Anelli

dispense provvisorie del corso di Algebra 1 2010-2011

Alessio Del Vigna - Giovanni Gaiffi

16 febbraio 2011

1 Prime definizioni

Abbiamo già dato in precedenza la definizione di anello associativo, e quindi la richiamiamo:

Definizione 1.1. Un insieme non vuoto R è un *anello* associativo se in R sono definite due operazioni, denotate con $+$ e $\cdot$ rispettivamente, tali che per $a, b, c \in R$:

(1) R è un gruppo abeliano con l'addizione;

(2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *(legge associativa)*;

(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ *(leggi distributive).*

Possiamo avere altre proprietà dell'operazione di moltiplicazione che caratterizzano tipi diversi di anello. Diciamo *anelli commutativi* quelli in cui la moltiplicazione è commutativa, e diciamo *anelli con identità* quelli per cui esiste l'elemento neutro della moltiplicazione, indicato con il simbolo 1, tale che, per ogni $a \in R$, $a \cdot 1 = 1 \cdot a = a$. **Nel seguito intenderemo con il termine anello un anello con identità**.

Esempio 1.1. Esempi di anelli sono l'insieme $\mathbb{Z}$ con addizione e moltiplicazione, l'insieme $\mathbb{R}[x]$ dei polinomi ad una variabile e a coefficienti reali con addizione e moltiplicazione usuali sui polinomi. Entrambi sono anelli commutativi con identità: sia nel primo che nel secondo l'identità è il numero intero 1. L'insieme $\mathbb{Z}_n$ con addizione e moltiplicazione definite sulle classi in modo ovvio è un anello commutativo con identità $[1]_n$.

Esempio 1.2. L'insieme degli interi pari rispetto alle ordinarie addizione e moltiplicazione è un anello commutativo ma senza elemento neutro per la moltiplicazione. [1]

Esempio 1.3. Anche l'insieme $R = \{0\}$ può essere visto come un anello in cui l'identità è lo 0 stesso[2].

Accenniamo che, analogamente per quanto accade con i gruppi, vale il seguente lemma:

Lemma 1.1. *Sia R un anello con identità. Allora valgono:*

(1) *l'identità 1 è unica;*

(2) $a \cdot 0 = 0 \cdot a = 0$ *per ogni $a \in R$;*

[1] Alcuni chiamano "rng" tali anelli che sono "ring" senza la "i", identità.

[2] Tale anello è talvolta chiamato "anello banale" o "stupid ring".

(3) $a(-b) = -(ab)$ *e* $(-a)b = -(ab)$ *per ogni* $a, b \in R$.

Dimostrazione. (1) La prima proprietà si ottiene osservando che se 1 e $1'$ sono due identità moltiplicative allora $1 = 1 \cdot 1' = 1'$.
(2) Sia $a \in R$, allora si ha $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$, e dunque segue $a \cdot 0 = 0$; analogamente si mostra $0 \cdot a = 0$.
(3) Mostriamo che $ab + a(-b) = 0$: per la proprietà distributiva $ab + a(-b) = a(b-b) = a \cdot 0 = 0$. In maniera del tutto analoga si mostra anche la seconda parte. □

Definizione 1.2. Un *sottoanello* di un anello R è un suo sottoinsieme che, con le operazioni indotte da R, risulta essere a sua volta un anello.

Quindi per vedere se un sottoinsieme R' di R è un sottoanello, bisogna verificare che R' sia un sottogruppo additivo di R e che sia chiuso rispetto alla moltiplicazione. Inoltre, **visto che stiamo considerando anelli con identità**, R' deve anche contenere l'identità moltiplicativa.

Esempio 1.4. Se consideriamo $\mathbb{Q}$ come anello rispetto ad usuali somma e prodotto, allora $\mathbb{Z}$ è un sottoanello.

Definizione 1.3. Un anello con identità in cui $0 \neq 1$ e, per ogni elemento $a \neq 0$ esiste un inverso b tale che $a \cdot b = b \cdot a = 1$, si dice *corpo*. Un *campo* è un corpo commutativo.

Esercizio 1.1. Avendo in mente il gruppo Q_8 dei quaternioni, consideriamo l'insieme dei quaternioni reali:

$$\mathbb{R}Q_8 = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

Dimostrare che tale insieme, con le operazioni di somma e moltiplicazione naturali, è un corpo ma non è un campo.

2 Elementi invertibili, divisori dello zero e domini di integrità

Definizione 2.1. Sia R un anello commutativo. Diciamo che $a \in R$, è un *divisore di zero* se esiste $b \in R$ e $b \neq 0$ tale che $ab = 0$.

Definizione 2.2. Sia R un anello. Un elemento $r \in R$ si dice *unità* se esiste un $s \in R$ tale che $rs = sr = 1$.

Denotiamo con $U(R)$ (useremo talvolta anche la notazione R^*) l'insieme delle unità di R.

Lemma 2.1. *Sia R un anello. Allora $U(R)$ è un gruppo con la moltiplicazione.*

Dimostrazione. Intanto osserviamo che $1 \in U(R)$, essendo $1 \cdot 1 = 1$. Siano poi $a_1, a_2 \in U(R)$, questo vuol dire che esistono $b_1, b_2 \in R$ tali che $a_1 b_1 = 1$ e $a_2 b_2 = 1$. Ma allora

$$a_1 a_2 b_2 b_1 = a_1 b_1 = 1,$$

e quindi $a_1 a_2 \in U(R)$. Sia poi $a \in U(R)$, allora esiste $b \in R$ tale che $ab = 1 = ba$, e dunque anche $b \in U(R)$, e $b = a^{-1}$. □

Definizione 2.3. Due elementi a, b di un anello A si dicono *associati* se $a = bu$ con $u \in U(A)$.

Definizione 2.4. Un anello commutativo in cui $1 \neq 0$ si dice *dominio di integrità* se non ha divisori di zero diversi da 0. Ossia: se $d_1 d_2 = 0$ implica $d_1 = 0$ o $d_2 = 0$.

Osservazione 2.1. L'insieme degli interi $\mathbb{Z}$ è un dominio di integrità; gli $\mathbb{Z}_n$ sono domini di integrità se e solo se n è primo. Ogni campo è un dominio di integrità. Mostrarlo è molto semplice: se abbiamo $d_1 d_2 = 0$ allora o $d_1 = 0$ e quindi abbiamo finito, o se $d_1 \neq 0$ si moltiplica per il suo inverso (che esiste perché siamo in un campo) e si ha $d_2 = 0$.

Esercizio 2.1. Dimostrare che un dominio di integrità finito è un campo.

Esercizio 2.2. Sia R un anello commutativo con identità, e sia D_0 l'insieme dei divisori di zero. Dimostrare che $D_0 \cap U(R) = \emptyset$.

Esercizio 2.3. Sia R un anello finito. Dimostrare che $R = U(R) \cup D_0$. L'ipotesi di finitezza è necessaria?

3 Omomorfismi

Definizione 3.1. Siano R e S due anelli[3]. Un'applicazione $\phi : R \to S$ si dice essere un *omomorfismo di anelli* se e solo se, per ogni $a, b \in R$

(1) $\phi(a + b) = \phi(a) + \phi(b)$;

(2) $\phi(ab) = \phi(a)\phi(b)$;

[3]Intendiamo come sempre anelli con identità. La definizione di omomorfismo che proponiamo si riferisce ad anelli con identità, cosa che risulta evidente dal punto (3).

(3) $\phi(1_R) = 1_S$.

Definizione 3.2. Sia $\phi : R \to S$ un omomorfismo di anelli. Se ϕ è sia iniettivo che surgettivo si dice essere un *isomorfismo*.

Definizione 3.3. Se $\phi : R \to S$ è un omomorfismo di anelli, definiamo *nucleo* di ϕ l'insieme $\ker \phi = \{a \in R \mid \phi(a) = 0_S\}$, dove 0_S è l'elemento neutro additivo in S.

Lemma 3.1. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora $\ker \phi$ è un sottogruppo additivo di R. Inoltre, se $a \in \ker \phi$ e $r \in R$ allora $ar \in \ker \phi$ e $ra \in \ker \phi$.*

Dimostrazione. Dal momento che ϕ è, in particolare, un omomorfismo di gruppi additivi, la prima parte è già stata dimostrata nella parte dei gruppi.
Siano ora $a \in \ker \phi$ e $r \in R$. Vediamo che $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$, e quindi $ar \in \ker \phi$. Allo stesso modo si dimostra che $ra \in \ker \phi$. □

Esercizio 3.1. Sia $\phi : R \to S$ un omomorfismo. ϕ è iniettivo se e solo se $\ker \phi = \{0_R\}$.

Esercizio 3.2. Sia $\phi : R \to S$ un omomorfismo. Dimostrare che $\phi(R)$ è un sottoanello di S.

4 Ideali di un anello

Definizione 4.1. Un *ideale* I di un anello R è un sottogruppo additivo tale che se $r \in R$ e $h \in I$ allora $rh \in I$ e $hr \in I$.

La proprietà moltiplicativa che caratterizza gli ideali ci dice che I "assorbe" la moltiplicazione a destra e a sinistra per elementi arbitrari dell'anello (la definizione che abbiamo dato è dunque quella di ideale "bilatero": in questo corso non approfondiremo il concetto di ideale non bilatero).

Osservazione 4.1. Un ideale I non è un sottoanello di R, a meno che non sia $I = R$. Infatti se $1 \in I$ allora $I = R$, per la proprietà di "assorbimento".

Osservazione 4.2. Abbiamo visto nel lemma 3.1 che il nucleo di un omomorfismo è un ideale.

Esercizio 4.1. Dimostrare che, se I e J sono due ideali dell'anello R, allora anche $I + J = \{i + j \mid i \in I, j \in J\}$ e $I \cap J$ sono ideali di R.

Esercizio 4.2. Dimostrare che, se I e J sono due ideali dell'anello R, allora anche IJ, l'insieme degli elementi che si possono scrivere come somme finite di elementi della forma ij, con $i \in I$ e $j \in J$, è un ideale di R. Dimostrare inoltre che $IJ \subset I \cap J$ e che l'inclusione può essere stretta.

Dato un ideale I in un anello R denotiamo con R/I l'insieme dei laterali di I in R, considerando I come sottogruppo additivo di R. Detto in altri termini R/I consta dei laterali $a+I$ con $a \in R$, e per i risultati sul capitolo dei gruppi abbiamo automaticamente che R/I è un gruppo additivo, dove la somma si fa nella maniera vista: $(a+I)+(b+I) = (a+b)+I$.
Per dotare R/I di una struttura di anello dobbiamo definire ora una moltiplicazione. Cosa c'è di più naturale che definire $(a+I)(b+I) = ab+I$? Dobbiamo intanto assicurarci che una tale definizione abbia senso:, ossia dobbiamo assicurarci che se $a+I = a'+I$ e se $b+I = b'+I$ allora valga $ab+I = a'b'+I$. Se $a+I = a'+I$ allora $a = a'+i_1$ con $i_1 \in I$; analogamente se $b+I = b'+I$ allora $b = b'+i_2$ con $i_2 \in I$. Ne segue

$$ab = (a'+i_1)(b'+i_2) = a'b' + a'i_2 + b'i_1 + i_1i_2,$$

ed essendo I un ideale di R abbiamo $a'i_2$, $b'i_1$, $i_1i_2 \in I$, e dunque $ab+I = a'b'+I$. Quindi l'operazione di moltiplicazione è ben definita. La verifica di tutti gli assiomi rimanenti per un anello è lasciata come esercizio.

Osservazione 4.3. Abbiamo appena *definito* la moltiplicazione nel quoziente con l'uguaglianza $(a+I)(b+I) = ab+I$. Questa è una definizione, ma in realtà per gli ideali vale che, dal punto di vista insiemistico,

$$(a+I)(b+I) = \{(a+i_1)(b+i_2) \mid i_1, i_2 \in I\} \subseteq ab+I$$

dove l'ultima inclusione può essere stretta. Prendiamo come esempio $\mathbb{Z}$ e l'ideale $I = 6\mathbb{Z}$: si ha $(2+6\mathbb{Z})(4+6\mathbb{Z}) \subsetneq 8+6\mathbb{Z}$. Infatti 14 sta in $8+6\mathbb{Z}$, ma non può essere scritto come $(2+6k)(4+6h)$ con h, k interi. Comunque l'inclusione basta perché $(a+I)(b+I) = ab+I$ sia una buona definizione.

Possiamo quindi enunciare il seguente risultato:

Lemma 4.1. *Siano R un anello e I un suo ideale. Allora R/I è un anello ed è un'immagine omomorfa di R.*

Osserviamo che se R è commutativo anche R/I lo è (il viceversa è falso) e che $1+I$ è l'unità moltiplicativa di R/I. Come nel caso dei gruppi c'è una relazione ben precisa tra R e R/I: se definiamo la proiezione $\pi : R \to R/I$ tale che $\pi(a) = a+I$ allora non è difficile mostrare che π è un omomorfismo e che il suo nucleo è proprio I.

Compiuta la costruzione dell'anello quoziente di un anello rispetto ad un suo ideale possiamo ora trasferire agli anelli il teorema di omomorfismo valido per i gruppi. Poiché la dimostrazione è semplicemente una traduzione parola per parola nel linguaggio degli anelli, enunciamo il *teorema di omomorfismo per anelli* senza dimostrarlo:

Teorema 4.1. *Siano R e S due anelli, e sia $\phi : R \to S$ un omomorfismo di anelli surgettivo. Allora $S \cong R/\ker\phi$. Inoltre, esiste una corrispondenza biunivoca fra l'insieme degli ideali di S e l'insieme degli ideali di R che contengono $\ker\phi$. Questa corrispondenza si ottiene associando ad un ideale I di S l'ideale $\Gamma = \{x \in R | \phi(x) \in I\}$.*

Esercizio 4.3. Con le notazioni del teorema, dimostrare che R/Γ è isomorfo a S/I.

5 Campo delle frazioni di un dominio di integrità

Sia D un dominio di integrità e consideriamo l'insieme

$$\Gamma = \{(a, b) \in D \times D \mid b \neq 0\} \subseteq D \times D.$$

Sull'insieme Γ definiamo la seguente relazione:

$$(a, b) \sim (c, d) \iff ad = bc.$$

Lasciamo al lettore la verifica che quella data è una relazione di equivalenza, commentando però la verifica della proprietà transitiva. Sia $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$: queste due significano $ad = bc$ e $cf = de$. Moltiplicando la prima per f e la seconda per b e ricordando che D è commutativo, possiamo scrivere $afd = bcf = bed$. Ora, D è un dominio di integrità, quindi $(af - be)d = 0$ implica $af = be$ in quanto $d \neq 0$. Dunque $(a, b) \sim (e, f)$ e questa verifica è dipesa in maniera sostanziale dal fatto che D è un dominio.
Denotiamo con K l'insieme delle classi di equivalenza della relazione $\sim$ e indichiamo con $\frac{a}{b}$ la classe di equivalenza della coppia (a, b). Dotiamo K di due operazioni, somma e prodotto:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{e} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd},$$

per ogni $a, b, c, d \in D$ e $b, d \neq 0$.

Esercizio 5.1. Dimostrare che le operazioni di somma e prodotto in K sono ben definite.

Proposizione 5.1. *K dotato di somma e prodotto è un campo.*

Dimostrazione. La verifica è lasciata per esercizio. □

Definizione 5.1. Sia D un dominio di integrità. Allora K costruito come sopra si dice *campo delle frazioni* di D.

Se si compie la costruzione di K partendo dall'anello $\mathbb{Z}$ il campo delle frazioni che si ottiene è $\mathbb{Q}$. Osserviamo anche che in generale il campo K contiene una copia isomorfa a D:

Proposizione 5.2. *Ogni dominio di integrità si può immergere in un campo.*

Dimostrazione. Sia D un dominio di integrità e K il suo campo delle frazioni. Allora abbiamo l'applicazione:

$$\begin{array}{rccc} \phi: & D & \longrightarrow & K \\ & d & \longmapsto & \frac{d}{1}. \end{array}$$

Tale applicazione è un omomorfismo iniettivo di D in K, che quindi contiene una copia isomorfa di D. □

6 Ancora su ideali e anelli quoziente

La domanda che ci poniamo è la seguente: sia R un anello e I un suo ideale, cosa possiamo dire di R/I? Sotto quali condizioni è un dominio oppure un campo?

Definizione 6.1. Sia R un anello e I un suo ideale diverso da R (ossia $1 \notin I$). I si dice *primo* se $rs \in I$ implica $r \in I$ o $s \in I$.

Definizione 6.2. Sia R un anello. Un ideale $I \neq R$ (ossia $1 \notin I$) si dice *massimale* se, quando un ideale J verifica $I \subseteq J \subseteq R$ allora $J = I$ o $J = R$.

Una applicazione del Lemma di Zorn permette di concludere che ogni anello A diverso dallo "stupid ring" $\{0\}$ possiede almeno un ideale massimale. Di ideali massimali in un anello ce ne possono essere anche più di uno, come mostra il eguente esempio.

Esempio 6.1. Sia $R = \mathbb{Z}$ l'anello degli interi e sia I un ideale di R. In particolare I è un sottogruppo additivo di $\mathbb{Z}$ e quindi è della forma $n\mathbb{Z}$. Questi in effetti sono anche ideali dell'anello e quindi $I = (n) = n\mathbb{Z}$.[4] Non è difficile dimostrare che tutti e soli gli ideali massimali sono quelli in cui n è un numero primo e che gli ideali primi sono quelli massimali più l'ideale $\{0\}$.

[4]Sottolineiamo il fatto che nel seguito, per indicare l'ideale generato da un elemento a in un anello commutativo A useremo entrambe le notazioni (a) e aA.

Vediamo cosa accade al quoziente R/I quando I è primo o massimale.

Proposizione 6.1. *Sia R un anello commutativo e I un ideale di R. L'anello R/I è un dominio di integrità se e solo se I è un ideale primo.*

Dimostrazione. ($\Longleftarrow$) Sia I un ideale primo, mostriamo che R/I è un dominio di integrità. Sia

$$(a+I)(b+I) = 0+I = I;$$

Questo equivale a dire che $ab \in I$: allora vale $a \in I$ oppure $b \in I$ perché l'ideale I è primo; quindi $a+I = 0+I$ oppure $b+I = 0+I$.
($\Longrightarrow$) Sia $ab \in I$: se $a \in I$ abbiamo finito; se $a \notin I$ allora andiamo a vedere nel quoziente il prodotto

$$(a+I)(b+I) = ab+I = I.$$

Essendo R/I un dominio di integrità, visto che $a+I \neq 0+I$, deve essere $b+I = I$ ossia $b \in I$. □

Proposizione 6.2. *Sia R un anello commutativo e I un ideale di R. L'anello R/I è un campo se e solo se I è un ideale massimale.*

Dimostrazione. ($\Longleftarrow$) Sia $a+I \neq I$, ossia $a \notin I$. Consideriamo in R l'ideale $I+Ra$: vale $I \subseteq I+Ra \subseteq R$ (non potendo essere $I+Ra = I$ perché $a \notin I$). Ma allora per la massimalità di I deve essere $I+Ra = R$. Dunque $R \ni 1 = j+ra$ per certi $j \in I$ e $r \in R$. Vogliamo mostrare che $r+I$ è l'inverso di $a+I$, infatti:

$$(r+I)(a+I) = ra+I = (1-j)+I = 1+I.$$

($\Longrightarrow$) Supponiamo che R/I sia un campo e sia $I \subseteq J \subseteq R$. Supponiamo che $J \neq I$: questo significa che esiste $j \in J$ ma $j \notin I$. Allora $j+I \neq I$ e quindi ammette inverso perché R/I è un campo, sia $r+I$ tale inverso. Vale:

$$rj+I = (r+I)(j+I) = 1+I.$$

Quindi $1 = rj+i$ con $i \in I$; allora $1 \in J$ poiché $rj, i \in J$. Possiamo dunque concludere che $J = R$. □

Esercizio 6.1. Dimostrare che un anello commutativo che ha come soli ideali $\{0\}$ e se stesso è un campo.

Proposizione 6.3. *Sia R un anello commutativo. Un ideale massimale di R è primo.*

Dimostrazione. Sia I un'ideale massimale, allora R/I è un campo e quindi, in particolare, un dominio di integrità. Di conseguenza I è un ideale primo. □

Esercizio 6.2. Sia $M(n, K)$ l'anello (con identità, ma non commutativo...) delle matrici $n \times n$ a coefficienti nel campo K. Dimostrare che gli unici ideali bilateri sono $\{0\}$ e $M(n, K)$ e che l'ideale $\{0\}$ è massimale ma non è primo.

7 Anelli euclidei, PID, UFD

Nei prossimi paragrafi parleremo di classi particolari di anelli: gli *anelli euclidei*, i *domini a ideali principali* detti PID, "principal ideal domain", e gli *anelli a fattorizzazione unica*, detti UFD, "unique factorization domain".
Anticipiamo sin da ora che questi tre insiemi di anelli sono uno incluso nell'altro.

7.1 Anelli euclidei

Definizione 7.1. Un dominio di integrità D si dice *anello euclideo* se esiste $g : D \setminus \{0\} \to \mathbb{N}$ tale che

(1) per $a, b \in D$, entrambi non zero, vale $g(a) \leq g(ab)$;

(2) per $a, b \in D$ e $b \neq 0$, esistono $q, r \in D$ tali che $a = qb + r$, dove $r = 0$ o $g(r) < g(b)$.

Osserviamo che non si assegna alcun valore a $g(0)$. L'anello $\mathbb{Z}$ è un esempio di anello euclideo (g è la funzione valore assoluto). L'anello dei $K[x]$ dei polinomi a coefficienti in un campo K è euclideo, (g è la funzione che associa ad un polinomio il suo grado).

Lemma 7.1. *In un anello euclideo siano $a, b \neq 0$. Se $b \mid a$ e $a \nmid b$ allora $g(b) < g(a)$.*[5]

Dimostrazione. Sia $a = bc$. Se a non divide b possiamo scrivere che $b = aq + r$ con $r \neq 0$ e $g(r) < g(a)$. Ma d'altra parte $r = b - aq = b - bcq = b(1 - cq)$ e dunque $g(r) \geq g(b)$. Si conclude che $g(a) > g(b)$.□

Lemma 7.2. *In un anello euclideo D vale che $g(1) \leq g(b)$ per ogni $b \in D$ e $g(b) = g(1)$ se e solo $b \in U(R)$.*

Dimostrazione. Per la prima è sufficiente osservare $g(b \cdot 1) \geq g(1)$, e questo mostra che $g(1)$ è il minimo dei gradi degli elementi dell'anello. Per la seconda parte utilizzeremo il fatto che b è invertibile se e solo se $(b) = D$.
($\Longrightarrow$) Supponiamo che $g(b) = g(1)$. Sia $a \in D$, allora $a = qb + r$ con $r = 0$ o $g(r) < g(b)$, ma b ha il grado minimo degli elementi e quindi $r = 0$. Quindi $a \in (b)$

[5] Il concetto di divisibilità negli anelli commutativi è quello ovvio: a divide c se e solo se esiste b tale che $ab = c$.

per ogni $a \in D$ e dunque $D = (b)$.
($\Longleftarrow$) Supponiamo che $b \in U(R)$ allora $(b) = D$ e quindi per ogni $a \in D$ esisterà $r \in D$ tale che $a = rb$. Si deduce che, per ogni $a \in D$, $g(a) \geq g(b)$ e quindi $g(b)$ deve avere il grado minimo: allora $g(b) = g(1)$. $\square$

Introduciamo un importante esempio di anello euclideo, di cui parleremo in maniera più approfondita nel paragrafo 8.

Definizione 7.2. L'insieme $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, viene chiamato *anello degli interi di Gauss.*

Affinché la definizione appena data abbia senso bisogna mostrare che $\mathbb{Z}[i]$ è un anello. Lasciamo questa semplice verifica per esercizio.

Proposizione 7.1. *L'anello $\mathbb{Z}[i]$ è euclideo.*

Dimostrazione. L'anello $\mathbb{Z}[i]$ è un dominio di integrità visto che è un sottoanello del campo $\mathbb{C}$. Scegliamo come grado g la funzione seguente:

$$\begin{array}{rccc} g: & \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ & a+bi & \longmapsto & |a+bi|^2 = a^2+b^2. \end{array}$$

Se $z, w \in \mathbb{Z}[i]$ allora $g(zw) \geq g(z)$: infatti $|zw|^2 \geq |z|^2$ poiché $|w| \geq 1$ (i coefficienti di w sono interi). Adesso siano $z, w \in \mathbb{Z}[i]$ con $w \neq 0$ e consideriamo tutti i multipli di w in $\mathbb{Z}[i]$: questi individuano nel piano complesso un reticolo di quadrati di lato $|w|$ e ogni punto del piano è in uno di questi quadrati (o in più di uno, se si trova al bordo). In particolare z starà in uno di questi quadrati. Sia $Q = w_0 w$ un vertice del quadrato che ha distanza minima da z. Stimiamo questa distanza: nel peggiore dei casi z è nel centro del quadrato, dunque,

$$|z - w_0 w| \leq \frac{|w|}{\sqrt{2}}.$$

Da questo segue che $g(z - w_0 w) \leq \frac{g(w)}{2} < g(w)$ e quindi possiamo prendere w_0 come quoziente della divisione e $z - w_0 w$ come resto. $\square$

Esercizio 7.1. Dimostrare che gli elementi invertibili di $\mathbb{Z}[i]$ sono quattro: 1,-1, i, $-i$. [Si può fare velocemente in maniera diretta, ma ricordiamo che si può usare il Lemma 7.2.]

7.2 Domini a ideali principali

Definizione 7.3. Un ideale I di un anello commutativo A è *principale* se e solo se è generato da un solo elemento, ossia se e solo se esiste $a \in D$ tale che $I = (a) = aD$.[6]

[6] Abbiamo scelto di dare la definizione per anelli commutativi. Nel caso in cui l'anello non sia commutativo, si distinguono gli ideali principali sinistri, destri e bilateri...

Definizione 7.4. Un dominio di integrità si dice a *dominio a ideali principali* (PID) se e solo se tutti i suoi ideali sono principali.

Osservazione 7.1. Consideriamo $F[x, y]$, anello dei polinomi a coefficienti in un campo F e nelle variabili x e y. Questo anello non è a ideali principali in quanto per esempio l'ideale (x, y) generato da $\{x, y\}$ non può essere generato da un solo elemento.

Esercizio 7.2. Consideriamo $\mathbb{Z}[x]$, ossia l'anello dei polinomi a coefficienti in $\mathbb{Z}$. Prendiamo I come insieme dei polinomi $p(x)$ tali che $p(0)$ è pari. Dimostrare che l'ideale I non può essere generato da un solo elemento e dunque $\mathbb{Z}[x]$ non è PID.

Proposizione 7.2. *Sia D un anello euclideo. Allora tutti i suoi ideali sono principali, ossia D è un PID.*

Dimostrazione. Sia I un ideale di D. Se $I = \{0\} = (0)$ non c'è niente da dimostrare. Supponiamo dunque $I \neq \{0\}$, e poniamo

$$m = \min\{g(a) \mid a \in I\},$$

che esiste per il principio del buon ordinamento. Sia $d \in I$, $d \neq 0$, tale che $g(d) = m$; vogliamo mostrare che $I = (d)$.
È ovvio che $dD \subseteq I$, dato che $d \in I$. Viceversa sia $y \in I$, allora esistono $q, r \in D$ tali che $y = qd + r$ con $r = 0$ oppure $g(r) < g(d)$. Osserviamo che $y - qd \in I$, e dunque $r \in I$. Se $r \neq 0$ allora $g(r) < g(d)$ sarebbe in contraddizione con la minimalità di d; dunque $r = 0$ e allora $y \in dD$. Questo mostra che $dD \supseteq I$. □

Osservazione 7.2. Un anello che è PID ma non è euclideo è

$$\mathbb{Z}[\frac{1}{2} + \frac{1}{2}i\sqrt{19}] = \{a + b(\frac{1}{2} + \frac{1}{2}i\sqrt{19}) \mid a, b \in \mathbb{Z}\}$$

Per una dimostrazione di questo fatto chi è interessato può leggere l'articolo di O. Campoli in American Mathematical Monthly, Vol 95, n. 9, 1988, pagg. 868-871.

7.3 Questioni di divisibilità nei PID. Ideali primi e massimali nei PID.

Proposizione 7.3. *Dati $a, b \in D$, dominio a ideali principali, esiste un divisore d di a e b tale che ogni altro divisore comune di a e b lo divide.*

Dimostrazione. Si consideri l'ideale $aD + bD$: tale ideale sarà principale e dunque avrà la forma dD per un certo $d \in D$. Questo d è proprio il divisore cercato. Si ha infatti $a \in dD$ e $b \in dD$ e quindi $d \mid a$ e $d \mid b$. Inoltre $d \in aD + bD$ dunque si può scrivere $d = a\lambda + b\mu$ per certi μ e λ in D. Sia adesso c un divisore comune di a e b, ossia $a \in cD$ e $b \in cD$: quindi $a\lambda + b\mu = d \in cD$ ossia $c \mid d$. □

Definizione 7.5. In un dominio a ideali principali D, dati $a, b \in D$ non entrambi nulli, diciamo che un elemento $d \in D$ che soddisfa le proprietà della proposizione precedente è un *massimo comun divisore* di a e b.

Osservazione 7.3. Nella definizione appena data di massimo comun divisore abbiamo detto *un* massimo comun divisore. In effetti il massimo comun divisore è unico a meno di moltiplicazione per invertibili. Siano d, d' due massimi comuni divisori di a e b in D dominio a ideali principali. Allora vale sia $d \mid d'$ che $d' \mid d$, ossia $d' = dk$ e $d = d'h$. Quindi

$$d' = d'hk \Longrightarrow d'(hk - 1) = 0 \Longrightarrow hk = 1,$$

dove l'ultima implicazione è dovuta al fatto che D è un dominio di integrità. Questo mostra che h e k sono entrambi invertibili.

Osservazione 7.4. Se D è un anello euclideo, per determinare un massimo comun divisore di a e b non entrambi nulli, possiamo utilizzare l'algoritmo di Euclide. La dimostrazione che conoscete per gli interi può essere ripetuta in modo del tutto analogo.

Definizione 7.6. Un elemento $p \neq 0$, $p \notin U(D)$, di un dominio di integrità D si dice *primo* se $p \mid ab$ implica $p \mid a$ o $p \mid b$.

Osservazione 7.5. Questo equivale a dire che p è un elemento primo se e solo se $p \neq 0$ e (p) è un ideale primo.

Definizione 7.7. Un elemento $\pi \neq 0$, $\pi \notin U(D)$, di un dominio di integrità D si dice *irriducibile* se $\pi = \gamma\delta$ implica $\gamma \in U(D)$ o $\delta \in U(D)$.

Nel caso di $\mathbb{Z}$ le due definizioni sono equivalenti, come sappiamo. In generale però questo non è vero. Cominciamo comunque con l'osservare che:

Proposizione 7.4. *Sia D un dominio di integrità. Se $p \in D$ è primo allora p è irriducibile.*

Dimostrazione. Sia p primo e sia $p = \gamma\delta$; allora vale $p \mid \gamma$ o $p \mid \delta$. Supponiamo che $p \mid \gamma$, ossia $\gamma = pk$. Dunque $p = \gamma\delta = pk\delta$, e da questo segue $p(1 - k\delta) = 0$. Dunque, visto che D è un dominio, $k\delta = 1$, ossia $\delta \in U(D)$. □

Perché sia vera l'implicazione inversa non basta che l'anello sia un dominio. Comunque se l'anello è un dominio a ideali principali allora i concetti di elemento primo e elemento irriducibile sono equivalenti. Prima di dimostrarlo premettiamo questa importante osservazione:

Proposizione 7.5. *Sia D un anello a ideali principali. Un ideale $I \neq \{0\}$ di D è primo se e solo se è massimale.*

Dimostrazione. ($\Longleftarrow$) Sappiamo (vedi Proposizione 6.3) che questa implicazione vale in qualsiasi anello commutativo con identità.
($\Longrightarrow$) Sia I un ideale primo diverso da $\{0\}$, allora sarà $I = (p)$ con p elemento primo. Supponiamo $I \subseteq J \subseteq D$ con J ideale: dobbiamo mostrare che $J = D$ o $J = I$. Intanto, dato che D è a ideali principali, avremo $J = (a)$ per qualche $a \in D$, e il fatto che $(a) \supseteq (p)$ implica che $p = ab$ per qualche $b \in D$. Ma essendo p primo si danno due possibilità: o $p \mid a$ o $p \mid b$. Se $p \mid a$ allora $a = pq$ e quindi $p = (pq)b = p(qb)$, da cui deduciamo che b è invertibile; ma allora p è associato ad a e dunque $J = (a) = (p) = I$. Se invece $p \mid b$ allora significa, analogamente, che a è invertibile e dunque $J = (a) = D$. $\square$

Osservazione 7.6. L'ideale $\{0\}$ in un dominio è sempre primo ma non è detto che sia massimale: è massimale se e solo se il dominio è un campo. Per esempio in $\mathbb{Z}$ l'ideale $\{0\}$ non è massimale.

Proposizione 7.6. *Sia D un dominio a ideali principali. Se $p \in D$ è un elemento irriducibile allora l'ideale (p) è massimale.*

Dimostrazione. Sia p irriducibile e consideriamo un ideale J tale che $(p) \subseteq J \subseteq D$. Vale $J = (\gamma)$ per un certo $\gamma \in D$. Dunque possiamo scrivere $p = \gamma\delta$ per un $\delta \in D$. Poiché p è irriducibile, vale che uno fra γ o δ è invertibile. Se γ è invertibile allora $J = D$, se δ è invertibile allora $(p) = J$. $\square$

Corollario 7.1. *Sia D un dominio a ideali principali. Se $p \in D$ è irriducibile allora è primo.*

Dimostrazione. Sia p irriducibile, allora (p) è massimale, dunque (p) è primo, dunque p è un elemento primo. $\square$

Attenzione, quanto abbiamo appena visto non è vero se l'anello non è PID, come mostra il seguente esercizio.

Esercizio 7.3. Consideriamo in $\mathbb{Q}[x, y]$ il polinomio $f(x, y) = x^2 + y^2 - 1$.
a) Dimostrare che f è irriducibile in $\mathbb{Q}[x, y]$.
b) Dimostrare che l'ideale $J = (f)$ non è massimale in $\mathbb{Q}[x, y]$ [Commento: pur essendo generato da un elemento irriducibile!].

7.4 Domini a fattorizzazione unica

Definizione 7.8. Un dominio di integrità D si dice *dominio a fattorizzazione unica* se ogni elemento di $D - \{0\}$ è invertibile oppure si scrive come prodotto di un numero finito di elementi irriducibili di D e tale decomposizione è unica a meno dell'ordine e di elementi associati.

Vogliamo dimostrare che un dominio a ideali principali è un dominio a fattorizzazione unica.

Esercizio 7.4. Sia D un anello euclideo. Dimostrare che D è un dominio a fattorizzazione unica. [Riprodurre la dimostrazione per induzione che avete visto nel caso dell'anello $\mathbb{Z}$ o di $\mathbb{R}[x]$.]

Definizione 7.9. Un anello commutativo R soddisfa la ACC ("ascending chain condition", la "*condizione della catena ascendente*") se non esiste una successione infinita di ideali di R in cui ogni ideale contiene propriamente il precedente.

Osservazione 7.7. Se abbiamo $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots I_n \subseteq \dots$ e R soddisfa la ACC, allora deve esistere m tale che $I_k = I_m$ per ogni $k \geq m$.

Definizione 7.10. Gli anelli commutativi che soddisfano la ACC si dicono *anelli noetheriani*.

Esempio 7.1. L'anello $\mathbb{Z}$ è a ideali principali ed è noetheriano. Prendiamo $I \subset \mathbb{Z}$ ideale, che sarà generato da un certo $n \in \mathbb{Z}$ con $n \geq 0$: se n è primo l'unico ideale di $\mathbb{Z}$ che lo contiene è $\mathbb{Z}$ stesso. Se n non è primo possiamo trovare ideali che contengono $n\mathbb{Z}$ solo prendendo divisori di n, che sono in numero finito. Non ci addentriamo in maggiori dettagli in quanto daremo la dimostrazione che ogni dominio a ideali principali è noetheriano.

Esempio 7.2. L'anello $R = F[x_1, x_2, \dots, x_n, \dots]$ dei polinomi su infinite variabili non è noetheriano. Possiamo infatti esibire una catena di ideali che non soddisfa la ACC:

$$(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \dots, x_n) \subset \cdots .$$

Ma R è un dominio e dunque avrà un campo delle frazioni, che invece è noetheriano[7]. Questo esempio mostra che un sottoanello di un anello noetheriano non necessariamente è noetheriano.

Esempio 7.3. Consideriamo $C(\mathbb{R})$, insieme delle funzioni continue da $\mathbb{R}$ a valori reali. Sia poi $I_1 = \{f \in C(\mathbb{R}) \mid f([-1,1]) = 0\}$ e sia

$$I_n = \left\{ f \in C(\mathbb{R}) \mid f\left(\left[-\frac{1}{n}, \frac{1}{n}\right]\right) = 0 \right\}.$$

Si vede facilmente che I_n è ideale per ogni $n > 0$. Inoltre vale anche $I_i \subsetneq I_{i+1}$ per ogni $i > 0$ e quindi $C(\mathbb{R})$ non è noetheriano.

Teorema 7.1. *Sia R un dominio a ideali principali. Allora R è noetheriano.*

[7] Un campo ha infatti solo due ideali: $\{0\}$ e tutto il campo.

Dimostrazione. Prendiamo una catena di ideali $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ in R infinita e sia

$$I = \bigcup_{i=1}^{\infty} I_i.$$

Non è difficile verificare che I è un ideale di R. Se abbiamo $a, b \in I$ allora $a \in I_i$ e $b \in I_j$: se $i > j$ allora $b \in I_i$ e allora $a + b \in I_j \subseteq I$; analogo per la moltiplicazione esterna. Ora R è un dominio a ideali principali, dunque $I = (c)$ per un certo $c \in D$, ma $c \in I$ e dunque $c \in I_k$ per un certo k. Da ciò segue

$$I = (c) \subseteq I_k \subseteq I$$

dunque deve essere $I = I_k$. In conclusione per $m \geq k$ la catena è stazionaria. □

Teorema 7.2. *Ogni dominio a ideali principali R è un dominio a fattorizzazione unica.*

Dimostrazione. Nella prima parte mostreremo l'esistenza della fattorizzazione in irriducibili per gli elementi non nulli e non invertibili, mentre nella seconda faremo vedere l'unicità. Sia $a \in R$ non nullo e non invertibile, mostriamo dapprima che a ha un fattore irriducibile. Abbiamo due possibilità: o a è irriducibile, e quindi abbiamo il fattore irriducibile voluto, o a non è irriducibile. In questo secondo caso $a = a_1 b_1$ con $a_1, b_1 \notin U(R)$ (cioè si ha una vera fattorizzazione). Dunque $(a) \subseteq (a_1)$, ma non può valere l'uguaglianza altrimenti b_1 sarebbe invertibile: infatti se valesse l'uguale $a_1 = a\gamma$ e quindi

$$a_1(1 - b_1\gamma) = 0 \Longrightarrow b_1\gamma = 1$$

perché siamo in un dominio di integrità. In definitiva $(a) \subsetneq (a_1)$. Per a_1 valgono ancora le stesse possibilità: se a_1 è irriducibile allora abbiamo trovato il fattore, sennò se $a_1 = a_2 b_2$ con $a_2, b_2 \notin U(R)$, e avremo $(a) \subsetneq (a_1) \subsetneq (a_2)$ per ragioni analoghe. Queso procedimento deve avere termime perché R, essendo un dominio a ideali principali, è noetheriano. Alla fine quindi troviamo r tale che a_r è irriducibile e $a_r \mid a$.
Cerchiamo ora una fattorizzazione in prodotto di irriducibile per a. Se a è irriducibile abbiamo finito; se a non è irriducibile, per quanto appena dimostrato, lo scriviamo come $a = p_1 c_1$ con p_1 irriducibile (quindi non invertibile) e $c_1 \notin U(R)$ perché sennò a sarebbe irriducibile. Dunque $(a) \subseteq (c_1)$ e dal fatto che $p_1 \notin U(R)$ segue $(a) \subsetneq (c_1)$. Se c_1 è irriducibile allora $a = p_1 c_1$ è una fattorizzazione in irriducibili di a e abbiamo finito; se c_1 non è irriducibile allora $c_1 = p_2 c_2$ con p_2 irriducibile e $c_2 \notin U(R)$: analogamente a prima $(a) \subsetneq (c_1) \subsetneq (c_2)$. Tale procedimento deve finire e si giunge dunque a scrivere $a = p_1 p_2 \cdots p_s$ con tutti i fattori

irriducibili.
Adesso dobbiamo mostrare l'unicità della fattorizzazione di a. Siano

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

con p_i e q_j irriducibili (ossia primi, dato che R è PID [8]) e $s \geq r$ due fattorizzazioni di a. Prendiamo p_1: notiamo che $p_1 \mid q_1 q_2 \cdots q_s$ e quindi $p_1 \mid q_j$ per un certo j; a meno di riordinare supponiamo $p_1 \mid q_1$. Dunque $q_1 = p_1 u_1$ con $u_1 \in U(R)$ (visto che q_1 è irriducibile):

$$p_1 p_2 \cdots p_r = p_1 u_1 q_2 \cdots q_s$$

Quindi, dato che siamo in un dominio di integrità, $p_2 \cdots p_r = u_1 q_2 \cdots q_s$. Procedendo in modo analogo si otterrà $1 = u_1 \cdots u_r (q_{r+1} \cdots q_s)$, ma se $s > r$ avremmo un assurdo perché i q_j erano irriducibili e quindi non possono essere invertibili. Allora si conclude che $r = s$ e che i p_i e i q_j sono tra loro associati a coppie. □

Esercizio 7.5. Dimostrare che in un UFD i concetti di elemento irriducibile e di elemento primo coincidono.

Osservazione 7.8. Osserviamo che in un dominio a fattorizzazione unica ogni coppia di elementi non entrambi nulli ammette un massimo comun divisore e un minimo comune multiplo (la dimostrazione la lasciamo come esercizio al lettore: si possono usare, proprio come in $\mathbb{Z}$, le fattorizzazioni degli elementi, e scegliere, per esempio per il massimo comun divisore, gli irriducibili che compaiono in entrambe col minimo esponente...il tutto a meno di associati...). Tali massimo comun divisore e minimo comune multiplo saranno definiti a meno di invertibili, ossia a meno di associati.

Esercizio 7.6. Dimostrare che $\mathbb{Z}[x]$ è un UFD.

Osservazione 7.9. Dunque $\mathbb{Z}[x]$ è un esempio di UFD che non è PID.

Senza dimostrazione enunciamo il seguente importante risultato (chi è interessato trova la dimostrazione sull'Herstein, sostanzialmente basata sull'analogo del Lemma di Gauss che avete visto ad Aritmetica nel caso $\mathbb{Z}[x]$):

Teorema 7.3. *Sia R un UFD. Allora anche $R[x]$ è un UFD.*

Corollario 7.2. *Sia R un UFD. Allora l'anello $R[x_1, x_2, \ldots, x_n]$ è un UFD. In particolare, se K è un campo, $K[x_1, x_2, \ldots, x_n]$ è un UFD.*

[8] Stiamo usando il fatto che nei PID i concetti di elemento irriducibile e di elemento primo coincidono. È facile osservare che tali concetti coincidono negli UFD (vedi esercizio 7.5), ma adesso ancora non sappiamo che R è un UFD...

8 Gli elementi primi nell'anello degli interi di Gauss

In questo paragrafo studieremo l'anello degli interi di Gauss; in particolare individueremo quali sono gli elementi primi (ossia gli irriducibili, visto che l'anello è euclideo, PID e UFD...) e scopriremo che questo è collegato ad una interessante osservazione aritmetica: ogni numero primo in $\mathbb{Z}$ che è congruo a 1 modulo 4 si può esprimere come somma di due quadrati di numeri interi.

Lemma 8.1. *Sia $p \in \mathbb{Z}$ un primo dispari che non è primo in $\mathbb{Z}[i]$; allora si può scrivere come somma di due quadrati.*

Dimostrazione. Supponiamo che p non sia primo in $\mathbb{Z}[i]$, allora $p = (a+bi)(c+di)$ con $a^2+b^2 > 1$ e $c^2+d^2 > 1$ affinché i due fattori non siano invertibili. Osserviamo che, essendo $\overline{p} = p$, si ha anche $p = (a-bi)(c-di)$. Allora moltiplicando le due relazioni abbiamo $p^2 = (a^2+b^2)(c^2+d^2)$; visto che $a^2+b^2 > 1$ e $c^2+d^2 > 1$ deve valere $a^2+b^2 = p$ e $c^2+d^2 = p$. □

Lemma 8.2. *Sia $p \in \mathbb{Z}$ un primo della forma $4n+1$. Allora la congruenza $x^2 \equiv -1 \pmod{p}$ ammette soluzione in $\mathbb{Z}$.*

Dimostrazione. Sia $x = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$. Essendo $p-1 = 4n$ nel prodotto precedente compare un numero pari di termini, per cui $x = (-1) \cdot (-2) \cdot (-3) \cdots \left(-\frac{p-1}{2}\right)$. A questo punto osserviamo che

$$\begin{aligned} x^2 &= 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}(-1) \cdot (-2) \cdot (-3) \cdots \left(-\frac{p-1}{2}\right) \equiv \\ &\equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\frac{p+1}{2} \cdots (p-1) \equiv (p-1)! \equiv -1 \pmod{p}, \end{aligned}$$

dove l'ultimo passaggio è il teorema di Wilson[9]. □

Adesso siamo pronti per enunciare il teorema che riguarda i primi $p \equiv 1 \pmod{4}$, ossia quelli nella forma $4n+1$. Ecco il risultato:

Teorema 8.1. *Sia $p \in \mathbb{Z}$ un primo della forma $4n+1$. Allora p non è primo in $\mathbb{Z}[i]$ e $p = a^2+b^2$ con $a, b \in \mathbb{Z}$.*

Dimostrazione. Basta dimostrare che p non è primo in $\mathbb{Z}[i]$, il resto dell'enunciato segue poi dal Lemma 8.1. Scegliamo $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \pmod{p}$ (tale x esiste per il lemma 8.2). Dunque $p \mid x^2+1 = (x-i)(x+i)$, e se p fosse primo

[9] Il teorema di Wilson è di semplice dimostrazione. Prendiamo $(p-1)!$ e consideriamo questo come prodotto di elementi di $\mathbb{Z}_p$: tutti i fattori si elideranno con il proprio inverso (che esiste perché $\mathbb{Z}_p$ è un campo) tranne quelli che coincidono con il proprio inverso. Ma quelli che coincidono con il proprio inverso sono le soluzioni di $x^2 = 1$ in $\mathbb{Z}_p$ e dunque sono solo 1 e -1.

in $\mathbb{Z}[i]$ dovrebbe valere $p \mid (x+i)$ per esempio. Questo vorrebbe dire che esistono $c, d \in \mathbb{Z}$ tali che $p(c+di) = x+i$. Uguagliando le parti immaginarie, dovrebbe valere $pd = 1$, che è assurdo.□

Teorema 8.2. *Sia p un primo dispari della forma $4n+3$. Allora p non può essere scritto come somma di due quadrati.*

Dimostrazione. Supponiamo che $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$. Dato che p è dispari deve essere che a e b sono uno pari e l'altro dispari; senza perdita di generalità supponiamo a pari e b dispari. Allora $a^2 \equiv 0 \pmod 4$ e $b^2 \equiv 1 \pmod 4$ (verificate!) e

$$p = a^2 + b^2 \equiv 1 + 0 \equiv 1 \pmod 4,$$

Ma questo è assurdo perché $p \equiv 3 \pmod 4$. □

Corollario 8.1. *I primi della forma $4n+3$ sono primi in $\mathbb{Z}[i]$.*

Dimostrazione. Sappiamo dal lemma 8.1 che se un primo dispari non è primo in $\mathbb{Z}[i]$ allora può essere scritto come somma di due quadrati. Non potendo i primi della forma $4n+3$ essere scritti in tal modo, ne segue che devono essere primi in $\mathbb{Z}[i]$. □

Riassumendo:

Proposizione 8.1. *Un primo $p \in \mathbb{Z}$ è primo in $\mathbb{Z}[i]$ se e solo se $p \equiv 3 \pmod 4$.*

Dimostrazione. ($\Longleftarrow$) Se $p \equiv 3 \pmod 4$ allora è primo in $\mathbb{Z}[i]$ per il corollario 8.1 precedente, quindi è irriducibile.
($\Longrightarrow$) Supponiamo che $p \equiv 1 \pmod 4$, allora abbiamo dimostrato (teorema 8.1) che p non è primo in $\mathbb{Z}[i]$, quindi non è irriducibile. Se invece $p = 2$ allora $2 = (1+i)(1-i)$, e nessuno dei due fattori è invertibile; quindi 2 non è irriducibile. □

Abbiamo scoperto quali primi di $\mathbb{Z}$ rimangono primi anche in $\mathbb{Z}[i]$: ci poniamo ora il problema di individuare tutti gli elementi primi di $\mathbb{Z}[i]$.

Teorema 8.3. *Tutti e soli gli irriducibili di $\mathbb{Z}[i]$ sono (a meno di associati) i primi di $\mathbb{Z}$ della forma $4n+3$ e gli $z \in \mathbb{Z}[i]$ tali che $g(z) = |z|^2$ è un primo di $\mathbb{Z}$.*

Dimostrazione. ($\Longleftarrow$) Se p è un primo della forma $4n+3$ la proposizione precedente ci dice che è irriducibile in $\mathbb{Z}[i]$. Se $g(z) = p$, con p primo, allora z è irriducibile perché se scriviamo $z = w_1 w_2$ allora, passando ai quadrati delle norme, $p = |w_1|^2 |w_2|^2$ e quindi una delle due norme deve essere uguale a 1, dunque uno dei fattori di z è invertibile.
($\Longrightarrow$) Sia $z \in \mathbb{Z}[i]$ irriducibile. Intanto $z \mid z\overline{z} = g(z) = q_1 \cdot \ldots \cdot q_s$ dove i q_i sono

primi in $\mathbb{Z}$ (ossia abbiamo fattorizzato $g(z)$ in $\mathbb{Z}$). Essendo z primo in $\mathbb{Z}[i]$ si ha che $z \mid q_i$ per un certo i. Deve essere dunque $zw = q_i$ per un certo $w \in \mathbb{Z}[i]$. Se w è invertibile allora z è associato a q_i in $\mathbb{Z}[i]$, e dunque q_i è primo in $\mathbb{Z}[i]$. Ma allora, per la proposizione 8.1, deve essere che q_i è un primo della forma $4n+3$. Quindi z, a meno di associati, è un primo di tale tipo. Se invece w non è invertibile allora $|w|^2 \neq 1$; passando ai quadrati delle norme, si osserva che

$$|z|^2|w|^2 = q_i^2.$$

da cui si deduce $|w|^2 = q_i$ e $|z|^2 = q_i$. □

9 Anelli particolari: esempio di anello non UFD

La nostra attenzione adesso di sposta su anelli del tipo $\mathbb{Z}[\sqrt{n}]$ e $\mathbb{Z}[i\sqrt{n}]$ Gli interi di Gauss che abbiamo visto nel precedente paragrafo appartengono a questa famiglia di anelli.
Intanto osserviamo che se n è un quadrato perfetto allora $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$, quindi in questo paragrafo n non sarà un quadrato perfetto e sarà un elemento in $\mathbb{Z}$. Inoltre adotteremo la notazione per cui per esempio $\mathbb{Z}[\sqrt{-14}]$ significa $\mathbb{Z}[i\sqrt{14}]$.

Questi anelli, come vedremo, in generale non sono euclidei. È possibile comunque definire su di essi una "seminorma" nel modo seguente

$$\begin{array}{rccc} \ell: & \mathbb{Z}[\sqrt{n}] & \longrightarrow & \mathbb{Z} \\ & a+b\sqrt{n} & \longmapsto & a^2-nb^2 \end{array}.$$

Lemma 9.1. *L'applicazione ℓ è moltiplicativa.*

Dimostrazione. Consideriamo $\mathbb{Z}[\sqrt{n}]$ e due elementi $a+b\sqrt{n}$ e $c+d\sqrt{n}$ dell'anello. Intanto

$$\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right) = ac+bdn+(ad+bc)\sqrt{n},$$

da cui

$$\begin{aligned} \ell\left(\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right)\right) &= (ac+bdn)^2 - n(ad+bc)^2 \\ &= a^2c^2+2abcdn+b^2d^2n^2-a^2d^2n-2abcdn-b^2c^2n = \\ &= c^2(a^2-nb^2)-nd^2(a^2-nb^2) = (a^2-nb^2)(c^2-nd^2) = \\ &= \ell\left(a+b\sqrt{n}\right)\ell\left(c+d\sqrt{n}\right), \end{aligned}$$

e abbiamo concluso. □

Lemma 9.2. *Un elemento $z \in \mathbb{Z}[\sqrt{n}]$ è invertibile se e solo se $\ell(z) \in \{1,-1\}$.*

Dimostrazione. ($\Longrightarrow$) Se $z \in \mathbb{Z}[\sqrt{n}]$ ed è invertibile allora $zw = 1$ per qualche $w \in \mathbb{Z}[\sqrt{n}]$. Per il lemma precedente si ha $\ell(z)\ell(w) = \ell(1) = 1$ e dunque $\ell(z) \in \{1, -1\}$.
($\Longleftarrow$) Sia $z = a + b\sqrt{n}$ con $|\ell(z)| = 1$, allora $|a^2 - nb^2| = 1$. Ma allora possiamo scrivere $(a + b\sqrt{n})(a - b\sqrt{n}) = 1$ o $(a + b\sqrt{n})(-a + b\sqrt{n}) = 1$, e in ogni caso z è invertibile. □

Studiando gli anelli di questo tipo ci possiamo imbattere per esempio in anelli che non sono a fattorizzazione unica.

Lemma 9.3. *L'anello $\mathbb{Z}[\sqrt{10}]$ non è un dominio a fattorizzazione unica. Inoltre in $\mathbb{Z}[\sqrt{10}]$ non ogni irriducibile è primo.*

Dimostrazione. Per esempio osserviamo che 6 possiamo scriverlo nei due modi che seguono:

$$(4 + \sqrt{10})(4 - \sqrt{10}) = 6 = 2 \cdot 3,$$

ma dobbiamo essere sicuri che le due fattorizzazioni siano in irriducibili. Mostriamo che 2 e 3 sono elementi irriducibili; se fosse $2 = (a + b\sqrt{10})(c + d\sqrt{10})$ una fattorizzazione senza invertibili allora

$$\ell(a + b\sqrt{10})\ell(c + d\sqrt{10}) = \ell(2) = 4$$

e quindi le due norme a primo membro devono essere entrambe 2 (non può essere che uno delle due è 1 in quanto sennò l'elemento sarebbe invertibile). Ma ciò non è possibile perché $a^2 - 10b^2 = \pm 2$ non ha soluzioni intere. Procedendo in modo analogo per il 3 si ottiene che anche 3 è irriducibile, visto che $a^2 - 10b^2 = \pm 3$ non ha soluzioni intere. L'irriducibilità di $(4 + \sqrt{10})$ e $(4 - \sqrt{10})$ è una conseguenza dei conti già svolti. Tali elementi hanno seminorma 6: dunque per esempio se $(4 + \sqrt{10})$ avesse una fattorizzazione senza invertibili, i due fattori dovrebbero avere seminorma rispettivamente uguale a 2 e a 3, ma abbiamo già visto che nell'anello non ci sono elementi di questo tipo.

Infine osserviamo che 2 è irriducibile ma non è primo. Infatti $2 \mid (4+\sqrt{10})(4-\sqrt{10})$ ma non divide nessuno dei due fattori: se fosse $2(a+b\sqrt{10}) = 4+\sqrt{10}$ allora $\ell(2)|\ell(4 + \sqrt{10})$ che è falso perché 4 non divide 6. □

Nel seguente paragrafo di esercizi potrete trovare altri esempi di anelli non UFD.

10 Esercizi

Esercizio 10.1. I due anelli $\mathbb{Z}[i]/(3)$ e $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ sono isomorfi?

Esercizio 10.2. Decidere se 5 è irriducibile in $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$.

Esercizio 10.3. Fattorizzare $43i - 19$ in prodotto di irriducibili in $\mathbb{Z}[i]$.

Esercizio 10.4. Mostrare che $\mathbb{Z} \times \mathbb{Z}$ non è un dominio di integrità ma i suoi ideali sono principali.

Esercizio 10.5. Determinare gli invertibili di $\mathbb{R}[x]/(x^2 + 1)$.

Esercizio 10.6. Determinare i divisori di zero e gli invertibili in $\mathbb{Q}[x]/(x^2 - 1)$.

Esercizio 10.7. Sia R un dominio, sia $a \in R$ e sia $\phi : R[x] \to R$ l'*omomorfismo di valutazione* in a, quello che manda $p(x)$ in $p(a)$. Dimostrare che $R[x]/(x - a) \cong R$.

Esercizio 10.8. Dimostrare che $\mathbb{Z}[x]/(x - 2, 3) \cong \mathbb{Z}_3$.

Esercizio 10.9. Siano $f(X) = X^4 + X^3 - X - 1$, $g(X) = X^{10} - X^7$ e I l'ideale $(f(X), g(X))$. Determinare

(i) gli ideali massimali di $\mathbb{R}[X]$ che contengono I;
(ii) un ideale massimale di $\mathbb{Z}[X]$ che contenga I;
(iii) un ideale primo non massimale di $\mathbb{Z}[X]$ che contenga I.

Esercizio 10.10. Trovare tutte le rappresentazioni di 2425 come somma di due quadrati.

Esercizio 10.11. Sia A un anello euclideo.
(i) Dimostrare che esiste $x \in A - U(A)$ tale che la restrizione della proiezione canonica $\pi : A \to A/(x)$ all'insieme $U(A) \cup \{0\}$ sia surgettiva.
(ii) Per un tale x, è vero che (x) è massimale ?
iii) Trovare un tale x nei casi $A = \mathbb{Z}, \mathbb{R}[x], \mathbb{Z}[i]$.

Esercizio 10.12. Si può dare all'anello $K[[x]]$ (le *serie* formali nella variabile x sul campo K) una struttura di anello euclideo?

Esercizio 10.13 (L'anello degli interi di Eisenstein)**.** Sia $\omega \neq 1$ una radice cubica di 1. È possibile dare una struttura euclidea all'*anello degli interi di Eisenstein* $\mathbb{Z}[\omega]$?

Esercizio 10.14. Si consideri l'anello $D = \{x \in Q \mid \exists n \in \mathbb{Z} \text{ tale che } 10^n x \in Z\}$.
(1) È un dominio?
(2) Sia I un ideale di D non nullo. Descrivere $I \cap \mathbb{N}_0$;
(3) Dimostrare che D è un dominio a ideali principali;
(4) Dimostrare che $D[x]$ non è un dominio a ideali principali.

Esercizio 10.15. È vero o falso che la fattorizzazione $\sqrt{6}\sqrt{6} = 2 \cdot 3$ dimostra che $\mathbb{Z}[\sqrt{6}]$ non è UFD ? [gli elementi coinvolti sono irriducibili?]

Esercizio 10.16. Trovare in $\mathbb{Z}[i\sqrt{6}]$:
a) un irriducibile che non è primo;
b) due elementi non nulli a, b tali che $MCD(a, b)$ non esiste;
c) due elementi a, b tali che $MCD(a, b) = 1$ ma non vale Bezout, ossia non esistono $\lambda, \mu \in \mathbb{Z}[i\sqrt{6}]$ tali che $a\lambda + b\mu = 1$.

Esercizio 10.17. Dimostrare che $\mathbb{Z}[\sqrt{2}]$ e $\mathbb{Z}[\sqrt{3}]$ non sono isomorfi.

Esercizio 10.18. Sia A un anello commutativo e siano $a, b \in A$. Dimostrare che se l'ideale $(a) + (b)$ è principale allora lo è anche l'ideale $(a) \cap (b)$.

Esercizio 10.19. Dimostrare che l'ideale $(2, 1 + i\sqrt{3})$ in $\mathbb{Z}[i\sqrt{3}]$ non è principale.