

Sista  
F18

## Mer om faktorisering

i  $\mathbb{Z}$ ,  $\mathbb{Z}[i]$  och  $F[x]$   
heltal) (gaussiska heltal) (polynom med koefficienter  
i  $F$  ( $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ ))

- Entydig faktorisering i irreducibla element  
    ( atom ordning, enheter  
        ( invertebara element
- Euklides algoritmen,  $\text{sgd}(m, n) = am + bn$

Följer av existens av en euklidisk valuation  $v$

1.  $v(0) = -\infty$ , för övriga  $n$   $v(n)$  heltal
2. För  $n, d \neq 0$  finns  $q, r$  så att  
$$n = qd + r, \quad v(r) < v(d)$$
3.  $v(m) \leq v(mn)$  om  $n \neq 0$

i  $\mathbb{Z}$ :  $v(n) = |n|$ , i  $\mathbb{Z}[i]$ :  $v(z) = |z|^2$

i  $F[x]$ :  $v(f(x)) = f(x)$ 's grad

Om  $(R, +, \cdot)$  är en euklidisk ring

med valuation  $v$  gäller

för alla  $x, y, u \in R$

- $x, y \neq 0 \Rightarrow xy \neq 0$
- $u$  enhet,  $x \neq 0 \Rightarrow v(u) \leq v(x)$
- $x, y$  associerade  $\Rightarrow v(x) = v(y)$
- $v(x) = v(1) \Leftrightarrow x$  enhet
- $x = yz$ ,  $y$  inte enhet,  $x \neq 0 \Rightarrow v(z) < v(x)$

Gaussiska primtal, irreducibla element i  $\mathbb{Z}[i]$

3 typer, enheter gänger

(dvs  $\pm 1, \pm i$ )

- $1+i$
- $p$ , reellt primtal  $\equiv_4 3$
- $a+bi$ ,  $a^2+b^2=p$ , reellt primtal  $\equiv_4 1$

För att faktorisera  $z$  i  $\mathbb{Z}[i]$ :

$$|z|^2 = p_1 p_2 \dots p_k$$

(reella primtal)

$$\text{Om } z = g_1 g_2 \dots g_r$$

(gaussiska primtal)

$$g_i = u_i p_i, \quad p_i \equiv_4 3$$

(enhet)

eller

$$|g_i|^2 = p_i, \quad p_i \equiv_4 1 \text{ eller } p_i = 2$$

$$\text{ex } |7+35i|^2 = 7^2 + 35^2 = 1274 = 2 \cdot 7^2 \cdot 13$$

$$7+35i = (1+i) 7 (3+2i)$$

↑ testa!

("kunde varit"  $3-2i$ )

## Faktorisering i $F[x]$

Faktorsatsen:  $f(x)$  har faktorn  $(x-a)$   
om  $f(a) = 0$

Irreducibla i  $\mathbb{C}[x]$ : förstegradspolynomen

i  $\mathbb{R}[x]$ : förstegradspolynom och  
andragradspolynom utan reella nollst.

Gauss lemma:  $f(x) \in \mathbb{Z}[x]$  är

irreducibelt i  $\mathbb{Z}[x] \Rightarrow$  irreducibelt i  $\mathbb{Q}[x]$

Eisensteins kriterium:

$f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$  är

irreducibelt om för ett primtal  $p$

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

ex  $x^{15} - 74x^{13} + 96x^7 - 38$  är irreducibelt  
i  $\mathbb{Q}[x]$