Lektion 5

Def: (Primelement och irreducibla element)

Et element $r \in R$ kallas för prim om
$r \mid st \Rightarrow r \mid s \vee r \mid t$ för alla $s,t \in R$.

" $r \in R$ kallas för irreducibel om
$r = st \Rightarrow$ enten s eller t är inverterbare

Motivation

Prim
- $p \in \mathbb{Z}$ prim:
  $p \mid ab \Rightarrow p \mid a \vee p \mid b$
  (Euklids lemma)

Irreducibel
- p prim: p har ingen delare,
  $p = r \cdot s \Rightarrow r = \pm p \quad s = \pm 1$
  $\vee\ r = \pm 1 \quad s = \pm p$

Obs: irr $\not\Rightarrow$ prim

Ex: $R = \mathbb{Z}[i\sqrt{5}]$
- R är et i.d. omr.
- 2 är irr. i R:

▷ 2 är inte inv:
$1 = 2(a + b \cdot i\sqrt{5}) = 2a + 2b i\sqrt{5}$
har ingen heltalslösning för a, b.

▷ $2 = (a + bi\sqrt{5})(c + di\sqrt{5})$

$$(a + bi\sqrt{5})(a - bi\sqrt{5}) = a^2 - (bi\sqrt{5})^2 = a^2 + b^2 5$$

$\Rightarrow 4 = \underbrace{(a^2 + b^2 5)(c^2 + d^2 \cdot 5)}_{\text{positiva}}$

$\Rightarrow a^2 + b^2 5,\ c^2 + d^2 \cdot 5 \leq 4$

$\Rightarrow b = 0 = d \quad \Leftrightarrow \quad a^2 \cdot c^2 = 4$

$\Rightarrow a \cdot c = 2 \quad \Rightarrow a$ inv. eller c inv.

▷ 2 är inte prim:
$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$

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

Anta att $2 \mid (1 \pm i\sqrt{5})$

$\Rightarrow 2(a \pm bi\sqrt{5}) = (1 \pm i\sqrt{5}) \Rightarrow 2a = 1,\ 2b = -1$
har ingen heltalslösning.

Problem: 6 har två olika faktoriseringar.

Def: Et int.omr. R heter faktoriell om alla
$x \in R$, x inte inv., har en entydig faktorisering i irreducibla:
$\exists\, p_1, \dots, p_n \in R,\ u \in R^* : \ x = p_1 \cdots p_n \cdot u$ och
Om $x = q_1 \cdots q_m \cdot v$ med $q_1, \dots, q_m$ irr., $v \in R^*$ så är $m = n$
och för varje i finnes presist et j med $p_i \sim q_j$

[Notation: $p_i \sim q_j :\Leftrightarrow p_i$ och q_j är associerade]

78) Har $x^2+x+4=0$ en lösning $a\in\mathbb{Z}_5$, dvs. $a^2+a+4\equiv 0 \mod 5$?

I $\mathbb{Z}_5$: $a=0$

$a=1$ $1+1+4=6=1$

$a=2$ $4+2+4=10=0$ i $\mathbb{Z}_5$:)

Sidan $\mathbb{Z}_5[X]$ är faktoriell är

$x^2+x+4=(x-2)(x+3)$ entydig,

alla lösningar är 2 och $-3=2$

I $\mathbb{Z}_7$: $a=0$ $a=1$ $1+1+4=6\neq 0$

$a=2$ $4+2+4=10=3\neq 0$

$a=3$ $9+3+4=16=2\neq 0$

$a=4$ $16+4+4=24=3\neq 0$

$a=5$ $25+5+4=34=6\neq 0$. Ingen lösning

$a=6$ $1-1+4=4\neq 0$.

80) Vilka inv. element finns i $K[X]$ där K är en kropp?

- $1 = 0\cdot x^n+0\cdot x^{n-1}+\dots+0\cdot x+1$ inv.
- Alla konstanter $\neq 0$ är inv.
- Anta att $p\in K[X]$, p inte konstant, är inv.

$\exists\, q\in K[X]:\ pq=1$.

$0=\deg(1)=\deg(p\cdot q)=\deg(p)+\deg(q)$

$p=k x^n+\dots x^{n-1}+\dots$
$q=l x^m+\dots x^{m-1}+\dots$

$pq=(k\cdot l)\,x^{n+m}+\dots$, $\neq 0$ om $k\neq 0\neq l$.

p inte konst. $\Rightarrow \deg(p)\geq 1$

$\Rightarrow \deg(q)<0$ ↯

$\Rightarrow p$ inte inv. $\Rightarrow K[X]^*=K^*$.

82) Hitta en inv. polynom i $\mathbb{Z}_4[X]$ med grad >0.

Som i 80: Vi behöver en nolldelare i $\mathbb{Z}_4$.

Ta $k=2=l$.

$$(2X+1)(2X+1)=4x^2+2x+2x+1 = 0+0+1$$

Notis: $2x$ har $\deg(2x)=1$ men två rötter 0 och 2.

86) Visa att följande är irr. i $\mathbb{Q}[X]$.

a) x^3+9

Observera: Om x^3+9 är reducibel, så är $x^3+9=p\cdot q$ med $\deg(p)=1$ eller $\deg(q)=1$

$\Rightarrow X^3+9$ har en rot i $\mathbb{Q}$.

Men x^3+9 har ingen rot i $\mathbb{Q}$.

b) $x^3+9x^2+24x+19=f$

Rotsats: alla rötter är av formen $\frac{p}{q}$ (reducerad bråk) där $p\mid 19$, $q\mid 1$

Men då är $q=\pm 1$, $p=\pm 19$.

$f(19)>0$ $f(-19)=(-19)^3+9\cdot(-19)^2+-23\cdot 19$
$=-(19^3)+9\cdot 19^2+(-23)\cdot 19$
$=19\,(-(19)^2+9\cdot 19+(-23))=0$

$\Rightarrow -(19^2)+9\cdot 19+(-23)=0$
$=-19\cdot 19+9\cdot 19+(-23)=-10\cdot 19-23<0$.

Alt.: $f=gh \Rightarrow \bar f=\bar g\bar h$ i $\mathbb{Z}_2[X]$

där $\bar f = x^3+\bar 9x^2+\overline{24}x+\overline{19}$ i $\mathbb{Z}_2[X]$
$= x^3+1x^2+0x+1$ har ingen rot mod 2

$\Rightarrow f$ har ingen rot i $\mathbb{Z}$ $(\underbrace{\Rightarrow}_{f \text{ primitiv}} f$ har ingen rot i $\mathbb{Q})$

92) a) Ja. $[\deg(X-2)=1]$

b) $3x-6=3\cdot(x-2)$ irr., $3\in\mathbb{Q}^*$

$3x-6=3\cdot(x-2)$ i $\mathbb{Z}[X]$, reducibel!

c) x^2-3 har ingen rot i $\mathbb{Q}$.

d) Ja.

e) K kropp $\Rightarrow K[X]$ faktoriell

$\deg(p\cdot q)=\deg(p)+\deg(q)$

$f=\prod_{i=1}^{m} f_i$, f_i irr. $m\leq \deg(f)$.

Alla rötter r_i av f ger en faktor $f_i=(X-r_i)$.

f) Förstagradspolynom: $aX+b$, $a\in K^*$, $b\in K$.

har rot: $\frac{-b}{a}$.

g) $R[X]=\{f:\mathbb{N}_0\to R \mid f(i)\neq 0$ för ändligt många $i\in\mathbb{N}\}$

$f(0)+f(1)\cdot X+f(2)\cdot X^2+f(3)X^3+\dots+f(n)\cdot X^n+0\cdot X^{n+1}+0\cdots$

$\Rightarrow \deg(f)<\infty$ f.a. $f\in R[X]$.

$\#\text{rot} \underbrace{\leq}_{R[X] \text{ faktoriell}} \deg(f)<\infty$.