~~Kom i~~ Från förra gången:

En <u>delkropp</u> till $\mathbb{C}$ är en delmängd $\mathbb{K}$ till $\mathbb{C}$ som innehåller 0 och 1 och som är sluten under de fyra räknesätten $+, -, *, /$.

<u>Ex.</u>: $\mathbb{C} \supsetneq \mathbb{R} \supseteq \mathbb{Q} (\supseteq \underset{\text{ingen delkropp}}{\mathbb{Z}})$.

Ett <u>polynom över $\mathbb{K}$</u> är ett polynom vars koefficienter alla ligger i $\mathbb{K}$.

Ett polynom f är <u>irreducibelt över $\mathbb{K}$</u> om man inte kan skriva $f = g \cdot h$ där g och h är polynom över $\mathbb{K}$ som båda har lägre grad än f.

<u>Ex</u>
$$\begin{aligned} & x^4 + 2x^3 - x - 2 \\ &= (x^2 + x + 1)(x^2 + x - 2) \\ &= (x^3 - 1)(x + 2) \end{aligned}$$
är reducibelt över $\mathbb{Q}$ (och $\mathbb{Z}$).

<u>Sats</u> Varje moniskt polynom (över $\mathbb{K}$) kan på ett entydigt sätt (upp till ordningen av faktorna) skrivas som produkt av moniska irreducibla polynom.

<u>Ex</u> $x^4 + 2x^3 - x - 2 = (x^2 + x + 1)(x - 1)(x + 2)$

irreducibla över $\mathbb{Q}$

Vilka polynom är irreducibla?

$\mathbb{K} = \mathbb{C}$: Ett polynom f är irreducibelt <u>omm</u>
~~dess grad~~ $\deg f \leq 1$.
(Algebrans fundamentalsats!)

$\mathbb{K} = \mathbb{R}$: De enda irreducibla polynomen är
(i) alla f där $\deg f \leq 1$
(ii) alla f där $\deg f = 2$ och
som har två icke-reella rötter

Vilka polynom är irreducibla över $\mathbb{Q}$?
över $\mathbb{Z}$?

OBS! f irreducibelt över $\mathbb{Q}$ $\Leftrightarrow$ $k \cdot f$ irreducibelt över k för $k \in \mathbb{Q}$

~~Betrak~~ (moniska) polynom över $\mathbb{Q}$ $\rightsquigarrow$ primitiva polynom över $\mathbb{Z}$

<u>Def</u> Ett polynom över $\mathbb{Z}$, $f(x) = a_n x^n + \ldots + a_0$, är <u>primitivt</u> om $\text{sgd}(a_n, \ldots, a_0) = 1$.

<u>Ex.</u>
$x^2 + \frac{1}{6}x - \frac{1}{3} \rightsquigarrow 6x^2 + 1x - 2$
$2x^3 + \frac{12}{5}x^2 - 6x - \frac{18}{5} \rightsquigarrow 5x^3 + 6x^2 - 15x - 9$
$\frac{1}{8}x^2 - \frac{1}{2}x + 1 \rightsquigarrow x^2 - 4x + 8$

<u>Hjälpsats.</u> För varje polynom f över $\mathbb{Q}$
finns ett rationellt tal $\alpha \in \mathbb{Q}$
så att $\alpha \cdot f$ ~~har~~ är primitivt.
(α är unik upp till tecken.)

<u>Sats</u> (Gauss Lemma #1).
Om f och g är primitiva polynom,
så är även $f \cdot g$ primitivt.

Bevis. Antag att $f \cdot g$ inte är primitivt,
dvs. $\exists$ primtal p så att p delar alla
koefficienter i $f \cdot g$.
f och g är ~~inte~~ primitiva
dvs. $\exists$ koefficienter a_i i f och b_j i g
som inte p delar ~~p~~
om a_i och b_j är lägstagradkoefficienterna
som inte p delar ~~p~~, så delar p inte heller
koefficienten c_{i+j} i $f \cdot g$.

<u>Sats</u> (Gauss Lemma #2).
Ett polynom över $\mathbb{Z}$ är irreducibelt
över $\mathbb{Z}$ om och endast om det är
irreducibelt över $\mathbb{Q}$.

Bevis. Vi kan anta ~~att~~ f är primitivt.

f irreduzibel över $\mathbb{Q}$ $\Rightarrow$ f irred. över $\mathbb{Z}$

Antag att f är reducibelt över $\mathbb{Q}$.
$f = g \cdot h$, där g och h har rationella koefficienter

$\Rightarrow \exists \alpha, \beta \in \mathbb{Q}$ s.a. αg och βh är primitiva.

$\Rightarrow (\alpha\beta) \cdot f = (\alpha g) \cdot (\beta h)$
$\Rightarrow (\alpha\beta) \cdot f$ och f är primitiva
$\Rightarrow \alpha\beta = \pm 1$ och $f = \pm (\alpha g) \cdot (\beta h)$

Därmed är f reducibelt över $\mathbb{Z}$. $\square$

<u>Följdsats.</u> Om $f(x) = a_n x^n + \ldots + a_0$ är ett polynom över $\mathbb{Z}$ och $x = p/q \in \mathbb{Q}$ är en rot till f där $\text{sgd}(p,q) = 1$, så gäller att p delar a_0 och q delar a_n.

Bevis. Vi kan anta att f är primitivt.

$$f(x) = \left(x - \frac{p}{q}\right) \cdot g(x) \quad \text{reducibelt över } \mathbb{Q}$$

$$\Rightarrow f(x) = \pm (qx - p) \cdot \left(\frac{1}{q} g(x)\right)$$
$$= (qx - p) \cdot h(x)$$

där $h(x)$ har heltalskoefficienter

$\Rightarrow a_0 = -p \cdot$ ~~lägstagrads~~ konstanttermen i $h(x)$

och $a_n = q \cdot$ högstagradskoefficienten i $h(x)$ $\square$

Exempel. $6x^2+x-2$ har möjliga rationella rötter
$(2x-1)(3x+2)$ $\pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{6}$ ~~och~~ och $\pm 1, \pm\frac{1}{2}$
± 2.

x^2-4x+8 har möjliga rötter $\pm 1, \pm 2, \pm 4, \pm 8$.

Ett kriterium för irreducibilitet:

Sats (Eisensteins kriterium)
Om $f(x) = a_n x^n + \ldots + a_0$ har heltalskoefficienter och det finns ett primtal p sådant att:
$p \mid a_i$ för $i<n$, $p \nmid a_n$, $p^2 \nmid a_0$
så är f irreducibelt över $\mathbb{Q}$.

Bevis. Antag att f är reducibelt över $\mathbb{Q}$,
då är f reducibelt över $\mathbb{Z}$,
dvs. $f = g \cdot h$, där g och h har heltalskoefficienter.

$\Rightarrow$ p delar inte högstagradskoefficienterna av g och h
$\Rightarrow$ dock måste alla andra koefficienter av g och h delas med p.
$\Rightarrow$ p^2 delar a_0 $\lightning$ $\square$

Exempel. $5x^3+6x^2-15x-9$
x^4-4x+8
OBS! Kriteriet visar inte att ett polynom är reducibelt!