotto definito sui *monomi* da $(ax^\alpha) \cdot (bx^\beta) = abx^{\alpha+\beta}$.

$A[x]$ è un anello, che è commutativo se lo è anche A. Se A è un anello con unità, anche $A[x]$ ammette 1 come unità. Se A è un dominio d'integrità, anche $A[x]$ è un dominio d'integrità. L'anello A si immerge in $A[x]$ come sottoanello. Vedremo il significato di questa affermazione dopo aver introdotto il concetto di omomorfismo tra anelli.

— L'anello $A[x][y]$ si dice *anello dei polinomi nelle indeterminate x e y a coefficienti in A*, e si indica anche con $A[x, y]$. Si può ripetere la costruzione per definire $A[x_1, x_2, ...]$.

— Sia $A[[x]]$ l'insieme delle somme infinite $a_0+a_1x+a_2x^2+...$ dove $a_i \in A$, con le operazioni definite come nell'anello dei polinomi. In particolare il prodotto è definito come

$$(a_0 + a_1x+a_2x^2 + ...) \cdot (b_0 + b_1x + b_2x^2 + ...) =$$
$$a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + ...$$

Allora $A[[x]]$ è l'anello delle *serie formali* a coefficienti in A. $A[[x]]$ è un anello, commutativo se A è commutativo, unitario se A è unitario. L'anello dei polinomi $A[x]$ si immerge in $A[[x]]$ come l'insieme delle serie formali in cui solo un numero finito di coefficienti sono diversi da 0.

Proposizione 1.1.1. *Sia A un anello. Allora $a \cdot 0 = 0 \cdot a = 0, a(-b) = (-a)b = -ab, (-a)(-b) = ab$, per ogni $a, b \in A$. Se A è unitario, allora $(-1) \cdot a = a \cdot (-1) = -a, (-1)(-1) = 1$, per ogni $a \in A$.*

Dimostrazione. Mutuata dall'Herstein. □

Definizione 1.2. Sia A un anello. Un sottoinsieme $B \subset A$ si dice *sottoanello* se le operazioni di A inducono su B una struttura di anello. Un sottoinsieme $I \subset A$ si dice *ideale destro* (risp. *sinistro*) di A se ne è un sottogruppo additivo ed assorbe il prodotto a destra (sinistra) per elementi di A; in altre parole, se $a \in A$ e $i \in I$, allora$ia \in I$ ($ai \in I$). Si dice *ideale bilatero* (o *tout-court*, ideale) se è un ideale sia destro che sinistro.

In particolare ogni ideale destro o sinistro di A è un sottoanello di A: gli ideali sono particolari tipi di sottoanello. Vedremo più in là che sono esattamente i sottoanelli per i quali possiamo quozientare, ovvero i nuclei di omomorfismi.

1.2. **Esempi.**

— (0) e A sono sempre ideali di un anello A. Sono detti *ideali banali*.

— Se A è un anello, il sottoinsieme $Ax = \{ax | a \in A\}$ è un ideale sinistro di A, così come xA ne è un ideale destro. Se A è commutativo, allora $(x) = Ax = xA$ è un ideale di A, ed è detto *ideale principale* di A generato da x.

— Sottoanelli ed ideali di $\mathbb{Z}$ sono per definizione sottogruppi additivi. Abbiamo già visto che i sottogruppi additivi di $\mathbb{Z}$ sono tutti della forma (n) per qualche intero $n \geq 0$. E' facile notare che tutti questi sottogruppi sono in realtà ideali: infatti se un multiplo di n viene moltiplicato per un intero, otteniamo nuovamente un multiplo di n.

— Sia $A = \mathbb{Z}/(6)$. Allora i sottogruppi additivi di A sono $A, (\overline{0}), (\overline{2}), (\overline{3})$, e si verifica facilmente che sono tutti ideali di A.

— Gli unici ideali dei campi $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono banali, come accade in ogni corpo $\mathbf{k}$. Infatti ogni elemento non nullo α ammette un inverso α^{-1}, e quindi se $\alpha \in I$, anche $\alpha\alpha^{-1} = 1$ appartiene a I. Allora $a = a \cdot 1 \in I$ per ogni $a \in \mathbf{k}$. Un campo può ammettere sottoanelli che non siano ideali. Ad esempio $\mathbb{R}$ è un sottoanello di $\mathbb{C}$, ma non ne è un ideale. Invece, ogni sottoanello di $\mathbb{Z}/(p)$, con p primo, è anche un ideale.

— Se gli unici ideali di un anello commutativo con unità A sono banali, allora A è un campo. Sia infatti $\alpha \neq 0$ un elemento di A. Allora l'ideale (α), che contiene elementi diversi dallo 0, deve essere uguale a tutto A. Questo mostra che (α) contiene 1, e che quindi 1 è un multiplo di α. Allora $1 = \alpha\beta$ per qualche $\beta \in A$, ed α ammette un inverso β.

— Sia $A = M_2(\mathbf{k})$, dove $\mathbf{k}$ è un campo. Allora $C = \{M \in A | \text{la seconda colonna di } M \text{ è nulla}\}$ è un ideale sinistro, ma non destro, di A. Invece $R = \{M \in A | \text{la seconda riga di } M \text{ è nulla}\}$ è un ideale destro ma non sinistro di A.

— Sia $J_{x_0} \subset \mathbb{R}[x]$ l'insieme dei polinomi che si annullano in $x_0 \in \mathbb{R}$. Allora J_{x_0} è un ideale di $\mathbb{R}[x]$. Infatti da $p(x_0) = q(x_0) = 0$ segue $(p + q)(x_0) = p(x_0) + q(x_0) = 0$, e da $p(x_0) = 0$ segue $(ap)(x_0) = a(x_0)p(x_0) = 0$ per ogni $a \in \mathbb{R}$.

1.3. **Esercizi.**

(a) Mostrare che gli unici ideali bilateri di $M_2(\mathbf{k})$ sono banali.

(b) Determinare gli ideali di $\mathbb{R}[x]$. Sono tutti principali?

(c) Sia $A = \{a + b\varepsilon | a, b \in \mathbb{R}\}$, dove la somma è data da $(a + b\varepsilon) + (c + d\varepsilon) = (a + c) + (b + d)\varepsilon$, e il prodotto si ottiene distribuendo $\varepsilon^2 = 0$. Mostrare che $a + b\varepsilon$ è sempre invertibile se $a \neq 0$. E' vero che l'unico ideale non banale di A è (ε)?

**(d)* Sia $B = \{a + b\varepsilon | a, b \in \mathbb{Z}\}$, con le operazioni definite come sopra per A. Determinare gli ideali di B. Sono tutti principali?

(e) Sia $C = \{a + b\zeta, a, b \in \mathbb{Q}\}$, dove la somma è data da $(a + b\zeta) + (c + d\zeta) = (a + c) + (b + d)\zeta$, e il prodotto è ottenuto distribuendo $\zeta^2 = 1$. E' vero che C è un dominio di integrità?

(f) Come sopra, ma con $\zeta^2 = 2$.

(g) Sia A un anello in cui $x^2 = x$ per ogni $x \in A$. Allora A è commutativo.

(h) Sia A un anello con unità in cui $(xy)^2 = x^2y^2$. Mostrare allora che A è commutativo.

**(i)* Dare un esempio di anello non commutativo in cui $(xy)^2 = x^2y^2$.

**(j)* Determinare tutti i sottoanelli di $\mathbb{Q}$ che contengono 1.

***(k)* Determinare tutti i sottoanelli di $\mathbb{Q}$.

1.4. **La caratteristica di un dominio.** Indichiamo con $nd, n \in \mathbb{N}$, la somma di n volte d: ad esempio $2d = d + d$.

Lemma 1.4.1. *Sia D un dominio d'integrità, $0 \neq d$ un elemento di D tale che $nd = 0$ per qualche $n > 0$. Supponiamo che p sia il minimo intero positivo con questa proprietà. Allora p è un numero primo, e $px = 0$ per ogni $x \in D$.*

Dimostrazione. Supponiamo che p non sia primo. Allora possiamo scrivere $p = hk$ con $h, k < p$. In tal caso avremmo

$$0 = (pd)d = pd^2 = hkd^2 = (hd)(kd),$$

ma D è un dominio, e da $(hd)(kd) = 0$ segue che $hd = 0$ oppure $kd = 0$, contro la minimalità di D. Quindi p è un numero primo.

Sia ora x un qualsiasi elemento di D. Allora $pdx = (pd)x = 0$, e quindi $0 = pdx = d(px)$. Ma $d \neq 0$, e D è un dominio, quindi $px = 0$. □

Definizione 1.3. La caratteristica di un dominio di integrità D è il minimo intero positivo p, se esiste, tale che $p1 = 0$. Un dominio si dice di caratteristica finita se non ha caratteristica 0.

Per quanto detto sopra, la caratteristica di un dominio di caratteristica finita è sempre un numero primo.

Corollario 1.4.2. *Il numero di elementi in un dominio di integrità finito è una potenza di un numero primo.*

Dimostrazione. Un dominio finito D non può avere caratteristica 0, altrimenti gli elementi $nd, n \in \mathbb{N}$ sarebbero tutti distinti. Se guardiamo il dominio D come gruppo abeliano finito, allora, ogni elemento diverso dallo 0 ha ordine p uguale alla caratteristica di D. Questo comporta che l'ordine di D sia una potenza di p. □

Teorema 1.4.3. *Ogni dominio di integrità finito è un campo.*

Dimostrazione. Mostriamo che ogni elemento non nullo di D ammette un inverso. Se $0 \neq a \in D$, consideriamo l'applicazione $m_a : D \to D$ definita da $m_a(x) = ax$. Poiché D è un dominio d'integrità, e $a \neq 0$, allora m_a è iniettiva. Un'applicazione iniettiva tra insiemi finiti della stessa cardinalità è anche suriettiva, ed esiste quindi $x \in D$ tale che $m_a(x) = 1$. Ma allora $ax = xa = 1$, e quindi x è l'inverso di a. □

Daremo più in là una classificazione di tutti i campi finiti, e mostreremo che per ogni numero della forma p^n, p primo, esiste un solo campo di ordine p^n a meno di isomorfismo.

1.5. **Operazioni tra ideali.** E' comodo definire alcune operazioni tra gli ideali di un anello.

Proposizione 1.5.1. *Sia A un anello, e I, J ideali di A. Allora i seguenti sottoinsiemi di A:*

— $I \cap J$;
— $I + J = \{i + j | i \in I, j \in J\}$;
— $I \cdot J = \{i_1j_1 + i_2j_2 + \ldots + i_kj_k | i_n \in I, j_n \in I \text{ per } 1 \leq n \leq k\}$

sono ideali di A.

Dimostrazione. Per esercizio. □

Esempio: Siano $a, b \in \mathbb{Z}$, $I = (a), J = (b)$. Allora $I \cap J$ è l'ideale i cui elementi sono sia multipli di a che di b. Il suo minimo elemento positivo è il minimo comune multiplo m tra a e b. Dal momento che tutti gli ideali di $\mathbb{Z}$ sono principali, avremo $(a) \cap (b) = (m)$.

L'ideale $I + J$ è un ideale che contiene sia a che b. Se $I + J = (d)$, allora sia a che b sono multipli di d. Abbiamo visto, quando abbiamo considerato la somma di sottogruppi, che d è il massimo comun

divisore tra a e b. In altre parole $(a)+(b)$ è l'ideale principale generato dal massimo comun divisore tra a e b.

L'ideale $I \cdot J$ è quello i cui elementi sono le somme finite di prodotti di multipli di a con multipli di b, ed è pertanto generato da ab.

Sarà utile in seguito adottare una notazione: l'ideale $(a_1)+(a_2)+...+(a_n)$ sarà indicato con $(a_1, a_2, ..., a_n)$. Esso è il più piccolo ideale contenente gli elementi $a_1, ..., a_n$. Secondo questa convenzione, nell'anello $\mathbb{Z}$ l'ideale (a, b) è l'ideale principale generato dal massimo comun divisore $\mathrm{MCD}(a, b)$.

1.6. **Un esempio di ideale non principale.** Consideriamo l'ideale $(x, 3)$ nell'anello $\mathbb{Z}[x]$. Abbiamo mostrato a lezione che non è un ideale principale. Ripercorro brevemente la dimostrazione.

Proposizione 1.6.1. *L'ideale $(x, 3)$ nell'anello $\mathbb{Z}[x]$ non è principale.*

Dimostrazione. Se $I = (x, 3)$ fosse un ideale principale, allora esisterebbe un polinomio $p(x)$ con la proprietà che gli elementi di I siano tutti e soli i multipli di $p(x)$.

Se così fosse, sia x che 3 dovrebbero essere multipli di $p(x)$. Ma se 3 è un multiplo di $p(x)$, allora $p(x)$ è un polinomio costante, e se x è un multiplo di una costante, questa costante deve essere 1. Allora l'ideale $(x, 3)$ sarebbe generato da 1, e coinciderebbe quindi con l'intero anello $\mathbb{Z}[x]$. Ma 1 non si può scrivere come somma di un multiplo di x e di un multiplo di 3, da cui un assurdo. □

1.7. **Esercizi.**

(a) Mostrate che $(x, y) \in \mathbb{R}[x, y]$ non è un ideale principale.
(b) Mostrate che $(x, 3) \in \mathbb{R}[x, y]$ è un ideale principale.
(c) E' vero che $(x, y) = (x) \cap (y)$ in $\mathbb{R}[x]$? E che $(x) \cap (y) = (x) \cdot (y)$?
(d) Mostrate che comunque presi due ideali I, J in un anello A, si ha $IJ \subset I \cap J \subset I + J$.

2. Omomorfismi tra anelli.

Definizione 2.1. Siano $A, \bar{A}$ anelli. Un'applicazione $\phi : A \to \bar{A}$ è un omomorfismo se $\phi(a+b) = \phi(a)+\phi(b)$ e $\phi(ab) = \phi(a)\phi(b)$ per ogni scelta di $a, b \in A$.

Siano $\mathrm{Im}\phi = \{x \in \bar{A} |$ esiste $a \in A$ tale che $\phi(a) = x\}$ l'immagine dell'omomorfismo ϕ e $\ker \phi = \{a \in A | \phi(a) = 0\}$ il suo nucleo. Come nei gruppi, vale la seguente

Proposizione 2.0.1. *Se $\phi : A \to \bar{A}$ è un omomorfismo di anelli, allora il nucleo e l'immagine di ϕ sono sottoanelli di A e $\bar{A}$ rispettivamente. Il nucleo, inoltre, è un ideale di A, e ϕ è iniettiva se e solo se $\ker \phi = (0)$.*

Dimostrazione. Le dimostrazioni sono immediate. □

Abbiamo visto che il nucleo di un omomorfismo è un ideale. Gli ideali di un anello giocano il ruolo giocato dai sottogruppi normali in teoria dei gruppi. In particolare, un sottoinsieme di un anello è un ideale se e solo se è il nucleo di qualche omomorfismo. Per mostrare questo, definiamo il concetto di anello quoziente.

Proposizione 2.0.2. *Sia I un ideale dell'anello A, e sia A/I l'insieme delle classi laterali $[a] = a + I$ di I in A. Allora le operazioni*

$$[a] + [b] = [a + b], \qquad [a] \cdot [b] = [ab]$$

sono ben definite, e costituiscono una struttura di anello su A/I.

Dimostrazione. Bisogna mostrare che le operazioni non dipendono dalla scelta dei rappresentanti. Ad esempio, per quanto riguarda il prodotto, se $a \equiv a', b \equiv b' \mod I$, allora $a' = a + i, b' = b + j$ con $i, j \in I$. Ma allora $(a + i)(b + j) = ab + (aj + ib + ij)$; dal momento che aj, ib e ij appartengono tutti a I, allora $(a + i)(b + j) \equiv ab \mod I$. Per la somma, la dimostrazione è analoga. □

L'anello A/I si chiama *anello quoziente* di A per l'ideale I. Vi è un ovvio omomorfismo $\pi : A \to A/I$ che manda $a \in A$ nella classe laterale $[a] = a + I$. Il nucleo dell'omomorfismo π coincide con l'ideale I. La seguente proposizione è centrale per i nostri interessi.

Proposizione 2.0.3. *Vi è una corrispondenza biunivoca tra l'insieme degli ideali di A che contengono I e l'insieme degli ideali di A/I.*

Dimostrazione. Dato un ideale J di A che contiene I, la sua immagine $\pi(J)$ attraverso π è un ideale di A/I. Alla stessa maniera, se $\bar{J}$ è un ideale di A/I, la sua controimmagine $\pi^{-1}(\bar{J})$ è un ideale di A, che contiene il nucleo di π, e quindi I. Il mio scopo è quello di mostrare che le applicazioni

$$J \mapsto \pi(J) \qquad \bar{J} \mapsto \pi^{-1}(\bar{J})$$

sono una inversa dell'altra. Per mostrarlo, farò vedere che $\pi^{-1}\pi(J) = J$ quando J è un ideale di A che contiene I, e che $\pi\pi^{-1}(\bar{J}) = \bar{J}$ se $\bar{J}$ è un ideale di A/I.

Per verificare che la prima asserzione è vera, osserviamo che $\pi^{-1}\pi(J) = \{a \in A | \pi(a) \in \pi(J)\}$. Ora, se $\pi(a) \in \pi(J)$, allora esiste $j \in J$ tale che $\pi(a) = \pi(j)$. Questo vuol dire che $\pi(a - j) = 0$ e che quindi $a - j \in I$. Allora a è somma di un elemento di J e di un elemento di I. Poiché $I \subset J$, allora a giace in J. Questo mostra che $\pi^{-1}\pi(J)$ è contenuto in J. L'altra disuguaglianza $J \subset \pi^{-1}\pi(J)$ è ovvia.

La seconda asserzione è immediata. Infatti $\pi^{-1}(\bar{J}) = \{a \in A | \pi(a) \in \bar{J}\}$. Ma allora $\pi\pi^{-1}(\bar{J})$ è composto dalle immagini $\pi(a)$ di elementi la cui immagine $\pi(a)$ giace in $\bar{J}$ per definizione. □

Abbiamo sfruttato questa corrispondenza a lezione per dare una caratterizzazione di ideali primi e massimali. Prima qualche definizione.

Definizione 2.2. Un ideale I dell'anello A si dice *primo* se $ab \in I$ implica $a \in I$ oppure $b \in I$. Si dice *massimale* quando non vi sono ideali $I \subset J \subset A$ propriamente contenuti tra I e A.

Proposizione 2.0.4. *Sia A un anello commutativo con unità. Un ideale I di A è primo se e solo se A/I è un dominio di integrità. E' massimale se e solo se A/I è un campo.*

Dimostrazione. I primo se e solo se A/I è un dominio di integrità segue immediatamente dalla definizione di ideale primo. La seconda proposizione è più interessante. La corrispondenza biunivoca appena descritta tra gli ideali di A/I e quelli di A che contengono I mostra che se gli unici ideali di A/I sono quelli banali, allora gli unici ideali di A che contengono I sono I ed A stesso. Allo stesso modo, se I è massimale, e non vi sono ideali di A strettamente contenuti tra I ed A, allora gli unici ideali di A/I sono $\pi(I) = (0)$ e $\pi(A) = A/I$. Quindi A/I ha solo ideali banali se e solo se I è un ideale massimale. Ma un anello commutativo con unità in cui gli unici ideali sono quelli banali è un campo, come abbiamo già visto. □

3. Campo delle frazioni. Equazioni polinomiali su di un campo.

Qui di seguito mostrerò che il numero di soluzioni di un'equazione polinomiale a coefficienti in un dominio di integrità è limitato dal grado del polinomio.

Ho bisogno di due preliminari, che descrivo qui di seguito:

Lemma 3.0.1. *Dati due polinomi $a(x), b(x) \in F[x]$ a coefficienti nel campo F, con $b(x) \not\equiv 0$, sono univocamente determinati due polinomi $q(x)$ detto quoziente e $r(x)$ detto resto con la proprietà che $a(x) = b(x)q(x) + r(x)$ e che $r(x)$ abbia grado inferiore a quello di $b(x)$.*

Dimostrazione. Basta eseguire l'algoritmo di divisione tra polinomi. □

Lemma 3.0.2. *Sia A un anello commutativo, a un elemento di A. Allora l'applicazione $A[x] \mapsto A$ che manda il polinomio $p(x)$ nel valore $p(a)$ assunto da p in a è un omomorfismo di anelli.*

Dimostrazione. L'unica verifica non ovvia è che $p(x)q(x)$, calcolato in a, valga esattamente $p(a)q(a)$. Questo è evidente, in quanto il prodotto delle espressioni

$$(p_0 + p_1x + p_2x^2 + ...p_nx^n)(q_0 + q_1x + ...q_mx^m)$$

e

$$(p_0 + p_1a + p_2a^2 + ...p_na^n)(q_0 + q_1a + ...q_ma^m)$$

si calcola alla stessa maniera. Si noti che la commutatività di A è usata in maniera essenziale. Infatti il prodotto dei polinomi $p_ix^i \cdot q_jx^j$ è definito come $p_iq_jx^{i+j}$ mentre il prodotto $p_ia^i \cdot q_ja^j$ è uguale a $p_iq_ja^{i+j}$ solo se q_j commuta con a^i. □

Proposizione 3.0.3. *Sia $0 \neq p(x) \in F[x]$ un polinomio a coefficienti in un campo F. Allora il numero delle soluzioni in F dell'equazione polinomiale $p(x) = 0$ è minore o uguale al grado di $p(x)$.*

Dimostrazione. Se $p(x) = 0$ non ha soluzioni in F, allora il teorema è vero a vuoto. Se invece $p(\alpha) = 0$ per qualche $\alpha \in F$, effettuiamo la divisione con resto di $p(x)$ per $x - \alpha$. Otterremo che

$$p(x) = (x - \alpha)q(x) + r(x), \tag{1}$$

dove il resto $r(x)$ è un polinomio di grado inferiore a $x - \alpha$, e quindi una costante $r(x) \equiv r$. Per calcolare questa costante, sostituiamo $x = \alpha$ in (1), e otteniamo $p(\alpha) = 0 \cdot q(\alpha) + r$. Poiché $p(\alpha) = 0$, avremo $r = 0$. Osserviamo che scrivendo $(x - \alpha)q(x)|_{x=\alpha} = (\alpha - \alpha)q(\alpha) = 0$ abbiamo utilizzato il Lemma 3.0.2.

Allora $p(x) = (x-\alpha)q(x)$, e risolvere $p(x) = 0$ equivale a risolvere $x-\alpha = 0$ e $q(x) = 0$. A questo punto l'enunciato segue per induzione. Supponiamo che il grado di $p(x)$ sia $n + 1$ e che l'enunciato sia vero per polinomi di grado n. Allora $q(x) = 0$ ha al più n soluzioni, in quanto il grado di q è n. Le soluzioni di $p(x)$ sono quelle di $q(x) = 0$ insieme ad α, quindi al più $n + 1$. La base induttiva è ovvia, in quanto un polinomio non nullo di grado 0 non ha soluzioni. □

Si noti che un analogo enunciato non vale se F non è commutativo. Ad esempio nel corpo $\mathbb{H}$ dei quaternioni, l'equazione polinomiale $x^2 + 1 = 0$ ha almeno le sei soluzioni $x = \pm i, \pm j, \pm k$. Una più attenta analisi mostra che essa ammette infinite soluzioni.

Il risultato della Proposizione 3.0.3 si può estendere al caso di un dominio di integrità. Abbiamo bisogno di un po' di prerequisiti prima di riuscire a mostrarlo.

Lemma 3.0.4. *Sia D un dominio di integrità, e X l'insieme delle coppie $(a, b), a, b \in D, b \neq 0$. La relazione $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ è di equivalenza.*

Dimostrazione. La riflessività e la simmetria sono ovvie. Per quanto riguarda la transitività, dobbiamo mostrare che se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$ allora $(a, b) \sim (e, f)$ cioè che se $ad = bc$ e $cf = de$ allora $af = be$. Per mostrare questo, si sfrutta il fatto che D sia un dominio. Infatti, da $ad = bc, cf = de$ segue $adf = (ad)f = (bc)f = b(cf) = bde$. Ma se in un dominio $d(af) = d(be)$ allora cancellando d si ottiene $af = de$. □

Indichiamo con F l'insieme quoziente $D/\sim$, cioè l'insieme delle classi di equivalenza rispetto a $\sim$. Indicheremo la classe di equivalenza di (a, b) con il simbolo a/b. In effetti il nostro scopo sarà quello di definire operazioni di somma e prodotto sull'insieme F che trattino la classe di equivalenza dell'elemento (a, b) come se fosse il risultato di una ipotetica divisione – che in D non è sempre possibile – tra a e b.

Definiamo quindi la somma e il prodotto di frazioni. Con un po' di buon senso, facciamo in modo che

$$a/b + c/d = (ad + bc)/bd \qquad a/b \cdot c/d = ac/bd.$$

Proposizione 3.0.5. *La somma ed il prodotto di elementi di F sono ben definiti, e danno su F una struttura di campo.*

Dimostrazione. Dobbiamo innanzitutto mostrare che il risultato delle operazioni è indipendente dalla scelta dei rappresentanti nelle classi di equivalenza. In altre parole, che se

$$(A, B) \sim (a, b) \qquad (C, D) \sim (c, d),$$

allora anche

$$(AD + BC, BD) \sim (ad + bc, bd) \qquad (AC, BD) \sim (ac, bd).$$

Questo è più o meno immediato: infatti da

$$Ab = aB \qquad Cd = cD$$

seguono da una parte

$$AbDd = aBDd \qquad BbCd = BbcD,$$

e quindi

$$(AD + BC)bd = AbDd + BbCd = aBDd + BbcD = (ad + bc)BD;$$

e dall'altra

$$Ab \cdot Cd = aB \cdot cD.$$

Pertanto le operazioni di somma e prodotto tra frazioni sono ben definite. La commutatività e l'associatività di entrambe le operazioni seguono da una semplice verifica, così come la distributività del prodotto rispetto alla somma. L'elemento neutro rispetto alla somma è $0/a$, mentre l'inverso additivo di a/b è chiaramente $(-a)/b$. L'unità moltiplicativa è a/a, e l'inverso moltiplicativo di $a/b, a \neq 0$ è b/a. □

Questa costruzione è analoga alla costruzione del campo $\mathbb{Q}$ dei numeri razionali a partire dal dominio $\mathbb{Z}$ degli interi, ed è un caso particolare di un procedimento detto di *localizzazione* di un anello, nel quale si invertono artificialmente alcuni elementi imponendoli come denominatori. Un esercizio istruttivo a proposito è il numero 3.6.5 dell'Herstein.

Teorema 3.0.6. *Ogni dominio di integrità D si immerge in un campo. Esiste cioè un omomorfismo iniettivo $\iota : D \to F$, dove F è un campo.*

Dimostrazione. Sia F il campo delle frazioni del dominio D. L'applicazione $\iota : D \to F$ come $\iota(d) = d/1$ è chiaramente un omomorfismo (verificatelo!). Inoltre ι è iniettiva; infatti $d/1 = 0/1$ — e cioè $(d, 1) \sim (0, 1)$ — esattamente quando $d \cdot 1 = 1 \cdot 0$ cioè quando $d = 0$. Pertanto il nucleo di ι consiste del solo elemento 0, e ι è iniettivo. □

Il campo F delle frazioni di D non è l'unico campo che contiene al suo interno una copia di D, ma ha la proprietà di essere il più piccolo: se $D \to F'$ è una immersione di D in un campo F', allora l'immagine di tale immersione deve essere isomorfa a F.

Proposizione 3.0.7. *Sia $0 \neq p(x) \in D[x]$ un polinomio a coefficienti in un dominio di integrità D. Allora il numero delle soluzioni in D dell'equazione polinomiale $p(x) = 0$ è minore o uguale al grado di $p(x)$.*

Dimostrazione. Sia F il campo delle frazioni di D. Allora $p(x)$ si può vedere anche come polinomio a coefficienti in F, tramite l'immersione ι. Ma allora il numero delle soluzioni in F dell'equazione $p(x) = 0$ è limitato dal grado di p. Le soluzioni in D sono un sottoinsieme di queste, da cui l'enunciato. □

L'ipotesi che D sia un dominio di integrità è anch'essa essenziale. Il polinomio $x^3 - x$ ha infatti 6 soluzioni nell'anello $\mathbb{Z}/(6)$.

4. Divisibilità in domini a ideali principali

4.1. **Ideali e divisibilità.** Il nostro obiettivo è quello di preparare il terreno prima di affrontare la dimostrazione del Teorema di fattorizzazione unica in domini a ideali principali. Il primo passo è quello di tradurre i principali concetti che girano intorno alla nozione di divisibilità nel linguaggio degli ideali. Iniziamo dalla definizione degli oggetti algebrici ai quali siamo interessati.

Definizione 4.1. Un anello commutativo con unità si dice *dominio d'integrità* se il prodotto di suoi elementi non nulli è ancora non nullo. Un dominio d'integrità D è un *dominio a ideali principali* se ogni suo ideale è della forma (d) per qualche $d \in D$.

In un dominio d'integrità, se $0 \neq a$, da $ax = ay$ segue $x = y$. Ricordiamo anche che $(d) = \{dh \,|\, h \in D\}$ è sempre un ideale, se D è un anello commutativo, e che $d \in (d)$ se D possiede un elemento unità. Dal momento che gli elementi di (d) sono tutti e soli i multipli di d, possiamo riformulare la nozione di divisibilità in termini di ideali.

Lemma 4.1.1. *Sia D un dominio d'integrità, I un suo ideale, $a, b \in D$. Allora:*

1. *$a \in I$ se e solo se $(a) \subset I$.*
2. *a divide $b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subset (a)$.*
3. *$(a) = (b)$ se e solo se a e b sono associati; se si ottengono, cioè, l'uno dall'altro tramite moltiplicazione per un elemento invertibile.*
4. *$(a) = D$ se e solo se a è invertibile. In particolare, ogni elemento che divide un elemento invertibile è anch'esso invertibile.*

Dimostrazione.

1. Se un ideale contiene un elemento, contiene anche tutti i suoi multipli.
2. Dire che a divide b è equivalente a dire che b è un multiplo di a, cioè che $b \in (a)$. La seconda equivalenza segue dal punto precedente.
3. Se a e b sono associati, ciascuno è multiplo dell'altro, e quindi $(a) \subset (b), (b) \subset (a)$ valgono entrambe. Viceversa, se $(a) = (b)$, allora $b = ax, a = by$ per un'opportuna scelta di x, y, e quindi $a = axy$. Se $a \neq 0$, concludiamo che $xy = 1$, e quindi che x, y sono entrambi invertibili; se invece $a = 0$, allora anche $b = 0$. In entrambi i casi, a e b sono associati.
4. $D = (1)$, ed un elemento è associato ad 1 se e solo se è invertibile. Se a divide u invertibile, allora $D = (u) \subset (a)$, da cui $(a) = D$.

□

Osservazione 4.1.2. Si osservi che se in un dominio d'integrità $0 \neq b = ax$, con x non invertibile, allora a e b non possono essere associati. In particolare, $(b) \subsetneq (a)$.

4.2. **Massimo comun divisore.** Dal momento che la divisibilità si esprime attraverso l'inclusione di ideali, non è una sorpresa che questo sia possibile anche per il concetto di massimo comun divisore.

Definizione 4.2. Sia D un dominio d'integrità, $a, b \in D$. Si dice che $d \in D$ è un *massimo comun divisore* di a e b, e si scrive $d = \mathrm{MCD}(a, b)$, se:

- d divide sia a che b.
- se $e \in D$ divide sia a che b, allora e divide anche d.

Questa definizione ha il difetto di non garantire né l'esistenza, né l'unicità del massimo comun divisore di due elementi dati.

Proposizione 4.2.1. *In un dominio d'integrità D, $d = \mathrm{MCD}(a, b)$ se e solo se (d) è il minimo ideale principale che contiene $(a) + (b)$.*

Dimostrazione. Si tratta di una semplice riformulazione della definizione. Dire che d divida sia a che b è equivalente a dire che $(a), (b)$ sono sottoinsiemi di (d) o, in altri termini, $(a) + (b) \subset (d)$.

Pertanto, $d = \mathrm{MCD}(a, b)$ se $(a) + (b) \subset (d)$ e da $(a) + (b) \subset (e)$ segue $(d) \subset (e)$. In altre parole, (d) contiene $(a) + (b)$, ed è contenuto in ogni (e) che contiene $(a) + (b)$. □

Corollario 4.2.2. *Sia D è un dominio a ideali principali, $a, b \in D$. Allora d è un massimo comun divisore di a e b se e solo se $(a) + (b) = (d)$. In particolare, a e b possiedono sempre almeno un massimo comun divisore; inoltre, se $d = \mathrm{MCD}(a, b)$, allora $d' = \mathrm{MCD}(a, b)$ se e solo se d e d' sono associati.*

Dimostrazione. Applichiamo la Proposizione precedente. Poiché in D ogni ideale è principale, d è un massimo comun divisore di a e b se e solo se (d) è il minimo ideale che contiene $(a) + (b)$. Ad ogni modo, $(a) + (b)$ è un ideale, e quindi $d = \mathrm{MCD}(a, b)$ se e solo se $(a) + (b) = (d)$.

L'esistenza del massimo comun divisore di a e b segue dal fatto che l'ideale $(a) + (b)$ è principale, e l'ultima affermazione dal Lemma 4.1.1. □

4.3. **Elementi primi ed irriducibili.** Abbiamo già visto come, nell'anello $\mathbb{Z}$ degli interi, le nozioni di primalità e irriducibilità coincidano. Questo è vero in qualsiasi dominio a ideali principali.

Definizione 4.3. Un elemento non invertibile $p \neq 0$ si dice

- *primo* se $p \mid ab \Rightarrow p \mid a$ oppure $p \mid b$.
- *irriducibile* se, in ogni fattorizzazione $p = ab$, uno tra a e b è invertibile.

Lemma 4.3.1. *Sia D un dominio d'integrità e $0 \neq p \in D$ un elemento non invertibile. Allora p è primo se e solo se (p) è un ideale primo.*

Dimostrazione. Immediato. □

Lemma 4.3.2. *Sia D un dominio a ideali principali e $0 \neq p \in D$ un elemento non invertibile. Allora p è irriducibile se e solo se (p) è un ideale massimale.*

Dimostrazione. Un elemento p è irriducibile se non è invertibile e gli unici suoi divisori sono invertibili o associati a p. In altri termini, $p \in D$ è irriducibile se $(p) \neq D$ e $(p) \subset (d) \Rightarrow (d) = D$ oppure $(d) = (p)$. Dal momento che gli ideali di D sono tutti principali, questo è equivalente a richiedere la massimalità di (p). □

Osservazione 4.3.3. L'argomento appena visto mostra che un elemento non invertibile $p \neq 0$ in un dominio d'integrità è irriducibile esattamente quando (p) è un ideale *massimale tra gli ideali principali*. Questo non vuol dire, in generale, che (p) sia un ideale massimale, a meno che non sappiamo che tutti gli ideali siano principali.

Per la cronaca, un dominio d'integrità in cui tutti gli ideali massimali siano principali è necessariamente un dominio a ideali principali.

Corollario 4.3.4. *Sia D un dominio a ideali principali, $p \in D$ irriducibile, $a \in D$. Allora*

$$\mathrm{MCD}(a, p) = \begin{cases} 1 & \text{se } p \text{ non divide } a \\ p & \text{se } p \text{ divide } a. \end{cases}$$

Dimostrazione. Se p divide a, allora $(a) \subset (p)$ e quindi $(a) + (p) = (p)$. Se invece p non divide a, allora $a \notin (p)$; ma allora $(a) + (p)$ contiene propriamente (p), che è massimale. Quindi $(a) + (p) = D = (1)$. □

Proposizione 4.3.5. *In un dominio a ideali principali, un elemento è primo se e solo se è irriducibile.*

Dimostrazione. Dobbiamo mostrare che un ideale non banale (p) è primo se e solo se è massimale. Dal momento che ogni ideale massimale è primo, è sufficiente far vedere che ogni elemento primo è anche irriducibile.

Questo è facile: se p è primo, sia $p = ab$ una sua fattorizzazione. Per la primalità, p deve dividere uno dei fattori. Se p divide ad esempio a, allora $a = px$ e quindi $p = pxb$, da cui $bx = 1$, e b deve essere invertibile. □

Lemma 4.3.6. *Se $p \mid q$ sono elementi primi di un dominio a ideali principali, allora sono necessariamente associati.*

Dimostrazione. Si ha $(q) \subset (p) \neq (1)$. Ma (q) è massimale, quindi $(q) = (p)$. □

4.4. **Noetherianità.** Vogliamo adesso dimostrare che ogni elemento non invertibile di un dominio a ideali principali possiede almeno un divisore primo. La dimostrazione per induzione data nel caso degli interi è però inaccessibile, perché sfruttava in maniera essenziale il buon ordinamento di $\mathbb{N}$, mentre in un dominio a ideali principali non abbiamo chiare relazioni d'ordine. La tecnica con cui sostituire quella induttiva è la cosiddetta *condizione della catena ascendente*.

Lemma 4.4.1. *Sia $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ una famiglia infinita di ideali di D contenuti l'uno nel successivo. Allora esiste N tale che $I_m = I_N$ se $m \geq N$.*

Dimostrazione. Sia $I = \bigcup_{n\in\mathbb{N}} I_n$. Si vede facilmente che I è un ideale di D. Essendo D un dominio ad ideali principali, I è generato da un elemento a. Ma se $a \in \bigcup_{n\in\mathbb{N}} I_n$, dovrà appartenere ad almeno uno degli I_n. Diciamo che $a \in I_N$. Se $m \geq N$, allora $a \in I_N \subset I_m$, e quindi $a \in I_m$. Ma allora $(a) \subset I_m$. Poiché $I = (a)$ contiene tutti gli ideali I_n, avremo $(a) \supset I_m$, da cui $I_m = (a) = I_N$. □

Abbiamo dimostrato che *ogni catena ascendente di ideali* del dominio D si stabilizza: gli anelli per i quali le catene ascendenti di ideali si stabilizzano sono detti anelli noetheriani. Si può mostrare che gli anelli noetheriani sono quelli in cui tutti gli ideali sono finitamente generati, cioè possono essere generati da un numero finito di elementi. Chiaramente un ideale principale può essere generato da un solo elemento, e quindi ogni dominio ad ideali principali è un dominio noetheriano. E' importante notare che in generale si possono costruire catene discendenti infinite di ideali in un dominio ad ideali principali. Ad esempio

$$(1) \supset (2) \supset (4) \supset (8) \supset (16) \supset ... \supset (2^n) \supset ...$$

è una catena discendente infinita di ideali di $\mathbb{Z}$.

Proposizione 4.4.2. *Sia D un dominio a ideali principali, $a \neq 0$ un suo elemento non invertibile. Allora a possiede almeno un divisore irriducibile.*

Dimostrazione. Supponiamo per assurdo che a non possieda divisori irriducibili; in particolare a stesso non è irriducibile. Poniamo $a_0 = a$, e costruiamo una successione di elementi di D scegliendo a_{n+1} non invertibile, in modo che valga $a_n = a_{n+1}b_{n+1}$ con b_{n+1} anch'esso non invertibile. Questo è sempre possibile, in quanto ciascun a_n è, per costruzione, un divisore di a; essendo per ipotesi non irriducibile, deve possedere almeno una fattorizzazione non banale. Poiché a_{n+1} divide a_n, si ha $(a_n) \subset (a_{n+1})$. Tale inclusione è inoltre stretta, poiché altrimenti b_{n+1} sarebbe invertibile.

Gli ideali generati dagli elementi a_n costituiscono quindi una catena infinita strettamente crescente di ideali

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq (a_{n+1}) \subsetneq \dots$$

che non può esistere per il Lemma 4.4.1. □

Teorema 4.4.3 (di fattorizzazione unica)**.** *Sia D un dominio a ideali principali. Allora ogni elemento $0 \neq a \in D$ si può esprimere come prodotto*

$$a = up_1 \dots p_r,$$

dove u è invertibile, e gli elementi p_i sono tutti primi. Tale espressione è inoltre essenzialmente unica, nel senso che se

$$up_1 \dots p_r = vq_1 \dots q_s,$$

con u, v invertibili e p_i, q_j primi, allora $r = s$ e, a meno di riordinare i q_j, gli elementi p_i e q_i sono associati per ogni $1 \leq i \leq r$.

Dimostrazione. Dimostriamo innanzitutto l'esistenza della fattorizzazione. Se a è invertibile, è sufficiente prendere $u = a$ e $r = 0$, e l'affermazione è quindi ovvia.

Se a non è invertibile, possiede allora almeno un divisore primo grazie alla Proposizione 4.4.2. Costruiamo quindi una successione di elementi di D ponendo $a_0 = a$, e scegliendo a_{n+1} in modo che p_{n+1} sia un divisore primo di a_n, e valga $a_n = a_{n+1}p_{n+1}$. Se a_N è invertibile per qualche N, allora $a = a_N p_1 p_2 \dots p_N$ è la fattorizzazione cercata. Se nessuno tra gli a_n è invertibile, abbiamo costruito una successione strettamente crescente di ideali

$$(a_0) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq (a_{n+1}) \subsetneq \dots$$

che non può esistere per il Lemma 4.4.1.

L'unicità della fattorizzazione è facile da dimostrare per induzione su r. Quando $r = 0$, abbiamo $u = vq_1 \dots q_s$ e quindi ciascun q_i divide l'elemento invertibile u. Poiché nessun primo divide un elemento invertibile, deve essere $s = 0$, cioè non ci sono fattori primi neanche a secondo membro.

Dimostriamo allora il passo induttivo. Se $r > 0$, da

$$up_1 \dots p_r = vq_1 \dots q_s,$$

si deduce che p_1 divide almeno uno dei fattori a secondo membro, e sicuramente non v, che è invertibile. A meno di riordinare i q_j, possiamo supporre che p_1 divida q_1: essendo tali elementi entrambi primi, il Lemma 4.3.6 ci garantisce che p_1 e q_1 sono associati. Se $q_1 = p_1 w$, con w invertibile, possiamo sostituire ed ottenere

$$p_1 \cdot up_2 \dots p_r = p_1 \cdot (vw)q_2 \dots q_s.$$

Dal momento che D è un dominio d'integrità, possiamo cancellare p_1:

$$up_2 \dots p_r = (vw)q_2 \dots q_s.$$

Possiamo adesso applicare l'ipotesi induttiva — il numero dei fattori primi a primo membro è $r-1<r$ — e dedurre che $r-1=s-1$ e che, a meno di riordinare nuovamente i q_j, gli elementi p_i e q_i sono associati per ogni $2\leq i\leq r$. □

5. DOMINI EUCLIDEI

Abbiamo esteso la dimostrazione del teorema di fattorizzazione unica, già vista per l'anello $\mathbb{Z}$ degli interi, al caso dei domini di integrità i cui ideali siano tutti principali. Dimostrare che un dominio è ad ideali principali è però generalmente cosa ardua. Vi è tuttavia una classe di anelli in cui tale dimostrazione può essere adattata da quella già data per $\mathbb{Z}$ durante questo corso. Sono gli anelli che possiedono una divisione euclidea, che vengono per questo chiamati *domini euclidei*.

I tre esempi fondamentali di dominio euclideo che vedremo in questo corso sono $\mathbb{Z}$, che già conosciamo; l'anello $\mathbf{k}[x]$ dei polinomi a coefficienti in un campo $\mathbf{k}$, che ci sarà utile quando studieremo le estensioni di campi; e l'anello $\mathbb{Z}[i]$ degli interi di Gauss, grazie al quale dimostreremo un classico teorema di teoria dei numeri: il teorema dei due quadrati. Ricordiamo che, per noi, ogni dominio di integrità è sempre un anello commutativo con unità.

Definizione 5.1. Un *dominio euclideo* è un dominio di integrità D dotato di una *norma euclidea*[2], cioè di una applicazione $d: D\setminus\{0\}\to\mathbb{N}$ con le seguenti proprietà:

— $d(a)\leq d(ab)$ per ogni $a,b\neq 0$;
— per ogni $a\in D$ e $0\neq b\in D$ si possono scegliere $q,r\in D$ tali che $a=bq+r$, con $r=0$ oppure $d(r)<d(b)$.

5.1. **Esempi.**

— $d(x)=|x|$ è una norma euclidea sull'anello $\mathbb{Z}$.
— Se $0\neq p\in\mathbf{k}[x]$ è un polinomio a coefficienti in un campo $\mathbf{k}$, definiamo $d(p(x))$ come il grado di p. Allora chiaramente $d(p(x))\leq d(p(x)q(x))$ qualunque sia $q(x)\neq 0$. Inoltre, l'usuale divisione con resto tra polinomi mostra come, per ogni scelta di $a(x)$ e di $b(x)\neq 0$ si possano scegliere $h(x)$ e $r(x)$ in modo che sia $a(x)=h(x)b(x)+r(x)$, ed il grado di $r(x)$ sia inferiore a quello di $b(x)$, oppure $r(x)=0$.
— Sia $D=\mathbb{Z}[i]$ il sottoanello di $\mathbb{C}$ dei numeri complessi di parti reale ed immaginaria intere. D è chiaramente un dominio di integrità. Definiamo $d(z)=|z|^2$. In altre parole, se $z=a+bi$, allora $d(z)=a^2+b^2$. Allora d è una norma euclidea su D. Ho mostrato questo fatto in classe con un argomento geometrico. Lo stesso argomento geometrico si applica all'anello $\mathbb{Z}[\sqrt{-2}]$, ma non ad esempio a $\mathbb{Z}[\sqrt{-3}]$ o a $\mathbb{Z}[\sqrt{-5}]$. Si può vedere che questi anelli non sono ad ideali principali, e quindi non sono euclidei per nessuna scelta di d.
— Sia $\mathbf{k}$ un campo, e definiamo $d(x)=0$ per ogni $x\neq 0$. E' facile verificare che allora d è una norma euclidea. In effetti $\mathbf{k}$ è un dominio ad ideali principali, dal momento che i suoi unici ideali sono (0) e (1).

5.2. **Fattorizzazione unica in un dominio euclideo.**

Proposizione 5.2.1. *Ogni dominio euclideo è un dominio ad ideali principali.*

Dimostrazione. Sia $I\neq(0)$ un ideale di un dominio euclideo D, e sia $0\neq b$ un elemento di norma euclidea minima[3] tra gli elementi non nulli di I; poiché $b\in I$, allora $(b)\subset I$. Mostriamo adesso che vale anche l'altra inclusione $I\subset(b)$: per qualsiasi scelta di $a\in I$ possiamo scrivere $a=bq+r$, dove $d(r)<d(b)$ oppure $r=0$. Comunque, $r=a-bq$, e sia a che bq appartengono ad I. Quindi $r\in I$ deve essere zero, perché $d(r)$ non può essere minore di $d(b)$, a causa della scelta di b. Allora $a=bq$ per qualche $q\in D$. Ne concludiamo che ogni elemento di I è un multiplo di b. □

La norma euclidea rende immediato il calcolo degli elementi invertibili, come andiamo a mostrare.

Lemma 5.2.2. *Sia $a\in D$ un elemento non nullo. Allora $d(a)=d(ab)$ se e solo se b è invertibile. In altre parole, se b non è invertibile, allora $d(a)<d(ab)$.*

Dimostrazione. Se b è invertibile, allora $d(a)\leq d(ab)$, ma anche $d(ab)\leq d(abb^{-1})=d(a)$. Concludiamo che $d(a)=d(ab)$. Mostriamo adesso l'altra implicazione, e cioè che se $d(a)=d(ab)$ allora b è invertibile. Sia $d(a)=d(ab)$, ed effettuiamo la divisione euclidea di a per ab. Allora, se $a=abq+r$, avremo $d(r)<d(ab)=d(a)$, oppure $r=0$. Ma $r=a-abq=a(1-bq)$ quindi $d(a)\leq d(r)$. Questo mostra che $r=0$, e quindi che $a=abq$. Cancellando $a\neq 0$, si ottiene $bq=1$, perciò b è invertibile. □

Corollario 5.2.3. *$u\in D$ è un elemento invertibile se e solo se $d(u)=d(1)$.*

[2] A lezione l'ho indicata con N.
[3] Esiste per il principio di buon ordinamento dei numeri naturali.

5.3. **Esempi.**

— Nell'anello $\mathbb{Z}$ degli interi, la norma euclidea è data dal valore assoluto. Pertanto, $u \in \mathbb{Z}$ è invertibile se e solo se $|u| = 1$. In effetti, gli unici elementi invertibili di $\mathbb{Z}$ sono ± 1.

— Nell'anello $\mathbb{Z}[i]$ degli interi di Gauss, la norma euclidea è definita da $d(a+bi) = |a+bi|^2 = a^2+b^2$. Gli elementi invertibili in $\mathbb{Z}[i]$ sono pertanto quelli che soddisfano $d(a+bi) = d(1)$, cioè quelli tali che $a^2+b^2 = 0$. Si vede subito che questo accade quando $a = 0, b = \pm 1$ oppure $a = \pm 1, b = 0$. Gli unici elementi invertibili di $\mathbb{Z}[i]$ sono pertanto $\pm 1, \pm i$.

— Il grado è la norma euclidea dell'anello $\mathbf{k}[x]$ dei polinomi a coefficienti nel campo $\mathbf{k}$. L'unità moltiplicativa di $\mathbf{k}[x]$ è il polinomio costante 1, che ha grado 0. Gli elementi invertibili di $\mathbf{k}[x]$ sono quindi quelli non nulli che hanno grado 0, cioè le costanti non nulle.

Dal momento che i domini euclidei sono a ideali principali, vale per essi tutto ciò che abbiamo già dimostrato per i domini a ideali principali. In particolare, i concetti di primalità ed irriducibilità coincidono; ogni coppia di elementi possiede un massimo comun divisore, unico a meno di moltiplicazione per elementi invertibili, per il quale vale l'identità di Bézout; ogni elemento non nullo si esprime in maniera essenzialmente unica come prodotto di elementi primi e di un invertibile.

5.4. **Esempi.**

— Sia I l'ideale generato dal polinomio x^2+1 nel dominio euclideo $\mathbb{R}[x]$. Poiché x^2+1 non ha radici reali, deve essere un polinomio irriducibile, e quindi I è un ideale massimale. Ma allora l'anello quoziente $\mathbf{k} = \mathbb{R}[x]/I$ è un campo. Le classi di equivalenza di polinomi costanti formano un sottoanello isomorfo a $\mathbb{R}$, mentre l'elemento $\alpha = x + I$ soddisfa $\alpha^2 = -1$ in $\mathbb{R}[x]/I$. Allora $\mathbf{k}$ è un campo che contiene tutti i numeri reali, e che contiene un elemento il cui quadrato sia -1. L'applicazione $[a+bx] \mapsto a+bi$ costituisce un isomorfismo esplicito di $\mathbf{k}$ con il campo dei numeri complessi.

— L'ideale generato da x^2+1 nell'anello $\mathbb{C}[x]$ non è massimale, dal momento che x^2+1 si fattorizza in $\mathbb{C}[x]$: $x^2+1 = (x+i)(x-i)$, e non è nemmeno primo. Quindi il quoziente $\mathbb{C}[x]/(x^2+1)$ ammette divisori dello zero.

— Sia $\mathbb{F}_3$ il campo delle classi di resto modulo 3. Il polinomio x^2+1 è irriducibile su $\mathbb{F}_3$ in quanto n^2+1 non è congruo a $0 \mod 3$ per nessun intero n. Allora (x^2+1) è un ideale massimale in $\mathbb{F}_3[x]$. Il quoziente $\mathbb{F}_3[x]/(x^2+1)$ è un campo che possiede esattamente nove elementi.

— Sia $\mathbb{F}_5$ il campo delle classi di resto modulo 5. Il polinomio x^2+1 è riducibile su $\mathbb{F}_5$, in quanto $x^2+1 = (x+2)(x+3)$. Il quoziente $\mathbb{F}_5[x]/(x^2+1)$ non è quindi un campo. E' un anello commutativo con unità, che possiede 25 elementi, ma che ha divisori dello zero.

6. Il teorema dei due quadrati

6.1. **Irriducibilità negli interi di Gauss.** Analizziamo ora più da vicino l'anello $\mathbb{Z}[i]$ degli interi di Gauss. Gli elementi primi di $\mathbb{Z}[i]$ sono quelli irriducibili, in quanto $\mathbb{Z}[i]$ è un dominio euclideo, e quindi un dominio ad ideali principali. In particolare, nessun elemento di $\mathbb{Z} \subset \mathbb{Z}[i]$ può essere un elemento primo di $\mathbb{Z}[i]$ a meno di essere primo anche in $\mathbb{Z}$, in quanto la fattorizzazione di un numero composto in $\mathbb{Z}$ è una fattorizzazione non banale anche in $\mathbb{Z}[i]$.

Tuttavia gli elementi primi di $\mathbb{Z}$ non sono necessariamente irriducibili in $\mathbb{Z}[i]$. Ad esempio $2 = (1+i)(1-i)$, $5 = (2+i)(2-i)$. Si vede invece facilmente che 3 è irriducibile anche in $\mathbb{Z}[i]$. Il nostro scopo è quello di determinare tutti gli elementi irriducibili di $\mathbb{Z}[i]$. Ricordiamo che la norma euclidea in $\mathbb{Z}[i]$ è data da $d(a+bi) = a^2+b^2$.

Lemma 6.1.1. *Se $\alpha, \beta \in \mathbb{Z}[i]$ sono elementi non nulli, allora $d(\alpha\beta) = d(\alpha)d(\beta)$. Conseguentemente, il prodotto di numeri che si scrivono come somma di due quadrati si scrive ancora come somma di due quadrati.*

Dimostrazione. Si ha $d(z) = |z|^2$, e l'enunciato segue allora dal fatto che $|zw| = |z||w|$ per ogni scelta di $z, w \in \mathbb{C}$. Possiamo anche dimostrare direttamente questo fatto. Se $\alpha = a+bi$ e $\beta = c+di$, allora $d(\alpha) = a^2+b^2$ e $d(\beta) = c^2+d^2$. Abbiamo anche

$$d(\alpha\beta) = d((ac-bd)+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2.$$

Sviluppando si ottiene

$$\begin{aligned}(ac-bd)^2+(ad+bc)^2 &= a^2c^2+b^2d^2-2abcd+a^2d^2+b^2c^2+2abcd = \\ &= a^2c^2+b^2d^2+a^2d^2+b^2c^2 = (a^2+b^2)(c^2+d^2).\end{aligned}$$

□

Abbiamo già visto come gli elementi invertibili di $\mathbb{Z}[i]$ siano $\pm 1, \pm i$. Questo mostra che ogni $0 \neq \alpha \in \mathbb{Z}[i]$ ha esattamente quattro associati, cioè $\pm\alpha, \pm\alpha i$.

Proposizione 6.1.2. *Sia $p > 0$ un primo dispari di $\mathbb{Z}$. Allora le seguenti affermazioni sono equivalenti:*

(1) $p \equiv 1 \mod 4$;
(2) $x^2 + 1 = 0$ *ha soluzione in* $\mathbb{Z}/(p)$;
(3) p *è riducibile in* $\mathbb{Z}[i]$;
(4) $p = a^2 + b^2$ *per qualche scelta di* $a, b \in \mathbb{Z}$.

Dimostrazione. 1) $\Rightarrow$ 2). Questo segue, ad esempio, dal Teorema di Wilson[4]: se $p \equiv 1 \mod 4$, allora $x = ((p-1)/2)!$ soddisfa $x^2 + 1 \equiv 0 \mod p$.
2) $\Rightarrow$ 3). Se $a^2 + 1 \equiv 0 \mod p$, allora p divide $a^2 + 1$ in $\mathbb{Z}$ e quindi anche in $\mathbb{Z}[i]$. Ad ogni modo, $a^2 + 1 = (a + i)(a - i)$, e p non divide né $a + i$, né $a - i$. Pertanto p non è primo in $\mathbb{Z}[i]$, e quindi nemmeno irriducibile.
3) $\Rightarrow$ 4). Sia $p = \alpha\beta$ una fattorizzazione non banale in $\mathbb{Z}[i]$. Allora $p^2 = d(p) = d(\alpha)d(\beta)$, e $d(\alpha), d(\beta)$ sono entrambi diversi da 1, dal momento che non possono essere invertibili. Pertanto, $d(\alpha) = d(\beta) = p$. Poiché $\alpha = a + bi$ per qualche scelta di $a, b \in \mathbb{Z}$, abbiamo $p = d(\alpha) = a^2 + b^2$.
4) $\Rightarrow$ 1). Se $p = a^2 + b^2$ è dispari, a e b hanno opposta parità, e i loro quadrati sono congrui uno a 0 e l'altro a 1 modulo 4. Di conseguenza, $p \equiv 1 \mod 4$. □

Lemma 6.1.3. *Sia $p \in \mathbb{N}$ un primo dispari congruo ad 1 modulo 4. Allora p ammette una fattorizzazione non banale $(a + bi)(a - bi)$ in $\mathbb{Z}[i]$, e gli elementi $a \pm bi$ sono primi non associati in $\mathbb{Z}[i]$.*

Dimostrazione. Per la proposizione precedente, esistono $a, b \in \mathbb{N} \setminus \{0\}$ tali che $p = a^2 + b^2 = (a + bi)(a - bi)$. Sappiamo che $d(a + bi) = p$, e quindi se $a + bi = \alpha\beta$, allora $d(\alpha)d(\beta) = p$, e uno tra $d(\alpha)$ e $d(\beta)$ vale 1. Questo mostra che in una fattorizzazione di $a + bi$ uno dei fattori deve essere invertibile, e quindi che $a + bi$ è irriducibile, e quindi primo. Analogamente, anche $a - bi$ è primo.

Si vede subito che gli elementi $a + bi$ e $a - bi$ sono associati se e solo se $b = a$. Ma se questo accade, allora $p = 2a^2$, il che non può accadere se p è dispari. □

Osservazione 6.1.4. Dal momento che $d(1 \pm i) = 2$ è primo, si mostra facilmente che $1 + i$ e $1 - i$ sono irriducibili in $\mathbb{Z}[i]$. Tuttavia $1 + i$ e $1 - i$ sono associati in $\mathbb{Z}[i]$, dal momento che $1 - i = -i(1 + i)$. Vale allora in $\mathbb{Z}[i]$ la fattorizzazione $2 = -i(1 + i)^2$.

Proposizione 6.1.5. *Ogni irriducibile di $\mathbb{Z}[i]$ divide, in $\mathbb{Z}[i]$, un numero naturale primo. Se inoltre $a + bi$ è un elemento irriducibile di $\mathbb{Z}[i]$ con $a, b \neq 0$, allora $p = a^2 + b^2$ è un numero naturale primo.*

Dimostrazione. Ogni intero di Gauss $a + bi$ divide $a^2 + b^2 = (a + bi)(a - bi) \in \mathbb{Z}$. Se $a + bi$ è irriducibile (e quindi primo) in $\mathbb{Z}[i]$, deve allora dividere almeno uno dei numeri primi che compaiono nella fattorizzazione di $a^2 + b^2$ in $\mathbb{Z}$.

Pertanto esiste un naturale primo p che è multiplo, in $\mathbb{Z}[i]$, di $a + bi$ e questo mostra che $d(a + bi)$ divide $d(p) = p^2$. $d(a + bi)$ non può essere 1, perché $a + bi$ sarebbe invertibile, e non può essere p^2, perché allora sarebbe un associato di p, e quindi uguale ad uno tra $\pm p, \pm pi$, mentre sia la parte reale che quella immaginaria sono diverse da zero. L'unica possibilità rimasta è che sia $d(a + bi) = p$, ed in tal caso $p = a^2 + b^2 = (a + bi)(a - bi)$. □

Ricapitolando, i primi di $\mathbb{Z}[i]$, a meno di associati, sono $1 + i$, i numeri naturali primi congrui a 3 modulo 4, e i fattori non banali di numeri naturali primi congrui ad 1 modulo 4.

Teorema 6.1.6. *Un intero positivo N si scrive come somma di due quadrati interi se e solo se nella sua fattorizzazione in fattori primi i primi congrui a 3 modulo 4 compaiono con esponente pari.*

Dimostrazione. Supponiamo che N si scriva come somma di due quadrati: $N = a^2 + b^2$. Poiché in $\mathbb{Z}[i]$ vale il Teorema di fattorizzazione unica, possiamo trovare in $\mathbb{Z}[i]$ un invertibile u ed elementi primi $\pi_1, \ldots, \pi_n$ tali che

$$a + bi = u\pi_1 ... \pi_n.$$

Allora $N = a^2 + b^2 = d(a + bi) = d(u)d(\pi_1) \ldots d(\pi_n)$. Sappiamo già che $d(u) = 1$ e che $d(\pi_i)$ vale 2, oppure un numero naturale primo congruo a 1 modulo 4, oppure il quadrato di un numero naturale primo congruo a 3 modulo 4. Di conseguenza, ogni numero naturale primo congruo a 3 modulo 4 comparirà nella fattorizzazione di N con esponente pari.

Viceversa, supponiamo che nella fattorizzazione di N tutti i primi congrui a 3 modulo 4 compaiano con esponente pari. Sappiamo già che 2 ed i primi congrui ad 1 modulo 4 si scrivono come somma di due quadrati. Inoltre, se $p \equiv 3$ modulo 4, allora anche $p^2 = p^2 + 0$ è somma di due quadrati. Per il Lemma 6.1.1, N è prodotto di numeri che si scrivono come somma di due quadrati, e quindi si esprime anch'esso come somma di due quadrati. □

[4] ma si può mostrare anche in altro modo. Sappiamo, ad esempio, che $\mathbb{F}_p^\times$ è un gruppo ciclico di ordine $p - 1$, che è multiplo di 4. Ma allora contiene un elemento di ordine 4, il cui quadrato non può che essere -1.

6.2. **Esercizi.**

(a) Trovare tutte le soluzioni intere dell'equazione $x^2 + 1 = y^3$, sfruttando le proprietà dell'anello $\mathbb{Z}[i]$.

**(b)* Sia p un numero primo. Mostrare che $-2 \in \mathbb{F}_p$ è il quadrato di qualche elemento se e solo se p è congruo a ± 1 modulo 8.

(c) Utilizzando il risultato dell'esercizio *(b)*, determinare gli elementi primi nell'anello $\mathbb{Z}[\sqrt{-2}]$.

(d) Trovare tutte le soluzioni intere dell'equazione $x^2 + 2 = y^3$, sfruttando la fattorizzazione unica nel dominio euclideo $\mathbb{Z}[\sqrt{-2}]$.

(e) Mostrare che $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$, e che $2, 1 \pm \sqrt{-3}$ sono tutti irriducibili in $\mathbb{Z}[\sqrt{-3}]$.

(f) Mostrare che $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, e che $2, 3, 1 \pm \sqrt{-5}$ sono tutti irriducibili in $\mathbb{Z}[\sqrt{-5}]$.

(g) Mostrare che non esiste nessuna norma euclidea sui domini di integrità $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-5}]$.

7. Fattorizzazione di polinomi ed irriducibilità

Abbiamo già visto che, se K è un campo, in $K[x]$ vale il Teorema di fattorizzazione unica. Con un minimo di fatica si può mostrare che vale un risultato analogo nell'anello $\mathbb{Z}[x]$, facendo un uso opportuno del fatto che $\mathbb{Z}[x]$ è un sottoanello di $\mathbb{Q}[x]$ e utilizzando la fattorizzazione unica in quest'ultimo anello.

Questa strategia dimostrativa si adatta facilmente ai polinomi i cui coefficienti giacciono in un qualsiasi dominio a fattorizzazione unica R. L'idea è quella di immergere l'anello $R[x]$ in $K[x]$, dove K è il campo delle frazioni di R, e di confrontare le proprietà di fattorizzazione dei polinomi a coefficienti in D con quelle dei polinomi a coefficienti in K.

7.1. **Divisibilità e** MCD **nei domini a fattorizzazione unica.** Un dominio d'integrità R si dice *dominio a fattorizzazione unica* se ogni elemento non nullo può esprimersi come prodotto di un invertibile e di un numero finito di elementi irriducibili, e se ogni elemento irriducibile è primo. Quest'ultima richiesta garantisce di poter dimostrare l'unicità della fattorizzazione nella forma che abbiamo incontrato più volte.

Gli unici esempi che abbiamo incontrato finora sono i domini a ideali principali. In tali anelli, la primalità degli elementi irriducibili si dimostra utilizzando l'identità di Bézout; ad ogni modo, in un dominio a fattorizzazione unica, l'identità di Bézout non deve valere necessariamente.

Da questo momento in poi R è un dominio a fattorizzazione unica e per *fattorizzazione di* a intendiamo ogni fattorizzazione dell'elemento non nullo $a \in R$ nel prodotto di un invertibile e una quantità finita di elementi irriducibili (cioè primi) di R.

Proposizione 7.1.1. *Siano $a, b \in R$ elementi non nulli e siano*

$$a = up_1 \dots p_k, \qquad b = vq_1 \dots q_l,$$

dove u, v sono invertibili e p_i, q_j sono irriducibili.

Allora a divide b se e solo se $k \leq l$ e, a meno di riordinare i primi nella fattorizzazione di b, p_i è associato a q_i per ogni $i = 1, \dots, k$.

Dimostrazione. Se a divide b, allora $b = ac$ per qualche $c \in R$. Sia $c = wr_1 \dots r_m$ la fattorizzazione di c nel prodotto di w invertibile e r_i irriducibili. Allora

$$vq_1 \dots q_l = (uw)p_1 \dots p_k r_1 \dots r_m.$$

Per il teorema di fattorizzazione unica, $l = k + m$ e quindi $k \leq l$. Inoltre, a meno di riordinare i fattori a primo membro, p_i, q_i sono primi associati.[5]

Viceversa, se $k \leq l$ e p_i, q_i sono primi associati per $i = 1, \dots, k$, scegliamo x_i invertibili tali che $q_i = p_i x_i$. Otteniamo

$$b = v(p_1 x_1) \dots (p_k x_k) q_{k+1} \dots q_l = (v x_1 \dots x_k u^{-1})\ up_1 \dots p_k\ q_{k+1} \dots q_l.$$

Ma allora $b = ac$, dove $c = (v x_1 \dots x_k u^{-1}) q_{k+1} \dots q_l$. □

Osservazione 7.1.2. La proposizione appena dimostrata chiarisce che la relazione di divisibilità in R può essere letta in termini di fattorizzazioni. Per rendere la cosa più evidente, può essere il caso di *ripulire* le fattorizzazioni nel seguente modo:

- Se nella fattorizzazione di un elemento $0 \neq a \in R$ compaiono irriducibili distinti associati tra loro, li sostituiamo tutti con il primo irriducibile che compare, modificando opportunamente il fattore invertibile.

[5] così come anche r_j e q_{k+j}, ma questa informazione non ci interessa.

- Se abbiamo una quantità finita di elementi non nulli in R, e nella fattorizzazione del loro prodotto compaiono irriducibili distinti associati tra loro, li sostituiamo tutti con il primo irriducibile che compare, modificando opportunamente i fattori invertibili della fattorizzazione di ciascun elemento.

In questo modo, possiamo confrontare più direttamente le fattorizzazioni, in quanto i fattori irriducibili che compaiono, quando associati, sono proprio uguali. Possiamo anche rimpiazzare, per semplicità, il prodotto di k fattori tutti uguali a p con la potenza p^k.

La proposizione precedente si riformula quindi nel seguente modo:

Proposizione 7.1.3. *Siano $a, b \in R$ elementi non nulli tali che*

$$a = up_1^{m_1} \dots p_r^{m_r}, \qquad b = vp_1^{n_1} \dots p_r^{n_r},$$

dove u, v sono invertibili e $p_1, \dots, p_r$ sono irriducibili a due a due non associati. Allora a divide b se e solo se $m_i \leq n_i$ per ogni $i = 1, \dots, r$.

Proposizione 7.1.4. *Due elementi di R possiedono sempre un massimo comun divisore in R.*

Dimostrazione. Possiamo supporre che gli elementi siano entrambi non nulli, dal momento che evidentemente $\mathrm{MCD}(a, 0) = a$ per ogni $a \in R$. Siano allora $a, b \in R$ elementi non nulli tali che

$$a = up_1^{m_1} \dots p_r^{m_r}, \qquad b = vp_1^{n_1} \dots p_r^{n_r},$$

dove u, v sono invertibili e $p_1, \dots, p_r$ sono irriducibili a due a due non associati.

Se $d \in R$ divide sia a che b, nella sua fattorizzazione compaiono esclusivamente irriducibili associati a $p_1, \dots, p_r$. Alla luce dell'Osservazione 7.1.2, possiamo fattorizzare d usando i soli irriducibili $p_1, \dots, p_r$. Allora dire che

$$wp_1^{k_1} \dots p_r^{k_r}$$

divide sia a che b è lo stesso che affermare che $k_i \leq \min(m_i, n_i)$ per ogni $i = 1, \dots, r$.

Ma allora $d = p_1^{\min(m_1, n_1)} \dots p_r^{\min(m_r, n_r)}$ divide sia a che b, e ogni altro divisore comune di a e b divide d. □

Le seguenti affermazioni seguono ora immediatamente:

Corollario 7.1.5. *Siano a, b, c elementi non nulli di R. Allora $\mathrm{MCD}(ab, ac) = a\,\mathrm{MCD}(b, c)$.*

Corollario 7.1.6. *Se a divide bc e $\mathrm{MCD}(a, b) = 1$, allora a divide c.*

7.2. **Il Lemma di Gauss e la fattorizzazione unica negli anelli di polinomi.** In quello che segue, F è il campo delle frazioni del dominio a fattorizzazione unica R e p è un elemento primo di R. Per seguire più agevolmente le dimostrazioni, considerate il caso $R = \mathbb{Z}$, $F = \mathbb{Q}$. Ricordate che i domini a fattorizzazione unica non sono necessariamente ad ideali principali, sebbene questi siano praticamente gli unici esempi che abbiamo incontrato finora.

In un dominio a fattorizzazione unica ogni elemento ammette una fattorizzazione come prodotto (finito) di elementi irriducibili, e ogni elemento irriducibile è primo, cioè genera un ideale primo. Il succo del lemma di Gauss è la seguente affermazione:

Lemma 7.2.1. *Sia A un anello commutativo con unità, e $\mathfrak{p} \subset A$ un suo ideale primo. Allora la famiglia $\mathfrak{p}[x]$ dei polinomi a coefficienti in $\mathfrak{p}$ è un ideale primo dell'anello $A[x]$.*

Dimostrazione. Il quoziente $A/\mathfrak{p}$ è un dominio di integrità, e quindi tale è anche l'anello dei polinomi $(A/\mathfrak{p})[x]$. Sia $\pi : A[x] \to (A/\mathfrak{p})[x]$ l'applicazione di riduzione modulo $\mathfrak{p}$ dei coefficienti di un polinomio. L'applicazione π è un omomorfismo suriettivo di anelli, ed il suo nucleo è costituito dai polinomi i cui coefficienti giacciono in $\mathfrak{p}$: in altre parole $\ker \pi = \mathfrak{p}[x]$. Ma allora $(A/\mathfrak{p})[x] \simeq A[x]/\mathfrak{p}[x]$: poiché $(A/\mathfrak{p})[x]$ è un dominio di integrità, $\mathfrak{p}[x]$ deve essere un ideale primo di $A[x]$. □

Corollario 7.2.2. *Sia A un anello commutativo con unità. Se $p \in A$ è un elemento primo in A, allora il polinomio costante $p \in A[x]$ è primo in $A[x]$.*

Dimostrazione. In un anello commutativo con unità, l'ideale (p) generato da un elemento non nullo p è primo se e soltanto se l'elemento p è primo.

Ma allora, se p è primo in A, l'ideale $\mathfrak{p} = pA$ è primo. Per il Lemma7.2.1 anche $\mathfrak{p}[x] = pA[x]$ è un ideale primo di $A[x]$. Tuttavia, $pA[x]$ è l'ideale generato da p in $A[x]$, e quindi p è primo in $A[x]$. □

Osservazione 7.2.3. Nella dimostrazione appena vista, si è avvertita la difficoltà di indicare con (p) l'ideale generato da p quando p è elemento di due anelli diversi. Pertanto preferiremo d'ora in poi indicare con pA l'ideale generato da p nell'anello A.

Se R è un dominio a fattorizzazione unica, è possibile calcolare il massimo comun divisore di una famiglia (anche infinita, ma non ci servirà) di elementi di R. Dato un polinomio $f(x) \in R[x]$ possiamo quindi calcolare il massimo comun divisore dei suoi coefficienti non nulli: questo è detto "*contenuto*" di $f(x)$, e si indica con $\mathrm{c}(f(x))$ — come ogni massimo comun divisore, è definito a meno di moltiplicazione per un elemento invertibile, e determina quindi una classe di elementi associati, e non un unico elemento di R.

In altre parole, il contenuto di un polinomio $f(x) \in R[x]$ è il "più grande" elemento in R che possiamo raccogliere a fattor comune da $f(x)$. Un polinomio è *primitivo* se ha contenuto 1.

Osservazione 7.2.4. Segue immediatamente dal Corollario 7.1.5 che $\mathrm{c}(af(x)) = a\,\mathrm{c}(f(x))$ se $a \in R$, $f(x) \in R[x]$. Inoltre $f(x)/\mathrm{c}(f(x)) \in R[x]$ per ogni scelta di $f(x) \in R[x]$.

In particolare, se $f(x)$ è un polinomio di grado > 0 e $\mathrm{c}(f(x)) \neq 1$, allora $f(x)$ non può essere irriducibile in quanto, in tal caso, $f(x) = \mathrm{c}(f(x)) \cdot f(x)/\mathrm{c}(f(x))$ è una fattorizzazione non banale in $R[x]$.

Lemma 7.2.5 (Gauss)**.** *Il prodotto di polinomi primitivi in $R[x]$ è ancora un polinomio primitivo.*

Dimostrazione. Siano $f(x), g(x) \in R[x]$ polinomi a coefficienti in R. Se il loro prodotto $f(x)g(x)$ non è primitivo, allora $\mathrm{c}(f(x)g(x)) \neq 1$, e possiamo quindi trovare un elemento primo $p \in R$ che lo divide. Se $\mathfrak{p} = pR$ è l'ideale primo di R generato da p, allora $f(x)g(x) \in \mathfrak{p}[x]$. Ma $\mathfrak{p}[x]$ è un ideale primo di $R[x]$, e quindi almeno uno tra $f(x)$ e $g(x)$ appartiene a $\mathfrak{p}[x]$, e non è quindi primitivo. In conclusione, se il prodotto di $f(x)$ e $g(x)$ non è primitivo, allora almeno uno tra $f(x)$ e $g(x)$ non è primitivo. Equivalentemente, se $f(x)$ e $g(x)$ sono entrambi primitivi, anche il loro prodotto deve esserlo. □

Corollario 7.2.6. *Il contenuto del prodotto di due polinomi in $R[x]$ è pari al prodotto dei contenuti dei polinomi.*

Dimostrazione. Se $f(x) = \mathrm{c}(f(x))F(x)$ e $g(x) = \mathrm{c}(g(x))G(x)$, allora i polinomi $F(x)$ e $G(x)$ sono primitivi. Il prodotto $f(x)g(x)$ è pari a $\mathrm{c}(f(x))\mathrm{c}(g(x))F(x)G(x)$, ed è quindi il prodotto di $\mathrm{c}(f(x))\mathrm{c}(g(x))$ e di un polinomio primitivo. Il suo contenuto è quindi $\mathrm{c}(f(x))\mathrm{c}(g(x))$. □

Corollario 7.2.7. *Due polinomi in $R[x]$ il cui prodotto è un polinomio primitivo sono entrambi primitivi.*

Dimostrazione. Se $a(x)b(c)$ è primitivo, allora $\mathrm{c}(a(x))\mathrm{c}(b(x)) = 1$ e quindi $\mathrm{c}(a(x)), \mathrm{c}(b(x))$ sono entrambi invertibili. □

Siamo pronti a mostrare il risultato fondamentale di questo paragrafo. Sia R un dominio a fattorizzazione unica, e $R[x]$ il suo anello dei polinomi. Sappiamo che R si immerge nel suo campo delle frazioni F, e alla stessa maniera $R[x]$ si immerge nell'anello $F[x]$, che è un dominio a ideali principali, ed è quindi a fattorizzazione unica. Possiamo quindi pensare di utilizzare la fattorizzazione di polinomi in $F[x]$ per fattorizzare un polinomio in $R[x]$. Questa strategia è vincente! Il punto essenziale per mostrarlo è il seguente:

Proposizione 7.2.8. *Sia $f(x) \in R[x]$ un polinomio non costante primitivo. Allora $f(x)$ è irriducibile in $R[x]$ se e solo se è irriducibile in $F[x]$.*

Dimostrazione. Innanzitutto, $f(x)$ non è invertibile, in quanto non costante. Poiché $f(x)$ è primitivo, in una fattorizzazione non banale $f(x) = a(x)b(x)$ in $R[x]$, né $a(x)$, né $b(x)$ sono costanti; pertanto, $f(x) = a(x)b(x)$ è anche una fattorizzazione non banale in $F[x]$. In conclusione, se $f(x)$ è riducibile in $R[x]$, deve esserlo anche in $F[x]$; equivalentemente, se $f(x)$ è irriducibile in $F[x]$, deve esserlo anche in $R[x]$. Rimane da mostrare che da una fattorizzazione non banale di $f(x)$ in $F[x]$ possiamo ricavare una sua fattorizzazione non banale in $R[x]$.

Supponiamo che $f(x) = a(x)b(x)$, dove $a(x), b(x) \in F[x]$ sono polinomi non costanti. I coefficienti del polinomio $a(x) = a_n x^n + \cdots + a_1 x + a_0$ sono frazioni $a_i = r_i/s_i$ con $r_i, s_i \in R$ e $s_i \neq 0$. Pertanto, se $A = s_0 s_1 \dots s_n$, allora $A \neq 0$ e $Aa(x) \in R[x]$. Allo stesso modo, è possibile trovare $B \in R$ tale che $Bb(x) \in R[x]$.

Allora $ABf(x) = (Aa(x))(Bb(x))$, con $Aa(x), Bb(x) \in R[x]$. Se poniamo $A' = \mathrm{c}(Aa(x)), B' = \mathrm{c}(Bb(x))$, il Lemma di Gauss ci assicura che $A'B' = \mathrm{c}(ABf(x)) = AB\mathrm{c}(f(x))$, che è uguale ad AB, poiché $f(x)$ è primitivo. Dividendo un polinomio a coefficienti in R per il suo contenuto, si ottiene ancora un elemento di $R[x]$, pertanto

$$f(x) = \frac{AB}{A'B'} f(x) = \frac{(Aa(x))(Bb(x))}{A'B'} = \frac{Aa(x)}{A'} \frac{Bb(x)}{B'}$$

è una fattorizzazione non banale di $f(x)$ in $R[x]$. □

Lemma 7.2.9. *Sia $f(x) \in R[x]$ un polinomio primitivo non costante, $a(x) \in R[x]$. Se $a(x) = f(x)q(x)$, con $q(x) \in F[x]$, allora $q(x) \in R[x]$. In altre parole, se $f(x)$ divide $a(x)$ in $F[x]$, lo divide anche in $R[x]$.*

Dimostrazione. Dal momento che i coefficienti di $q(x)$ appartengono al campo F delle frazioni di R, possiamo come prima trovare $Q \neq 0$ in R tale che $Qq(x) \in R[x]$. Allora $Qa(x) = f(x) \cdot (Qq(x))$. Detto c il contenuto del polinomio $Qq(x)$, abbiamo

$$Q \cdot \mathrm{c}(a(x)) = \mathrm{c}(Qa(x)) = \mathrm{c}(f(x)) \cdot c(Qq(x)) = 1 \cdot c = c.$$

Questo mostra che Q divide c, e quindi tutti i coefficienti di $Qq(x)$. Pertanto, $q(x) = (Qq(x))/Q$ appartiene a $R[x]$. □

Corollario 7.2.10. *Sia $f(x) \in R[x]$ un polinomio irriducibile di grado > 0. Allora $f(x)$ è primo in $R[x]$.*

Dimostrazione. Il polinomio $f(x)$ è irriducibile e non costante, ed è quindi primitivo. Dall'irriducibilità di $f(x)$ in $R[x]$ segue la sua irriducibilità in $F[x]$; poiché $F[x]$ è un dominio a ideali principali, $f(x)$ è primo in $F[x]$.

Siano $a(x), b(x)$ polinomi a coefficienti in R. Se $f(x)$ divide il prodotto $a(x)b(x)$ in $R[x]$, allora lo divide anche in $F[x]$. Ma $f(x)$ è primo in $F[x]$, e quindi $f(x)$ divide in $F[x]$ uno tra $a(x)$ e $b(x)$. Per il Lemma 7.2.9, $f(x)$ divide allora in $R[x]$ uno tra $a(x)$ e $b(x)$. In altre parole, $f(x)$ è primo in $R[x]$. □

Gli elementi irriducibili di $R[x]$ sono di due tipi: quelli costanti sono gli elementi irriducibili di R; quelli non costanti sono primitivi, e sono irriducibili in $F[x]$. Gli irriducibili di entrambi i tipi sono anche primi, grazie ai Corollari 7.2.2 e 7.2.10. Siamo quindi pronti a dimostrazione che in $R[x]$ vale la fattorizzazione unica.

Teorema 7.2.11. *Sia R un dominio a fattorizzazione unica. Allora l'anello $R[x]$ è un dominio a fattorizzazione unica.*

Dimostrazione. Sia $f(x) \in R[x]$ un polinomio non nullo. Allora $f(x) = cF(x)$, dove $c = \mathrm{c}(f(x))$ e $F(x) = f(x)/c$ è un polinomio primitivo. Fattorizziamo ora c e $F(x)$ separatamente.

Poiché in R vale la fattorizzazione unica, possiamo trovare un invertibile $u \in R$ ed elementi primi $\pi_1, \ldots, \pi_r \in R \subset R[x]$ tali che $c = u\pi_1 \ldots \pi_r$. Allo stesso modo, è possibile fattorizzare $F(x)$ nel prodotto di polinomi irriducibili (primitivi) in $R[x]$: mostriamolo per induzione sul grado di $F(x)$. Se $F(x)$ è irriducibile, non c'è nulla da mostrare; se invece $F(x) = G(x)H(x)$, allora $G(x)$ e $H(x)$ sono primitivi, ed hanno grado inferiore. Per ipotesi induttiva, possiamo esprimerli come prodotto di polinomi irriducibili primitivi. La base dell'induzione è ovvia, poiché i polinomi primitivi di grado 1 sono tutti irriducibili.

L'unicità della fattorizzazione si dimostra alla maniera solita sfruttando il fatto che tutti gli irriducibili sono primi. Alternativamente, si può sfruttare l'unicità della fattorizzazione in R e in $F[x]$. □

Corollario 7.2.12. *Gli anelli $\mathbb{Z}[x_1, ..., x_n]$ e $\mathbf{k}[x_1, ..., x_n]$, dove $\mathbf{k}$ è un campo, sono domini a fattorizzazione unica.*

Dimostrazione. Per induzione, notando che $\mathbb{Z}[x_1, \ldots, x_{n+1}] = \mathbb{Z}[x_1, \ldots, x_n][x_{n+1}]$ e $\mathbf{k}[x_1, \ldots, x_{n+1}] = \mathbf{k}[x_1, \ldots, x_n][x_{n+1}]$. La base dell'induzione segue dal fatto che $\mathbb{Z}$ e $\mathbf{k}[x_1]$ sono domini a ideali principali, e quindi a fattorizzazione unica.

□

Gli anelli $\mathbb{Z}[x_1, ..., x_m], m \geq 1$ e $\mathbf{k}[x_1, ..., x_n], n \geq 2$ costituiscono esempi di domini a fattorizzazione unica in cui non ogni ideale è principale (provate a dimostrarlo!).

7.3. **Il criterio di irriducibilità di Eisenstein.** Può capitare, come vedremo in teoria dei campi, che un problema di algebra si riduca alla fattorizzazione di un polinomio in polinomi irriducibili, e quindi a stabilire se un dato polinomio sia irriducibile. Può essere utile avere qualche metodo utile a portata di mano.

Proposizione 7.3.1. *Sia $a(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0$ un polinomio primitivo (cioè senza divisori costanti che non siano invertibili) a coefficienti nel dominio d'integrità R e $p \in R$ un elemento primo, tali che*

- *p non divide a_m;*
- *p divide a_i per ogni $0 \leq i \leq m-1$;*
- *p^2 non divide a_0.*

Allora $a(x)$ è irriducibile in $R[x]$.

Dimostrazione. Supponiamo, per assurdo, che esista una fattorizzazione non banale $a(x) = f(x)g(x)$ in $R[x]$. Poiché $a(x)$ è primitivo, nessuno dei fattori è costante. Inoltre, se $f(x) = f_h x^h + f_{h-1}x^{h-1} + \cdots + f_1 x + f_0$, $g(x) = g_k x^k + g_{k-1}x^{k-1} + \cdots + g_1 x + g_0$, $f_h g_k = a_m$ non è divisibile per p, e quindi neanche f_h, g_k lo sono.

Osserviamo ora che $(p) = pR$ è un ideale massimale di R e quindi $R/(p)$ è un campo. Di conseguenza, $R/(p)[x]$ è un dominio euclideo ed è quindi a fattorizzazione unica. Riducendo modulo p, otteniamo $\overline{a(x)} = \overline{f(x)}\,\overline{g(x)}$, e per le ipotesi fatte si ha $\overline{a(x)} = \overline{a_m}x^m$.

Il polinomio x ha grado 1 ed è quindi irriducibile in $R/(p)[x]$. Utilizzando la fattorizzazione unica in $R/(p)[x]$, otteniamo allora $\overline{f(x)} = \overline{f_h}x^h$, $\overline{g(x)} = \overline{g_k}x^k$, e quindi $f(x)$ e $g(x)$ hanno entrambi termine noto multiplo di p. Ma allora $a(x)$ ha termine noto $a_0 = f_0 g_0$, che è multiplo di p^2, da cui l'assurdo. □

Ovviamente, il criterio di Eisenstein trova la sua più frequente applicazione quando $R = \mathbb{Z}$.

Esempi:

- I polinomi $x^4 + 2$, $x^4 + 3$ sono irriducibili in $\mathbb{Z}[x]$. Infatti il criterio di Eisenstein si applica al primo polinomio con il primo $p = 2$ ed al secondo con il primo $p = 3$.
- Il polinomio $x^4 + 4$ è riducibile in $\mathbb{Z}[x]$. Infatti $x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - (2x)^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$.
- Il polinomio $x^4 + 9$ è irriducibile in $\mathbb{Z}[x]$. Si vede facilmente come non possieda soluzioni razionali – in realtà non ne possiede neanche di reali! – e quindi non ammette fattori lineari che lo dividano. Bisogna tuttavia scartare anche l'eventualità che $x^4 + 9$ si fattorizzi come prodotto di due polinomi di secondo grado. Se questo accade allora

  $$x^4 + 9 = (x^2 + ax + b)(x^2 + cx + d),$$

  dove a, b, c, d sono numeri interi, e i fattori a secondo membro sono monici in quanto il prodotto dei primi coefficienti deve essere 1: a meno di cambiare segno ad entrambi possiamo supporre che siano entrambi uguali ad 1. Sviluppando il prodotto si ottengono le equazioni $a + c = 0$, $b + d + ac = 0$, $ad + bc = 0$, $bd = 9$, che dobbiamo risolvere sugli interi. Dalla prima otteniamo $c = -a$, da cui $ad + bc = a(d - b) = 0$. Quindi $a = 0$ oppure $d = b$.

  Ma se $a = c = 0$, allora $b + d + ac = b + d = 0$, che è incompatibile con $-b^2 = bd = 9$. Invece, se $b = d$, allora da $bd = 9$ segue $b = d = \pm 3$ e quindi $0 = ac + b + d = -a^2 + 2b$ da cui $a^2 = \pm 6$. Ma ± 6 non sono quadrati di interi, e quindi anche questa possibilità è da scartare. Il polinomio $x^4 + 9$ non ammette fattori né di primo né di secondo grado, ed è quindi irriducibile. Si noti che il criterio di Eisenstein non si applica a tale polinomio, pur essendo irriducibile.
- Sia p un numero primo. Il polinomio ciclotomico $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$ è irriducibile in $\mathbb{Z}[x]$. Possiamo infatti facilmente calcolare $\Phi_p(x + 1)$: dal momento che $\Phi_p(x) = (x^p - 1)/(x - 1)$ avremo $\Phi_p(x + 1) = ((x + 1)^p - 1)/x$ e quindi

  $$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + ... + \binom{p}{p-2}x + \binom{p}{p-1}.$$

  E' facile vedere come tutti i coefficienti successivi al primo di tale polinomio siano divisibili per p, e come il termine noto non sia divisibile per p^2. Pertanto $\Phi_p(x + 1)$ è irriducibile, e quindi anche $\Phi_p(x)$ lo è. Infatti una fattorizzazione $\Phi_p(x) = a(x)b(x)$ fornirebbe una corrispondente fattorizzazione $\Phi_p(x + 1) = a(x + 1)b(x + 1)$.

7.4. **Radici razionali di polinomi a coefficienti interi.** Per verificare la possibile irriducibilità di un polinomio a coefficienti in $\mathbb{Z}$ è utile sapere se possiede radici razionali, per escludere la presenza di fattori di primo grado. Qui generalizzo al caso di un dominio a fattorizzazione unica un'affermazione fatta a lezione nel caso di $\mathbb{Z}$ e $\mathbb{Q}$.

Lemma 7.4.1. *Sia R un dominio a fattorizzazione unica, F il suo campo delle frazioni, $f(x) = f_n x^n + ... + f_1 x + f_0 \in R[x]$, e $a/b \in F$ una radice di $f(x)$, con $\mathrm{MCD}(a, b) = 1$. Allora a divide f_0, e b divide f_n.*

Dimostrazione. Sia $f(a/b) = 0$. Semplificando i denominatori si ottiene:

$$f_n a^n + f_{n-1} a^{n-1} b + ... + f_1 a b^{n-1} + f_0 b^n = 0.$$

Tutti gli addendi tranne l'ultimo sono multipli di a, e quindi anche l'ultimo lo è. Allo stesso modo, tutti gli addendi tranne il primo sono multipli di b, e quindi anche il primo lo è. Sappiamo quindi che a divide $f_0 b^n$ e b divide $f_n a^n$. Poiché $\mathrm{MCD}(a, b) = 1$ possiamo usare il Corollario 7.1.6 e concludere che a deve dividere f_0 e b deve dividere f_n. □

Esempi:

- Il polinomio $x^3 + 15x + 4$ è irriducibile sugli interi. Se fosse riducibile, infatti, avrebbe almeno un fattore di grado 1, e quindi una radice (intera) razionale. Ma le possibili radici razionali sono soltanto $\pm 1, \pm 2, \pm 4$, e si controlla facilmente (sostituendo) che nessuno di questi valori soddisfa il polinomio dato.
- Il polinomio $4x^3 - 15x - 2$ è riducibile sugli interi. Per cercarne soluzioni razionali, scriviamo tutti i possibili rapporti tra divisori del termine noto e divisori del primo coefficiente: essi sono $\pm 2, \pm 1, \pm 1/2, \pm 1/4$. Sostituendo nel polinomio, scopriamo che 2 è l'unico di tali valori ad annullare il polinomio, e ne è quindi l'unica radice razionale. Dividendo per $x - 2$ otteniamo

$4x^3 - 15x - 2 = (x-2)(4x^2+8x+1)$. Dal momento che $x = 2$ non è soluzione del polinomio $4x^2 + 8x + 1$, esso è allora sicuramente irriducibile, non essendoci altre radici razionali di $4x^3 - 15x - 2$.

7.5. **Riduzione modulo p.** Verificare la riducibilità o l'irriducibilità di un polinomio a coefficienti negli interi modulo un primo p è talvolta molto semplice. Ad esempio il polinomio $x^2 + x + 1 \in \mathbb{F}_2[x]$ è sicuramente irriducibile: infatti si spezza in fattori lineari solo se ammette soluzioni in $\mathbb{F}_2$. Per controllare se questo succeda dobbiamo sostituire in $x^2 + x + 1$ ogni elemento di $\mathbb{F}_2$. Ma ve ne sono soltanto due: 0 e 1. Sostituendo vediamo che questi due valori non sono soluzioni, e che quindi $x^2 + x + 1$ è un polinomio irriducibile. E' in effetti l'unico polinomio irriducibile di secondo grado. Gli altri sono

$$x^2 = x \cdot x, \qquad x^2 + 1 = (x+1)(x+1), \qquad x^2 + x = x(x+1).$$

Allo stesso modo, troviamo i polinomi irriducibili di grado 3: essi sono

$$x^3 + x + 1, \qquad x^3 + x^2 + 1.$$

Ora, l'applicazione che associa ad un polinomio in $\mathbb{Z}[x]$ il polinomio ottenuto riducendo i suoi coefficienti modulo 2 è un omomorfismo di anelli. Pertanto ad una fattorizzazione di un polinomio in $\mathbb{Z}[x]$ corrisponde una fattorizzazione del polinomio corrispondente in $\mathbb{F}_2[x]$. Se il polinomio corrispondente è irriducibile, deve essere irriducibile anche il polinomio dal quale siamo partiti. Ricapitoliamo il ragionamento, generalizzandolo a un qualsiasi dominio a fattorizzazione unica.

Proposizione 7.5.1. *Siano R un dominio d'integrità, $f(x) \in R[x]$ un polinomio non costante primitivo, $p \in R$ un elemento primo che non divide il coefficiente direttore[6] di $f(x)$. Se la riduzione modulo p di $f(x)$ è irriducibile in $R/(p)\,[x]$, allora $f(x)$ è irriducibile in $R[x]$.*

Dimostrazione. Se $f(x)$ è riducibile, e $f(x) = a(x)b(x)$ è una sua fattorizzazione non banale, allora $a(x)$ e $b(x)$ non sono costanti, dal momento che $f(x)$ è primitivo. Ma allora $\overline{f(x)} = \overline{a(x)}\,\overline{b(x)}$ è una fattorizzazione nel dominio d'integrità $R/(p)\,[x]$ nel prodotto di polinomi non costanti. □

Esempi:

- Il polinomio $x^3 + 15x + 25$ è irriducibile sugli interi. In effetti la sua riduzione modulo 2 è il polinomio $x^3 + x + 1$ che è irriducibile su $\mathbb{F}_2$.
- Il polinomio $4x^2 - 7x - 16$ è irriducibile sugli interi dal momento che la sua riduzione modulo 3 è irriducibile su $\mathbb{F}_3$. Infatti sostituendo i valori $x = 0, 1, 2$ in $x^2 + 2x + 2$ otteniamo $2, 2, 1$ e quindi $x^2 + 2x + 2$ non può spezzarsi in fattori lineari.
- Il polinomio $4x^2 + 8x + 1$ è irriducibile su $\mathbb{Z}$ in quanto la sua riduzione modulo 5 è irriducibile modulo 5. Essa è $-x^2 + 3x + 1$, ed i suoi valori su $0, 1, 2, 3, 4$ sono $1, 3, 3, 1, 2$.
- Attenzione! Il polinomio $x^4 + 1$ è irriducibile su $\mathbb{Z}$, eppure la sua riduzione modulo p è riducibile per ogni primo p. (Per mostrarlo, fate vedere che il prodotto di due non quadrati modulo p è un quadrato modulo p..)

7.6. **Esercizi.**

(a) Mostrare che $x^6 + x^3 + 1$ è irriducibile in $\mathbb{Z}[x]$.

***(b)* Indichiamo con $\mathbf{k}(x)$ il campo delle espressioni razionali in x a coefficienti in un campo $\mathbf{k}$, cioè il campo delle frazioni di $\mathbf{k}[x]$. Mostrare che se $\phi : \mathbf{k}(x) \to \mathbf{k}(x)$ è un isomorfismo che si restringe all'identità su $\mathbf{k}$, allora $\phi(x) = (ax + b)/(cx + d)$ per un'opportuna scelta di $a, b, c, d \in \mathbf{k}$. *[Sugg.: ridurre tutto alla risoluzione di un'equazione in una variabile t, da risolvere nell'anello $\mathbf{k}[x]$, ed utilizzare il Lemma 7.4.1.]*

7.7. **Il teorema fondamentale dell'algebra.** Se analizzare l'irriducibilità di polinomi su $\mathbb{Z}$ e su $\mathbb{Q}$ può presentare qualche difficoltà, il panorama è completamente diverso quando analizziamo lo stesso problema sui campi $\mathbb{R}$ e $\mathbb{C}$. Il campo dei numeri complessi è infatti un esempio di *campo algebricamente chiuso*, il che vuol dire che ogni polinomio a coefficienti complessi si spezza nel prodotto di fattori lineari. Questo ha conseguenze anche per il campo dei numeri reali, nel quale i polinomi irriducibili possono avere soltanto grado uno o due.

Vi fornirò la dimostrazione del teorema fondamentale dell'algebra più tardi, dopo aver enunciato la corrispondenza di Galois (se mai lo faremo!). Per il momento, eccovi l'enunciato.

Teorema 7.7.1. *Sia $p(x) = p_n x^n + \ldots + p_1 x + p_0$ un polinomio non costante a coefficienti in $\mathbb{C}$. Allora esiste un complesso $z_0 \in \mathbb{C}$ tale che $p(z_0) = 0$.*

Corollario 7.7.2. *Gli unici polinomi irriducibili in $\mathbb{C}[x]$ sono quelli di grado 1.*

[6] cioè il coefficiente del termine di grado massimo.

Corollario 7.7.3. *I polinomi irriducibili in $\mathbb{R}[x]$ sono tutti quelli di grado 1, e quelli della forma $ax^2 + bx + c$, con $a \neq 0, b^2 - 4ac < 0$.*

Dimostrazione. Ogni polinomio di grado 1 è necessariamente irriducibile. Quelli di grado 2 sono irriducibili se non hanno radici reali.

Per mostrare che non vi sono altri polinomi irriducibili, utilizziamo il teorema fondamentale dell'algebra. Sia $p(x)$ un polinomio a coefficienti reali di grado maggiore di 2. Per il teorema fondamentale dell'algebra, l'equazione $p(x) = 0$ ammette almeno una soluzione x_0 in $\mathbb{C}$. Se questa soluzione è reale, allora $p(x)$ è divisibile per $x - x_0$, e quindi $p(x)$ è riducibile.

Se invece x_0 non è reale, scriviamo $x_0 = \alpha + \beta i$. Dal momento che i coefficienti di $p(x)$ sono tutti reali, anche il complesso coniugato di x_0 è radice di $p(x)$. Questo mostra che $p(x)$ è divisibile per $(x - \alpha - \beta i)(x - \alpha + \beta i) = x^2 - 2\alpha x + (\alpha^2 + \beta^2)$, un polinomio a coefficienti reali. Anche in questo caso $p(x)$ non può essere irriducibile. □

E-mail address: dandrea@mat.uniroma1.it