Matematik, KTH
Bengt Ek
januari 2014 (ett tryckfel på sid. 10 rättat 14 april 2015)

Material till kursen
SF1662, Diskret matematik för CLGYM1, TSVDK2:

Mer om faktorisering

Inledning. Är alla ringar som $\mathbb{Z}$?

De första matematiska objekt vi studerade i den här kursen var heltalen, elementen i $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Vi har nu kommit till det abstrakta begreppet **ring** och sett att $\mathbb{Z}$ är en ring. Det betyder ju att allt som är sant i alla ringar (allt som kan visas från axiomen för ringar) också gäller för heltalen. Däremot betyder det inte att allt som är sant för heltalen $\mathbb{Z}$ säkert också gäller i alla ringar.

T.ex. är multiplikationen, $\cdot$, kommutativ i $\mathbb{Z}$ ($ab = ba$ för alla $a, b \in \mathbb{Z}$), men det behöver den inte vara i en ring. Men inte ens om vi begränsar oss till kommutativa ringar kan vi vara säkra på att alla $\mathbb{Z}$:s egenskaper gäller.

En viktig egenskap för heltal gäller faktorisering. Vi har lärt oss att i $\mathbb{Z}_+ = \{1, 2, 3, \dots\}$ gäller **entydig faktorisering**, dvs att varje positivt heltal kan skrivas som en produkt av primtal på (bortsett från ordningen mellan faktorerna) precis ett sätt (1 är "den tomma produkten", produkten av inga primtal alls). Vi skall uttrycka det som en egenskap för hela $\mathbb{Z}$ och se om det möjligen gäller i alla kommutativa ringar med etta, eller kanske bara i vissa av dem.

Vi påminner oss att **en kommutativ ring med etta $(R, +, \cdot)$** kan definieras som en struktur som uppfyller att $(R, +)$ är en abelsk grupp (med identitetselement 0), operationen $\cdot$ är associativ och kommutativ och har ett identitetselement 1 på R och $\cdot$ är distributiv med avseende på $+$, dvs

För alla $s, t, u \in R$ gäller

$$s + t \in R \qquad s \cdot t \in R$$
$$(s + t) + u = s + (t + u) \qquad (s \cdot t) \cdot u = s \cdot (t \cdot u)$$
$$s + t = t + s \qquad s \cdot t = t \cdot s$$
$$s + 0 = s \qquad s \cdot 1 = s$$

det finns ett $-s \in R$ med

$$s + (-s) = 0$$

$$s \cdot (t + u) = s \cdot t + s \cdot u$$

(Eftersom det förekommer att man definierar ringar utan krav på att det finns ett identitetselement för multiplikationen, skriver vi ibland för att vara tydliga "med etta", för att ange att den aktuella ringen verkligen har ett sådant.)

Om entydig faktorisering i ringar

Låt nu $(R, +, \cdot)$ vara en kommutativ ring med etta. För att undvika underligheter antar vi också att $0 \neq 1$ i R (annars skulle R bara ha ett element). Vi skall se vad vi bör mena med entydig faktorisering i R.

I $\mathbb{Z}_+$ handlar det om att skriva elementen entydigt som produkter av primtal, där ett tal p är ett primtal omm det har precis två delare (1 och p själv). I $\mathbb{Z}$ skulle definitionen av primtal få ändras till att p har precis fyra delare (± 1 och $\pm p$), men då blir för ett sådant p både p och $-p$ primtal. I fallet $\mathbb{Z}$ kan vi förstås lägga till i definitionen att primtal är positiva, men i vår allmänna ring R finns inte säkert någon motsvarighet till "positiv". Om vi å andra sidan tillåter att både p och $-p$ är primtal blir faktoriseringen inte entydig, t.ex. vore ju $6 = 2 \cdot 3 = (-2)(-3)$.

Definition: En **enhet** (eng. unit) $u \in R$ är detsamma som ett inverterbart element, dvs u är en enhet precis om det finns $u^{-1} \in R$ så att $uu^{-1} = 1$.

Liksom förut låter vi $U(R)$ (eller bara U) beteckna mängden av enheter i R.

I varje ring R är $1 = 1^{-1}$, så $1 \in U(R)$.
I början av kursen visade vi att $U(\mathbb{Z}_m) = \{x \in \mathbb{Z}_m \mid \text{sgd}(x, m) = 1\}$.
Tydligen är $U(\mathbb{Z}) = \{1, -1\}$.

I varje ring R är $(U(R), \cdot)$ en grupp. Om R är en **kropp** (dvs om $(R \setminus \{0\}, \cdot)$ är en abelsk grupp) är $U(R) = R \setminus \{0\}$.

Att p och $-p$ i $\mathbb{Z}$ vad gäller faktorisering "väsentligen" är samma svarar i allmänt R mot

Definition: Två element $x, y \in R$ kallas **associerade element** om det finns ett $u \in U(R)$ sådant att $x = uy$.

I $\mathbb{Z}$ är x och y alltså associerade precis om $x = y$ eller $x = -y$.

Relationen att vara associerade element är en ekvivalensrelation (reflexiv eftersom 1 är en enhet, symmetrisk eftersom u^{-1} är en enhet om u är det, transitiv eftersom $u_1 u_2$ är en enhet om u_1 och u_2 båda är det), så R delas in i ekvivalensklasser av associerade element. $U(R)$ är alltid en av klasserna.

(Om $x \in R$, är mängden av element som är associerade med x precis xU. Den liknar en sidoklass i en grupp, men eftersom $(R, \cdot)$ inte är en grupp kan xU och yU innehålla olika många element. Det gäller dock alltid att $|xU| \leq |U|$.
I t.ex. $\mathbb{Z}_6$ är $U = \{1, 5\}$. Klasserna av associerade element är $\{0\}$, $\{1, 5\}$, $\{2, 4\}$ och $\{3\}$.)

I R kan vi nu definiera motsvarigheten till att vara $\pm$ ett primtal i $\mathbb{Z}$,

Definition: Ett element $\pi \in R$ är ett **irreducibelt element** i R omm det för varje faktorisering i R, $\pi = x \cdot y$, gäller att precis en av x och y tillhör $U(R)$.

I $\mathbb{Z}$ är de irreducibla elementen alla p och $-p$, där p är ett primtal.

I $\mathbb{Z}_6$ finns inga irreducibla element, ty alla elementen kan skrivas som produkter antingen utan enheter ($0 = 0 \cdot 0$, $2 = 2 \cdot 4$, $3 = 3 \cdot 3$, $4 = 2 \cdot 2$) eller med två enheter ($1 = 1 \cdot 1$, $5 = 1 \cdot 5$).

En enhet u är aldrig irreducibel, ty $u = 1 \cdot u$, en produkt av två enheter.

Om ringen R är en kropp innehåller den inga irreducibla element, ty alla element är då enheter eller $0 (= 0 \cdot 0)$.

Kravet på entydig faktorisering kan nu formuleras så,

Definition: Ringen R (kommutativ med etta) sägs ha **entydig faktorisering** omm

(1) varje element $x \in R$ som inte är 0 eller en enhet kan skrivas som

$$x = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_k,$$

där $k \in \mathbb{Z}_+$ och $\pi_1, \pi_2, \ldots, \pi_k$ är irreducibla i R och

(2) om

$$\pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_k = \pi'_1 \cdot \pi'_2 \cdot \ldots \cdot \pi'_\ell,$$

där alla π_i, π'_j är irreducibla, så är $k = \ell$ och man kan numrera om π_i:na så att för alla $i = 1, \ldots, k$ är π_i och π'_i associerade.

Med denna definition har $\mathbb{Z}$ faktiskt entydig faktorisering, trots att t.ex.

$$-20 = 2 \cdot (-5) \cdot 2 = 5 \cdot 2 \cdot (-2).$$

Genom att ordna om faktorerna i den första produkten kan den ju skrivas $(-5) \cdot 2 \cdot 2$ och $\langle -5, 5\rangle$, $\langle 2, 2\rangle$ och $\langle 2, -2\rangle$ är associerade par i $\mathbb{Z}$.

$\mathbb{Z}_6$ har inte entydig faktorisering, ty t.ex. 2 är varken 0, en enhet eller en produkt av irreducibla element. Om R är en kropp har den entydig faktorisering (på ett trivialt sätt), varje element är ju 0 eller en enhet.

De gaussiska heltalen $\mathbb{Z}[i]$ och polynomen $F[x]$

Vi studerar här två huvudexempel (utöver $\mathbb{Z}$) på ringar och skall snart visa att de båda har entydig faktorisering.

Det ena exemplet är **de gaussiska heltalen**

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\},$$

dvs alla komplexa tal vars real- och imaginärdelar båda är heltal. $\mathbb{Z}[i]$ är tydligen en kommutativ ring med etta (med vanlig addition och multiplikation för komplexa tal och talet 0 som 0 och talet 1 som 1). $U(\mathbb{Z}[i]) = \{1, i, -1, -i\}$ (för alla $z \in \mathbb{Z}[i] \setminus \{0\}$ är ju $|z| \geq 1$ och $|z^{-1}| = |z|^{-1}$, så fler inverterbara element finns inte i $\mathbb{Z}[i]$). Exempel på associerade element i $\mathbb{Z}[i]$ är $3 + 4i$ och $4 - 3i$. De irreducibla elementen i $\mathbb{Z}[i]$ kallas **gaussiska primtal**. En del "vanliga primtal" (dvs från $\mathbb{Z}_+$) är gaussiska primtal och andra inte. T.ex. är $2 = (1+i)(1-i)$, 3 ett gaussiskt primtal och $5 = (2+i)(2-i)$. $\mathbb{Z}[i]$ har som sagt entydig faktorisering och vi skall om några sidor se hur man kan faktorisera (inte alltför stora) element i $\mathbb{Z}[i]$.

Vårt andra huvudexempel på ringar är **polynomen över en kropp F**

$$F[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid n \in \mathbb{N},\ a_i \in F \text{ för } i = 0, 1, \ldots, n\},$$

alla polynom med koefficienter i F.

$F[x]$ är en kommutativ ring med etta (med $+$, $\cdot$ som vanligt för polynom med 0, 1 polynomen med alla koefficienter 0 respektive $a_0 = 1$, övriga a_i alla 0). Enheterna i $F[x]$ utgörs av de konstanta nollskilda polynomen (dvs de med $a_0 \neq 0$, övriga a_i alla 0) och två polynom $f(x)$ och $g(x)$ är associerade precis om $f(x) = a \cdot g(x)$ för ett $a \in F \setminus \{0\}$. Vi återkommer till $F[x]$:s irreducibla element.

En ring utan entydig faktorisering

Ett standardexempel på en ring som inte har entydig faktorisering (trots att den har gott om irreducibla element) är

$$\mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b \mid a, b \in \mathbb{Z}\}$$

med $+$, $\cdot$, 0, 1 som vanligt för komplexa tal. $\mathbb{Z}[i\sqrt{5}]$ är sluten under multiplikation (ty $(a_1 + i\sqrt{5}b_1)(a_2 + i\sqrt{5}b_2) = (a_1a_2 - 5b_1b_2) + i\sqrt{5}(a_1b_2 + b_1a_2)$) och med definitionen av kommutativ ring med etta ser man att $\mathbb{Z}[i\sqrt{5}]$ är en.

Om $z = a + i\sqrt{5}b \neq 0$ är $|z|^2 = a^2 + 5b^2 \geq 1$, så om $z \in \mathbb{Z}[i\sqrt{5}]$ är inverterbar måste $|z| = 1$ (ty $|z^{-1}| = |z|^{-1}$) dvs $b = 0$ och $a = \pm 1$, dvs $U(\mathbb{Z}[i\sqrt{5}]) = \{1, -1\}$ och x, $y \in \mathbb{Z}[i\sqrt{5}]$ är associerade omm $x = y$ eller $x = -y$. Vi ser också att om $z \in \mathbb{Z}[i\sqrt{5}]$ inte är 0 eller en enhet är $|z|^2 (= a^2 + 5b^2) \geq 4$ (använder vi strax).

För att visa att $\mathbb{Z}[i\sqrt{5}]$ inte har entydig faktorisering noterar vi först att

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

och att 6 varken är 0 eller en enhet. Eftersom $1+i\sqrt{5}$ varken är associerad med 2 eller med 3, räcker det att visa att 2, 3, $1+i\sqrt{5}$, $1-i\sqrt{5}$ alla är irreducibla. Om $z, z_1, z_2 \in \mathbb{Z}[i\sqrt{5}]$ och $z = z_1 \cdot z_2$ gäller $|z|^2 = |z_1|^2|z_2|^2$ och om varken z_1 eller z_2 är 0 eller en enhet är $|z|^2 \geq 4 \cdot 4 = 16$. Men $|2|^2 = 4$, $|3|^2 = 9$, $|1 \pm i\sqrt{5}|^2 = 6$, så 2, 3, $1 \pm i\sqrt{5}$ är alla irreducibla och $\mathbb{Z}[i\sqrt{5}]$ har inte entydig faktorisering.

Euklidiska ringar

Låt oss nu betrakta ringar med en motsvarighet till division med rest:

Definition: Om R är en kommutativ ring med etta är en **euklidisk valuation på R** en funktion $\nu : R \to \mathbb{N} \cup \{-\infty\}$ sådan att

(1) $\nu(s) \in \mathbb{N}$ om $s \in R \setminus \{0\}$ och $\nu(0) = -\infty$,
(2) för alla $s, d \in R$, $d \neq 0$, finns q, $r \in R$ med $s = qd + r$ och $\nu(r) < \nu(d)$,
(3) för alla $s, t \in R \setminus \{0\}$ gäller $\nu(s) \leq \nu(st)$.

(Symbolen $-\infty$ uppfyller förstås $-\infty < n$ för alla $n \in \mathbb{N}$.)

Definition: En **euklidisk ring** är en kommutativ ring med etta som har en euklidisk valuation.

I själva verket är följande sant i varje euklidisk ring:

$$(3') \text{ för alla } s, t \in R \setminus \{0\} \text{ gäller } \nu(s) \begin{cases} = \nu(st) & \text{om } t \in U(R), \\ < \nu(st) & \text{om } t \notin U(R). \end{cases}$$

(3′) följer ur (1)–(3), ty
om $t \in U(R)$: $\nu(st) \leq \nu(stt^{-1}) = \nu(s) \leq \nu(st)$ (båda '$\leq$' enligt (3)),
om $t \notin U(R) \cup \{0\}$: tag $q, r \in R$ med $s = qst + r$, $\nu(r) < \nu(st)$
(sådana q, r finns enligt (2), ty $st \neq 0$ om $s, t \neq 0$ (enligt (1), (3))),
så $r = (1 - qt)s$ och $\nu(s) \leq \nu(r) < \nu(st)$ ($1 - qt \neq 0$, ty $t \notin U(R)$).

Om $x, y \in R$, en ring, och $x, y \neq 0$, $xy = 0$ kallas x och y **nolldelare**. I en euklidisk ring finns som vi såg inga nolldelare.

Med (1)–(3') får man att för ν:s värden i en godtycklig euklidisk ring gäller:

- Det minsta ν-värdet ($-\infty$) antas bara av $0 \in R$.
- Det näst minsta ν-värdet (det minsta i $\mathbb{N}$) antas av alla enheter och bara av dem.
- Associerade element har samma ν-värden.
- Om $s, t \in R \setminus \{0\}$ och $t \notin U(R)$, är $\nu(s) < \nu(st)$.

När vi nu skall visa att varje euklidisk ring har entydig faktorisering, kan vi nästan kopiera definitioner och satser från behandlingen av $\mathbb{Z}$ (och tar det kortfattat):

Definition: Om $d, m \in R$, en ring, betyder "$\boldsymbol{d}$ **delar** $\boldsymbol{m}$", "d är en delare till m", "m är en multipel av d" osv, med symboler $\boldsymbol{d \mid m}$, att det finns ett $q \in R$ sådant att $m = qd$.

Exempel: $1 + 3i \mid 4 + 2i$ i $\mathbb{Z}[i]$, ty $4 + 2i = (1 - i)(1 + 3i)$.
$2x^2 + 2x + 1 \mid x^5 + x^4 + x^3 + 2x + 2$ i $\mathbb{Z}_3[x]$,
ty $x^5 + x^4 + x^3 + 2x + 2 = (2x^3 + x + 2)(2x^2 + 2x + 1)$ i $\mathbb{Z}_3[x]$.

Definition: Om $x, y \in R$, en ring, är en **största gemensam delare**, sgd (eng. gcd), till x och y ett $d \in R$ sådant att

i) $d \mid x$, $d \mid y$ gemensam delare
ii) $c \mid x$, $c \mid y \Rightarrow c \mid d$ "störst"

Sats: För alla $s, t \in R$, en euklidisk ring, finns (minst) en största gemensam delare $\boldsymbol{d = \text{sgd}(s, t)}$ och $\boldsymbol{d = as + bt}$ för några $a, b \in R$. Alla sgd:er till s och t är associerade.

Element som är associerade till en sgd är också en sgd. Om man vill ha sgd entydigt definierad kan man kräva att den är ≥ 0 i $\mathbb{Z}$, att den är 0 eller har realdel > 0 och imaginärdel ≥ 0 i $\mathbb{Z}[i]$ och att den är 0 eller har koefficienten 1 för högstagradstermen i $F[x]$, men eftersom vi inte har något "allmänt" sätt att välja sgd entydigt låter vi det finnas flera, men associerade, sgd:er till s, t.

s och t har samma gemensamma delare som t och $s - qt$, $q \in R$, så $\boldsymbol{\text{sgd}(s, t) = \text{sgd}(t, s - qt)}$ (om någon av dem finns). Genom att upprepa det kommer man till $\text{sgd}(d, 0) = d$, så d, a, b fås med **Euklides algoritm:**

$$
\begin{array}{ll}
s = q_1 t + r_1 & 0 < \nu(r_1) < \nu(t) \\
t = q_2 r_1 + r_2 & 0 < \nu(r_2) < \nu(r_1) \\
r_1 = q_3 r_2 + r_3 & 0 < \nu(r_3) < \nu(r_2) \\
\quad \vdots & \qquad\qquad \text{som ger } \boldsymbol{\text{sgd}(s, t) = r_{k-1}}. \\
r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} & 0 < \nu(r_{k-1}) < \nu(r_{k-2}) \\
r_{k-2} = q_k r_{k-1} + 0 &
\end{array}
$$

Näst sista ekvationen ger $d = r_{k-1}$ uttryckt i r_{k-2} och r_{k-3}, r_{k-2} uttrycks med ekvationen före i r_{k-3} och r_{k-4} etc, slutligen $d = as + bt$ för några $a, b \in R$.

Exempel: $\text{sgd}(2 + 4i, 5 - 5i) = 1 - 3i$, $(2 + 4i = (1 - 3i)(-1 + i)$, $5 - 5i = (1 - 3i)(2 + i))$
och $1 - 3i = i(2 + 4i) + 1(5 - 5i)$.
$\text{sgd}(x^4 + 2x^3 + 2x + 2, x^3 + x + 2) = x^2 + 2x + 2$ i $\mathbb{Z}_3[x]$,
$(x^4 + 2x^3 + 2x + 2 = (x^2 + 1)(x^2 + 2x + 2)$, $x^3 + x + 2 = (x + 1)(x^2 + 2x + 2))$
och $x^2 + 2x + 2 = 2(x^4 + 2x^3 + 2x + 2) + (x + 2)(x^3 + x + 2)$.

Följdsats: Om $d, s, t \in R$, en euklidisk ring, sådana att $d \mid st$ och $\text{sgd}(d, s)$ är enheter (dvs d och s är **relativt prima**), så $d \mid t$.

(Ty om $1 = ad + bs$ för några a, $b \in R$, så $t = atd + bst = (at + bq)d$, så $d \mid t$.)

$\mathbb{Z}$, $\mathbb{Z}[i]$ och $F[x]$ är euklidiska

Vi har ovan tagit $\mathbb{Z}[i]$ och $F[x]$ som exempel för att illustrera euklidiska ringar. Låt oss visa att de, liksom $\mathbb{Z}$, verkligen är sådana.

$\mathbb{Z}$ är en euklidisk ring med den euklidiska valuationen $\nu(n) = |n|$ för $n \neq 0$, $\nu(0) = -\infty$. Vi vet att $\mathbb{Z}$ är en kommutativ ring med etta, så vi skall bara verifiera att detta ν är en euklidisk valuation på $\mathbb{Z}$ (dvs kontrollera (1)–(3) i definitionen). (1) är klar, (2) följer ur divisionsegenskapen för $\mathbb{Z}$ (visad i början av kursen) och (3) är att $|s| \leq |st|$ då $s, t \in \mathbb{Z} \setminus \{0\}$, vilket ju gäller eftersom $|st| = |s||t|$ och $|s|$, $|t| \geq 1$ för sådana s, t.

$\mathbb{Z}[i]$ är en euklidisk ring med den euklidiska valuationen $\nu(z) = |z|^2$ för $z \neq 0$, $\nu(0) = -\infty$. Vi vet att $\mathbb{Z}[i]$ är en kommutativ ring med etta, så liksom för $\mathbb{Z}$ räcker det att visa att detta ν är en euklidisk valuation på $\mathbb{Z}[i]$. (1) är klar (då $z \neq 0$ tog vi $\nu(z) = |z|^2$, inte $|z|$, för att få naturliga tal som värden). För (2) kan vi ta $q \in \mathbb{Z}[i]$ så att $|\frac{s}{d} - q|^2 \leq \frac{1}{2}$ (q kan ha real- och imaginärdelar som närmaste heltal till $\frac{s}{d}$:s), det ger $\nu(s - qd) \leq \frac{1}{2}\nu(d) < \nu(d)$ eftersom $\nu(d) \geq 1$. (3) är analogt med det för $\mathbb{Z}$.

Exempel: Med $s = 31 + 4i$, $d = 4 + 3i$ får man $\frac{s}{d} = \frac{(31+4i)(4-3i)}{25} = \frac{136}{25} - \frac{77}{25}i$ och tar $q = 5 - 3i$. Det ger $r = s - qd = 31 + 4i - (5 - 3i)(4 + 3i) = 2 + i$.

$F[x]$ är en euklidisk ring med den euklidiska valuationen $\nu(f(x)) = \deg f(x)$, graden av polynomet $f(x)$ (det största n med $a_n \neq 0$ om $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in F[x] \setminus \{0\}$ och $\deg f(x) = -\infty$ om $f(x) = 0$, nollpolynomet). Vi vet att $F[x]$ är en kommutativ ring med etta, så liksom för $\mathbb{Z}$ och $\mathbb{Z}[i]$ räcker det att visa att detta ν är en euklidisk valuation på $F[x]$. (1) är klar. (2) uttrycker att man alltid kan dividera med nollskilda polynom och få en rest av grad lägre än det man dividerade med (när man visar detta för reella polynom använder man bara att koefficienterna ligger i en kropp). (3) följer av att $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ (och att $\deg f(x) \geq 0$ om $f(x) \neq 0$).

Exempel: Med $s = 2x^3 + 2x^2 - 2x + \frac{5}{2}$, $d = 2x^2 + 3x - 1$ i $\mathbb{Q}[x]$ ger division att $2x^3 + 2x^2 - 2x + \frac{5}{2} = (x - \frac{1}{2})(2x^2 + 3x - 1) + \frac{1}{2}x + 2$, dvs $q = x - \frac{1}{2}$ och $r = \frac{1}{2}x + 2$.

Entydig faktorisering i euklidiska ringar

Egenskaperna som vi konstaterat för euklidiska ringar gör att beviset för entydig faktorisering nästan blir identiskt med det för $\mathbb{Z}$.

Först existensen av faktorisering i irreducibla element:

Sats: Om R är en euklidisk ring kan varje $s \in R$ som inte är 0 eller en enhet skrivas som $s = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_k$, där $k \in \mathbb{Z}_+$ och $\pi_1, \pi_2, \ldots, \pi_k$ är irreducibla i R.

Ty: Induktion över $\nu(s)$. Antag att påståendet stämmer för alla $t \in R$ med $\nu(t) < a$ och låt $\nu(s) = a$. Om s är irreducibelt, en enhet eller 0 är saken klar, annars finns $s_1, s_2 \in R \setminus U$ med $s = s_1 s_2$. Då är $\nu(s_i) < \nu(s) = a$ så enligt induktionsantagandet är de, och därmed s, produkter av irreducibla element.

Sats: Om π är ett irreducibelt element i en euklidisk ring R och $\pi \mid s_1 s_2 \ldots s_n$ i R, så $\pi \mid s_i$ för något $i \in \{1, 2, \ldots n\}$.

Ty: Induktion över antalet faktorer, n. Om $\pi \nmid s_1$ är $\text{sgd}(\pi, s_1)$ en enhet (alla π:s delare är antingen associerade med π (och inte delare till s_1) eller enheter), så enligt "följdsatsen" ovan $\pi \mid s_2 s_3 \ldots s_n$, en produkt med färre faktorer.

Återstår att visa entydigheten.

Sats: Om $\pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_k = \pi'_1 \cdot \pi'_2 \cdot \ldots \cdot \pi'_\ell$, där alla π_i, π'_j är irreducibla, så är $k = \ell$ och man kan numrera om π_i:na så att för alla $i = 1, \ldots, k$ är π_i och π'_i associerade.

Ty: $\pi_1 \mid \pi'_1 \cdot \pi'_2 \cdot \ldots \cdot \pi'_\ell$, så (enligt den förra satsen) $\pi_1 \mid \pi'_j$ för något $j \in \{1, 2, \ldots, \ell\}$. Men då är π_1 och π'_j associerade (π'_j är irreducibelt och $\pi_1 \notin U(R)$). Dividera med π_1 i båda leden (och låt enheten $\frac{\pi'_j}{\pi_1}$ ingå i ett kvarvarande π' (om inga finns är $\pi_1 = \pi'_j$)). Då återstår $\pi_2 \cdot \ldots \cdot \pi_k = \pi'_1 \cdot \ldots \cancel{\pi'_j} \ldots \cdot \pi'_\ell$ och genom att upprepa (dvs med induktion) tills π_i:na tar slut får man det önskade.

Tillsammans ger de den viktiga

Sats: Varje euklidisk ring har entydig faktorisering.

Gaussiska primtal och faktorisering i $\mathbb{Z}[i]$

Vi vet alltså nu att ringen $\mathbb{Z}[i]$ har entydig faktorisering.

De irreducibla elementen i $\mathbb{Z}[i]$ kallas som redan nämnts **gaussiska primtal**. Exempel på gaussiska primtal är $1 + i$, 3, $2 - i$, $-2 + 3i$, 11, $13 + 8i$, 31 och $20 + 13i$, men $4 + 3i = (2 - i)(1 + 2i) = i(2 - i)^2$, $5 + i = (1 + i)(3 - 2i)$, $17 = (4+i)(4-i)$, $7+4i = (2-i)(2+3i)$, $65 = (2+i)(2-i)(3+2i)(3-2i)$, $597-74i = (2 + i)(11 + 6i)(10 - 19i)$, $373 = (18 + 7i)(18 - 7i)$.

Hur kan man känna igen gaussiska primtal och hur gör man för att faktorisera ett givet gaussiskt heltal?

Låt g vara ett gaussiskt primtal. Om man (i $\mathbb{N}$) primfaktoriserar det naturliga talet $\nu(g)$ fås $\nu(g) = g\bar{g} = p_1 \cdot p_2 \cdot \ldots \cdot p_n$, men detta är också en produkt i $\mathbb{Z}[i]$, så det irreducibla elementet g delar någon faktor, $g \mid p_k$, något k. Kalla p_k för p. Då fås också $\bar{g} \mid p$ och alltså $|g|^2 \mid p^2$ och det naturliga talet $|g|^2$ måste vara någon av de positiva delarna till p^2, dvs 1, p eller p^2. Eftersom g inte är en enhet är $|g| \neq 1$.

För alla reella primtal $p \equiv_4 1$ finns (enligt en sats av Fermat från 1640) två (reella) heltal a, b så att $p = a^2 + b^2$, dvs $p = (a+bi)(a-bi)$ och g är associerat

med $a+bi$ eller $a-bi$ (entydig faktorisering), $|g|^2 = p$. Vi ger ett bevis för Fermats sats i "Om gruppers verkan på mängder", som också ingår i denna kurs.

Om $p = 2$ är g associerat med $1+i$, ty $2 = (1+i)(1-i)$.

Om $p \equiv_4 3$ är $|g|^2 = a^2 + b^2 \neq p$ (ty $a^2, b^2 \equiv_4 0$ eller 1) och $g = u \cdot p$, u en enhet (entydig faktorisering, $g \mid g\bar{g} = p^2$, så $g \mid p$ och $|g| = p$), dvs g och p är associerade.

Det finns alltså **tre typer av gaussiska primtal**:

- $a+bi$, där $a, b \in \mathbb{Z}$ och $a^2 + b^2 = p$, ett (reellt) primtal som är $\equiv_4 1$,
- associerade med $1+i$ (dvs $\pm(1 \pm i)$),
- associerade med p, ett reellt primtal som är $\equiv_4 3$ (dvs $\pm p$ eller $\pm ip$).

För att **faktorisera ett gaussiskt heltal z** i irreducibla faktorer (gaussiska primtal) kan man således:

Faktorisera $|z|^2$ i reella primtal, $|z|^2 = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ och

- för varje $p_k \equiv_4 1$, finna $a_k, b_k \in \mathbb{Z}$ så att $p_k = a_k^2 + b_k^2$. Då är minst en av $a_k \pm b_k i$ en (prim)faktor i z,
- för varje $p_k = 2$ finns en (prim)faktor $1+i$ i z,
- för varje p_k^2 med $p_k \equiv_4 3$ (de finns alltid parvis i $|z|^2$) finns en (prim)faktor p_k i z.

Exempel: För att faktorisera $z = 44835 - 33075i$, beräkna och faktorisera reellt $|z|^2 = 44835^2 + 33075^2 = 3104132850 = 2 \cdot 3^2 \cdot 5^2 \cdot 7^4 \cdot 13^2 \cdot 17$.
3^2 ger faktorn 3 och 7^4 ger faktorn 7^2 ($3, 7 \equiv_4 3$) och 2 ger faktorn $1+i$. 5^2 ger två faktorer $2 \pm i$ (enklare förstås att börja med att bryta ut $5 = (2+i)(2-i)$ ur z), 13^2 ger två termer $3 \pm 2i$ och 17 ger en faktor $4 \pm i$. Man får testa om det i varje fall skall vara $+$ eller $-$. Man finner $z = 3 \cdot 7^2(1+i)(2+i)(2-i)(3-2i)^2(4-i)$.

Irreducibla polynom och faktorisering i $F[x]$

Eftersom $F[x]$, där F är en kropp, är euklidisk vet vi nu att varje polynom entydigt kan faktoriseras i irreducibla polynom. Till skillnad från i $\mathbb{Z}[i]$ är det dock normalt inte lätt att känna igen irreducibla polynom i $F[x]$, eller att faktorisera ett givet polynom. Om det har ett nollställe i F kan man använda

Faktorsatsen: Polynomet $f(x)$ i $F[x]$ har en förstagradsfaktor $(x-a)$ omm $f(a) = 0$.

Ty: Om $f(x) = (x-a)g(x)$ är förstås $f(a) = 0$, så "$\Rightarrow$" är klart.
För ett godtyckligt $f(x)$ finns $q(x)$, $r(x)$ så att $f(x) = q(x)(x-a) + r(x)$, där $\deg r(x) < \deg(x-a) = 1$, så $r(x) = r$, en konstant. Om $f(a) = 0$ är $r = 0$, så "$\Leftarrow$" är också klart.

Eftersom varje icke-konstant polynom i $\mathbb{C}[x]$ har (minst) ett nollställe i $\mathbb{C}$ ("algebrans fundamentalsats"), är de **irreducibla polynomen i $\mathbb{C}[x]$ precis förstagradspolynomen**.

För att avgöra vilka de irreducibla polynomen i $\mathbb{R}[x]$ är kan man utnyttja att $\mathbb{R}$ är en delkropp till $\mathbb{C}$, så varje polynom i $\mathbb{R}[x]$ kan betraktas som ett polynom i $\mathbb{C}[x]$. Om ett reellt polynom faktoriseras i komplexa förstagradsfaktorer kommer för varje icke-reell faktor $(x - z_0)$ också den konjugerade $(x - \bar{z_0})$ att förekomma. Deras produkt är ett reellt irreducibelt (det har ju inget reellt nollställe) polynom. De **irreducibla polynomen i $\mathbb{R}[x]$ är alltså precis förstagradspolynomen och de andragradspolynom som saknar reella nollställen**.

De irreducibla polynomen i $\mathbb{Q}[x]$ är inte lika lätta att beskriva. Lite förenklas det av följande avsnitt, som säger att det räcker att betrakta polynom i $\mathbb{Z}[x]$, dvs med heltalskoefficienter. I det avsnittet kommer också ett resultat (Eisensteins kriterium) som gör det lätt att finna irreducibla polynom i $\mathbb{Q}[x]$ av godtycklig grad.

Inte heller de irreducibla polynomen i $\mathbb{Z}_p[x]$, p ett primtal, är lätta att känna igen. Eftersom det bara finns ett ändligt antal polynom av varje grad i $\mathbb{Z}_p[x]$ ($(p-1)p^n$ av grad n) kan man ganska enkelt visa att det också här finns irreducibla polynom av godtycklig grad. De är viktiga för vissa typer av kryptering och finns därför tabellerade för många p-värden.

Om faktorisering i $\mathbb{Q}[x]$ och $\mathbb{Z}[x]$

Om R är en ring är också $R[x]$ det. Vi skall visa en sats om faktorisering i $\mathbb{Z}[x]$, som hjälper oss att finna irreducibla polynom av godtyckligt hög grad i $\mathbb{Q}[x]$. Eftersom varje heltal är ett rationellt tal, kan varje polynom i $\mathbb{Z}[x]$ uppfattas som ett polynom i $\mathbb{Q}[x]$.

Sats (Gauss' lemma): Om $f(x) \in \mathbb{Z}[x]$ är reducibelt i $\mathbb{Q}[x]$ är det reducibelt i $\mathbb{Z}[x]$. Om $f(x) = f_1(x)f_2(x)$ i $\mathbb{Q}[x]$, finns $\alpha \in \mathbb{Q}$ så att $\alpha f_1(x), \alpha^{-1} f_2(x) \in \mathbb{Z}[x]$.

Ty: Låt $f(x) = f_1(x)f_2(x)$, $f_i(x) \in \mathbb{Q}[x]$ och låt $k_i \in \mathbb{Z}$ vara sådana att $h_i(x) = k_i f_i(x) \in \mathbb{Z}[x]$. Det betyder att $k_1k_2 f(x) = h_1(x)h_2(x)$ och vi skall visa att varje primfaktor $p \mid k_1k_2$ finns som en gemensam faktor i koefficienterna i $h_1(x)$ eller i dem i $h_2(x)$. Varje primfaktor i k_1k_2 kan alltså divideras ut, vilket ger den önskade faktoriseringen i $\mathbb{Z}[x]$. Det andra påståendet följer av att entydig faktorisering gäller i $\mathbb{Q}[x]$, de två faktoriseringarna har parvis associerade faktorer.

Antag för motsägelse att det inte är så, dvs att $p \mid a_0, a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1}$ och $p \nmid a_r, b_s$ för några $r \leq m$, $s \leq n$, där $h_1(x) = a_m x^m + \ldots + a_1 x + a_0$, $h_2(x) = b_n x^n + \ldots + b_1 x + b_0$. p delar varje koefficient i $h_1(x)h_2(x)$, speciellt den för x^{r+s}, dvs $p \mid a_0 b_{r+s} + a_1 b_{r+s-1} + \ldots + a_r b_s + \ldots + a_{r+s} b_0$. Men det ger vår motsägelse, ty p delar alla talen i summan utom $a_r b_s$. Saken är klar.

Om ett $f(x)$ inte kan faktoriseras i $\mathbb{Z}[x]$ kan det alltså inte heller faktoriseras i $\mathbb{Q}[x]$ (trots att det finns många fler tänkbara faktorer där).

(Ett polynom som är irreducibelt i $\mathbb{Z}[x]$ är alltså irreducibelt också i $\mathbb{Q}[x]$. Man kunde tro att omvändningen gäller, dvs att ett polynom som är irreducibelt i $\mathbb{Q}[x]$ måste vara irreducibelt i $\mathbb{Z}[x]$, men så är det faktiskt inte. $f(x) = 2x$ är ju irreducibelt i $\mathbb{Q}[x]$ (det är alla förstagradspolynom), men i $\mathbb{Z}[x]$ är varken 2 eller x enheter, så $f(x) = 2 \cdot x$ är en faktorisering som inte innehåller någon enhet.)

Vissa (men inte alls alla) irreducibla polynom i $\mathbb{Z}[x]$ kan kännas igen med

Eisensteins kriterium: Om för $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ och ett primtal p

$$p \mid a_0,\ p \mid a_1, \ldots,\ p \mid a_{n-1}, \text{ men } p \nmid a_n,\ p^2 \nmid a_0$$

så är $f(x) = a_n x^n + \ldots + a_1 x + a_0$ irreducibelt i $\mathbb{Z}[x]$ (och därmed i $\mathbb{Q}[x]$).

Ty: Låt för motsägelse $f(x) = f_1(x)f_2(x)$, $f_i(x) \in \mathbb{Z}[x]$ och $f_1(x) = b_k x^k + \ldots + b_1 x + b_0$, $f_2(x) = c_l x^l + \ldots + c_1 x + c_0$ vara en faktorisering utan konstanta faktorer, så $k, l > 0$. $p \mid a_0, p^2 \nmid a_0 = b_0 c_0$, så $p \mid b_0$, $p \nmid c_0$ (eller tvärtom). Om $p \mid b_0, b_1, \ldots, b_{r-1}$ för $0 \leq r \leq k < n$ gäller eftersom $p \mid a_r = b_0 c_r + b_1 c_{r-1} + \ldots + b_r c_0$ att $p \mid b_r c_0$, så $p \mid b_r$. Det ger att $p \mid b_r$ för $r = 0, 1, \ldots, k$ och därmed $p \mid a_n$, vilket motsäger förutsättningarna i satsen. Saken är klar.

I $\mathbb{Z}[x]$ (så i $\mathbb{Q}[x]$) finns alltså irreducibla polynom av godtyckligt hög grad, t.ex. $x^n + p$, p primtal.

Exempel: $x^{17} - 15x^{12} + 36x^6 + 27x^2 - 21$ är irreducibelt i $\mathbb{Q}[x]$. (Tag $p = 3$ i kriteriet.)
$f(x) = \frac{2}{3}x^{11} - \frac{5}{8}x^7 + 25x^4 - \frac{5}{7}x^2 - \frac{10}{3}$ är irreducibelt i $\mathbb{Q}[x]$, ty $3 \cdot 7 \cdot 8 \cdot f(x)$ är irreducibelt i $\mathbb{Z}[x]$ (kriteriet med $p = 5$).
$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ är irreducibelt i $\mathbb{Q}[x]$ för varje primtal p, ty $f(x) = \frac{x^p - 1}{x - 1}$, så $f(y+1) = \frac{1}{y}((y+1)^p - 1) = \sum_{k=1}^{p} \binom{p}{k} y^{k-1}$ är irreducibelt (ty $p \mid \binom{p}{k}$ då $0 < k < p$, $p \nmid \binom{p}{p} = 1$ och $p^2 \nmid \binom{p}{1} = p$) och en faktorisering av $f(x)$ skulle ge en av $f(y+1)$.

Avslutning

Detta avsnitt har illustrerat hur man genom att ta fram det väsentliga i ett bevis (i vårt fall divisionsegenskapen för $\mathbb{Z}$ när vi bevisade entydig faktorisering för de naturliga talen) kan återanvända beviset på andra system (alla euklidiska ringar, bl.a. de gaussiska heltalen och polynomen över en kropp – ett exempel till ges i övningsexemplen) som har motsvarande egenskap. Man kan säga att det är samma idé som när vi studerade alla grupper utgående från gruppaxiomen; i stället för att bara visa saker för **ett visst** system (heltalen $\mathbb{Z}$) gjorde vi det för **alla** system med vissa egenskaper (alla euklidiska ringar).

Man kan också göra mer av det vi tidigare gjorde för $\mathbb{Z}$ för godtyckliga euklidiska ringar. T.ex. fungerar modulär aritmetik för en euklidisk ring, på samma sätt som $\mathbb{Z}_m$. Om modulen (det vi dividerar med och tar rest) är ett irreducibelt element i ringen är motsvarande ring en kropp (som $\mathbb{Z}_p$, p ett primtal). Ett par exempel finns i övningsexemplen här nedan.

Övningsexempel

1a. Finn $a \in \mathbb{Z}$ så att $87 + 13i$ och $13 + ai$ är associerade i $\mathbb{Z}[i]$.

b. Finn $a, b, c \in \mathbb{Z}_5$ så att $2x^3 + 4x^2 + 3$ och $3x^3 + ax^2 + bx + c$ är associerade i $\mathbb{Z}_5[x]$.

2. Finn ett annat (än 6) element i $\mathbb{Z}[i\sqrt{5}]$ som har (minst) två olika faktoriseringar i irreducibla element.

3a. Finn i $\mathbb{Z}[i]$ $\text{sgd}(-3+11i, 8-i)$ och uttryck den som $a(-3+11i)+b(8-i)$.

b. Finn i $\mathbb{Z}[i]$ $\text{sgd}(1 + 47i, 26 + 12i)$.

4. Faktorisera $17 - 11i$ i irreducibla faktorer i $\mathbb{Z}[i]$, dvs skriv det som en produkt av gaussiska primtal.

5. Faktorisera $f(x) = x^3 + x + 1$ i irreducibla faktorer i $\mathbb{Z}_3[x]$.

6. Om modulär aritmetik i $\mathbb{Z}[i]$. Om $a \in \mathbb{Z}[i]$ kan vi räkna $(\text{mod } a)$ i $\mathbb{Z}[i]$ (dvs "räkna som vanligt, men ta resten vid division med a av resultatet") och den resulterande $\mathbb{Z}[i]/(a)$ är en kropp precis om a är ett gaussiskt primtal (liksom $\mathbb{Z}_p$ är en kropp precis om p är ett primtal).
Om elementen i $\mathbb{Z}[i]/(3)$ representeras som $\{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$, vad är $(2 + i) + (2 + 2i)$, $(2 + i)(2 + 2i)$, $-(2 + i)$ och $(1 + 2i)^{-1}$ i $\mathbb{Z}[i]/(3)$?

7. $x^2 + 1$ är ju ett irreducibelt polynom i $\mathbb{R}[x]$.
Om man som i förra uppgiften bildar $\mathbb{R}[x]/(x^2+1)$ och tar resterna vid division med x^2+1 som polynom av grad högst 1, vad är $(ax+b)(cx+d)$ i $\mathbb{R}[x]/(x^2+1)$? Vilken känd kropp är isomorf med $\mathbb{R}[x]/(x^2 + 1)$?

8*. Låt $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ och definiera $\nu : \mathbb{Z}[\sqrt{3}] \to \mathbb{N} \cup \{-\infty\}$ enligt $\nu(a + b\sqrt{3}) = |a^2 - 3b^2|$ om $a + b\sqrt{3} \neq 0$, $\nu(0) = -\infty$.

a. Visa att $\nu(\alpha\beta) = \nu(\alpha)\nu(\beta)$ då $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ ($k(-\infty) = -\infty$ för alla $k \in \mathbb{N} \cup \{-\infty\}$).

b. Visa att $\mathbb{Z}[\sqrt{3}]$ med detta ν är en euklidisk ring.

c. Visa att $\alpha \in \mathbb{Z}[\sqrt{3}]$ är en enhet omm $\nu(\alpha) = 1$.

d. Visa att $\alpha \in \mathbb{Z}[\sqrt{3}]$ är irreducibelt om $\nu(\alpha)$ är ett primtal.

e. Verifiera att $(3 + 2\sqrt{3})(4 + \sqrt{3}) = (5 - 2\sqrt{3})(12 + 7\sqrt{3})$ och visa att alla dess faktorer är irreducibla i $\mathbb{Z}[\sqrt{3}]$.

f. Har $\mathbb{Z}[\sqrt{3}]$ entydig faktorisering i irreducibla faktorer?

g.** Finn alla enheter i $\mathbb{Z}[\sqrt{3}]$.

Svar till övningsexemplen

1a. $13+ai$ skall vara $u(87+13i)$ med u en av $1, i, -1, -i$. Enda möjligheten är $u=-i$, så $\boldsymbol{a=-87}$.

b. $3x^3+ax^2+bx+c$ måste vara $4(2x^3+4x^2+3)$, så $\boldsymbol{a=1,\ b=0,\ c=2}$.

2. $\boldsymbol{9=3\cdot 3=(2+i\sqrt{5})(2-i\sqrt{5})}$ och eftersom $1<|3|^2, |2\pm i\sqrt{5}|^2<16$ är alla faktorerna irreducibla element och 3 är uppenbarligen inte associerat med någon faktor i HL (de enda enheterna är ju ± 1).

3a. Euklides algoritm. $\frac{-3+11i}{8-i}=\frac{(-3+11i)(8+i)}{65}=-\frac{-7}{13}+\frac{17}{13}i\approx -1+i$, $-3+11i=(-1+i)(8-i)+(4+2i)$, $\frac{8-i}{4+2i}=\frac{3}{2}-i\approx 1-i$, $8-i=(1-i)(4+2i)+(2+i)$ och $4+2i=2(2+i)$ ger $\boldsymbol{\mathrm{sgd}(-3+11i, 8-i)=2+i}$ $=(8-i)+(-1+i)(4+2i)=(8-i)+(-1+i)[(-3+11i)+(1-i)(8-i)]$ $\boldsymbol{=(-1+i)(-3+11i)+(1+2i)(8-i)}$.

b. P.s.s. fås $\boldsymbol{\mathrm{sgd}(1+47i, 26+12i)=-3-i}$ (eller $3+i$).

4. $|17-11i|^2=17^2+11^2=410=2\cdot 5\cdot 41$. Faktorn 2 visar att $17-11i$ har en faktor $1+i$ och man får $17-11i=(1+i)(3-14i)$. Faktorn 5 visar att $17-11i$ (så $3-14i$) har en av $2\pm i$ som faktor. Man finner $2+i\nmid 3-14i$, men $3-14i=(2-i)(4-5i)$, där $4-5i$ är ett gaussiskt primtal (ty $|4-5i|^2=41$, ett primtal). Så $\boldsymbol{17-11i=(1+i)(2-i)(4-5i)}$ är den önskade faktoriseringen.

5. Om $f(x)$ kan faktoriseras utan enheter, måste någon faktor ha grad 1 (eftersom dess grad är 3 och faktorer av grad 0 ju är enheter). Enligt faktorsatsen finns en sådan faktor precis om $f(x)$ har ett nollställe. $f(0)=1$, men $f(1)=1+1+1=0$, så $x-1=x+2$ är en faktor. Polynomdivision ger $f(x)=(x+2)(x^2+x+2)$. Om $g(x)=x^2+x+2$ kan faktoriseras utan enheter måste den ha ett nollställe (som inte kan vara 0), men $g(1)=1$, $g(2)=2$. Den sökta faktoriseringen är alltså $\boldsymbol{f(x)=(x+2)(x^2+x+2)}$.

6. $(2+i)+(2+2i)=4+3i=1+3(1+i)\equiv_3 1$, så $\boldsymbol{(2+i)+(2+2i)=1}$.
$(2+i)(2+2i)=2+6i=2+3\cdot 2i\equiv_3 2$, så $\boldsymbol{(2+i)(2+2i)=2}$.
$-(2+i)=-2-i=1+2i+3(-1-i)\equiv_3 1+2i$, så $\boldsymbol{-(2+i)=1+2i}$.
$(1+2i)^{-1}$ kan fås med Euklides algoritm (ty $\mathrm{sgd}(3, 1+2i)=1$). Man finner $1=(-1-i)(1+2i)+3i=(2+2i+3(-1-i))(1+2i)+3i=(2+2i)(1+2i)+3(1-2i)$, vilket ger $(2+2i)(1+2i)=1$ och $\boldsymbol{(1+2i)^{-1}=2+2i}$ i $\mathbb{Z}[i]/(3)$.

7. Eftersom $(ax+b)(cx+d)=acx^2+(ad+bc)x+bd=(ad+bc)x+(bd-ac)+ac(x^2+1)\equiv_{x^2+1}(ad+bc)x+(bd-ac)$ är $\boldsymbol{(ax+b)(cx+d)=(ad+bc)x+(bd-ac)}$ i $\mathbb{R}[x]/(x^2+1)$.
Eftersom också $(ax+b)+(cx+d)=(a+c)x+(b+d)$ ger $\varphi(ax+b)=b+ai$ en isomorfi mellan $\mathbb{R}[x]/(x^2+1)$ och $\mathbb{C}$**, de komplexa talen**.

8*a. Visa $(ac+3bd)^2-3(ad+bc)^2=(a^2-3b^2)(c^2-3d^2)$, tag $||$ av båda led.

b. Axiomen för en kommutativ ring med etta är uppfyllda i $\mathbb{Z}[\sqrt{3}]$.
ν en euklidisk valuation: (1) klart, (2) $s, d\in\mathbb{Z}[\sqrt{3}]$, $d\neq 0$ ger $\frac{s}{d}=q+(x+y\sqrt{3})$ med $q\in\mathbb{Z}[\sqrt{3}]$, $x, y\in\mathbb{Q}$, där $|x|, |y|\leq\frac{1}{2}$, så $-\frac{3}{4}\leq x^2-3y^2\leq\frac{1}{4}$. Så $s=qd+r$, $r\in\mathbb{Z}[\sqrt{3}]$ och $\nu(r)<\nu(d)$ (som i a.), (3) ur a. ($\nu(t)\geq 1$ om $t\neq 0$).

c. $\frac{1}{a+b\sqrt{3}}=\frac{a-b\sqrt{3}}{a^2-3b^2}\in\mathbb{Z}[\sqrt{3}]$ omm $a^2-3b^2=1$ ($a^2-3b^2=-1$ omöjligt, ty $a^2\equiv_3 0, 1$).

d. Om $\alpha=\beta\gamma$ och $\nu(\alpha)$ primt är $\nu(\alpha)=\nu(\beta)\nu(\gamma)$ och en av β, γ en enhet.

e. Beräkna och använd d.

f. Ja, enligt b. (I e. är $5-2\sqrt{3}=(2-\sqrt{3})(4+\sqrt{3})$, $12+7\sqrt{3}=(2+\sqrt{3})(3+2\sqrt{3})$.)

g.** Alla enheter ges av $\pm(2+\sqrt{3})^n$, $n\in\mathbb{Z}$. ($(2+\sqrt{3})^{-1}=2-\sqrt{3}$.)
(Om $a^2=3b^2+1$, $a, b\in\mathbb{Z}_+$ och $a_1+b_1\sqrt{3}=(2-\sqrt{3})(a+b\sqrt{3})$ är $0<a_1<a$, $0\leq b_1<b$ och $b_1=0$ omm $b=1$ (så $a=2$). Induktion över a för enheter med $a, b>0$.)