(SF1662 Diskret matte, vt17: F18, ti 4 april 2017)

Mer om faktorisering

Entydig faktorisering bevisas för vissa ringar (i stort sett) som för de positiva heltalen $\mathbb{Z}_+$.

Låt R vara en kommutativ ring. Vi betraktar särskilt: **heltalen** $\mathbb{Z}$, de **gaussiska heltalen** $\mathbb{Z}[i]$ (alla komplexa tal med både real- och imaginärdel heltal) och **polynom** $F[x]$ med koefficienter i en kropp F (t.ex. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ eller $\mathbb{Z}_p$ (p ett primtal)).

Definition: $u \in R$ är en **enhet** (eng. unit) omm u är inverterbart i R. Mängden $U(R)$ av enheter är en grupp under $\cdot$.

$U(\mathbb{Z}) = \{\pm 1\}$, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ och $U(F[x]) = \{\text{konstanter utom 0 i } F\} = F \setminus \{0\}$.

Definition: För d, $m \in R$ kallas d en **delare** till m, skrivet $d \mid m$ omm det finns $q \in R$ så att $m = qd$.

Två element x, $y \in R$ som är delare till varandra, $x \mid y$ och $y \mid x$, kallas **associerade element**. Det är de precis om $x = uy$ (och därmed $y = u^{-1}x$) för en enhet u.

Definition: För x, $y \in R$ 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"

Två sgd:er till x, y är alltid associerade och element som är associerade till en sgd är också en sgd.

Definition: $\pi \in R$ är ett **irreducibelt element** i R omm
$\pi = x \cdot y$ med x, $y \in R$ medför att precis en av x och y är en enhet.

π är alltså ett irreducibelt element precis om det inte är en enhet och alla dess delare är enheter eller associerade till π.

I $\mathbb{Z}$ är de irreducibla elementen alla $\pm p$, p primtal. Irreducibla element i $\mathbb{Z}[i]$ kallas "gaussiska primtal".

Definition: ν är en **euklidisk valuation** på R omm

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

Om R har en euklidisk valuation ν har R inga nolldelare (dvs $st = 0 \Rightarrow s = 0$ eller $t = 0$) och $\nu(s) = \nu(t)$ om s, t är associerade, $\nu(s) < \nu(t)$ om $s \mid t$ och s, t inte är associerade.
För våra exempelringar: $\nu(0) = -\infty$ i alla (ju), $\nu(n) = |n|$ för $n \in \mathbb{Z} \setminus \{0\}$, $\nu(z) = |z|^2$ då $z \in \mathbb{Z}[i] \setminus \{0\}$ och $\nu(f(x)) = f(x)$:s grad då $f(x) \in F[x] \setminus \{0\}$.

Låt nu R vara en ring med en euklidisk valuation, en **euklidisk ring**.

Euklides algoritm fungerar i R som för heltalen och visar att för $s, t \in R$ existerar en sgd d och den kan skrivas $d = as + bt$ för några a, $b \in R$.

Sats: För d, s, $t \in R$ gäller att $d \mid st$, $\text{sgd}(d, s) \in U(R)$ ger att $d \mid t$.

Sats (entydig faktorisering i euklidiska ringar):
Varje $s \neq 0$ i R är associerat med en produkt av irreducibla element i R. Ingående irreducibla element är entydigt bestämda av s, sånär som ordningen och faktorer som är enheter (dvs de irreducibla elementen kan kastas om och bytas ut mot associerade element (som ju också är irreducibla)).

Varje **gaussiskt primtal** är associerat med precis en av:

- $1+i$
- p, ett (vanligt) primtal som är $\equiv 3 \pmod 4$
- $a+bi,\ a^2+b^2=p$, ett (vanligt) primtal som är $\equiv 1 \pmod 4$

För att **faktorisera** ett (måttligt stort) gaussiskt heltal z, beräkna $|z|^2 = z\bar{z}$ och primfaktorisera (reellt) produkten. Om en gaussisk primfaktorisering av z är $z = g_1 g_2 \dots g_k$, kan man känna igen $|g_i|^2$ bland primfaktorerna till $|z|^2$.

Följande hanns inte på föreläsningen. En del av det tas upp nästa gång.

Faktorisering i $F[x]$

Det är inte alltid lätt att faktorisera ett polynom i $F[x]$.
Om det har ett nollställe kan man använda
Faktorsatsen:
Polynomet $f(x) \in F[x]$ har en förstagradsfaktor $(x-a)$ omm $f(a)=0$.

De irreducibla polynomen i $\mathbb{C}[x]$ är precis förstagradspolynomen.

De irreducibla polynomen i $\mathbb{R}[x]$ är precis förstagradspolynomen och de andragradspolynom som saknar reella nollställen.

De irreducibla polynomen i $\mathbb{Q}[x]$ är inte lätta att beskriva. En del hittas med:

Gauss lemma: Om $f(x) \in \mathbb{Z}[x]$ är reducibelt i $\mathbb{Q}[x]$ är det också reducibelt i $\mathbb{Z}[x]$, med associerade faktorer.
(Men det finns polynom som är reducibla i $\mathbb{Z}[x]$ och irreducibla i $\mathbb{Q}[x]$, t.ex. $f(x)=2x$.)

Eisensteins kriterium: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ i $\mathbb{Z}[x]$ är irreducibelt om det för något primtal p gäller att $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, men $p \nmid a_n$, $p^2 \nmid a_0$.
I $\mathbb{Z}[x]$ (så i $\mathbb{Q}[x]$) finns alltså irreducibla polynom av godtyckligt hög grad.

Också i $\mathbb{Z}_p[x]$ finns irreducibla polynom av godtyckligt hög grad (men där kan Eisensteins kriterium inte tillämpas).