Kapcsolat $\mathbb{Z}$ és $\mathbb{Q}$ fölötti irred. között.

$2x$ irred $\mathbb{Q}$ fölött (elsőfokú)

nem —"— $\mathbb{Z}$ —"— mert $2\cdot x$ nemtriviális felbontás.

Azért $\mathbb{Z}$ fölött a konstans egyed is számítanak.

<u>Pl</u> $6(x^2-1) = 2\cdot 3\cdot (x-1)(x+1)$ $\mathbb{Z}$ fölött.

<u>Tétel</u>: f irred $\mathbb{Z}$ felett $\Leftrightarrow$

(1) Kiemelhető-e egy egész szám, nem ± 1.
Ha igen, akkor csak akkor lehet irred ha konstans prímszám. Pl $2\in\mathbb{Z}[x]$

(2) Ha nem: PRIMITÍV
lnko(együtthatók) = 1
Ez akkor irred $\mathbb{Z}$ felett, ha $\mathbb{Q}$ felett.

<u>Pl.</u> $3x^7+6x-18 = 3(x^7+2x-6)$ (Sch-I)
nem irred $\mathbb{Z}$ fölött ← ↗ de ezek már irredek $\mathbb{Z}$ fölött

Képzeljük, hogy nincs más szám, csak 0, 1.

$0 \cdot 0 = 0 = 0 \cdot 1 = 1 \cdot 0 \quad , \quad 1 \cdot 1 = 1$

$0 + 0 = 0 \quad , \quad 0 + 1 = 1 + 0 = 1 \quad , \quad 1 + 1 \overset{\text{def}}{=} 0$

Kivonás: $0 - 1 = x \iff x + 1 = 0$

$x = 1 \quad (1 + 1 = 0)$

$\boxed{-1 = 1}$

$x / 1 = x$: osztás.

Polinomok: együtthatók 0, 1 $\quad x^2 + x + 1 = x^2 - x + 1$

$(x+y)^2 = (x+y)(x+y) = x^2 + \underbrace{yx + xy}_{} + y^2$

$= xy + xy =$

$= \underset{\substack{\parallel \\ 0}}{(1+1)} xy = 0$

$\boxed{(x+y)^2 = x^2 + y^2}$

Egyenletmegoldás $\quad x^2 + 1 = 0 \qquad x^2 + x + 1 = 0$

$x^2 + x = 0$

$x^2 + x = x(x \underset{\nearrow +}{-} 1) \qquad \boxed{x = 0, 1} \qquad$ Próbálgatással is!

$x^2 + x + 1$ $\quad x = 0$ nem jó $\quad 0 + 0 + 1 \neq 0$

$x = 1$ — " — $\quad 1 + 1 + 1 = 1 \neq 0$

nincs gyöke (2. fok)

irred!

$x^2 + 1$ $\quad x = 0$ nem, $\quad x = 1$ jó, $\quad 1 + 1 = 0$

	1	0	1
$x = 1$	1	1	0

$x + 1$

$x^2 + 1 = (x - 1)(x + 1)$

$x^2 + 1 = x^2 - 1$ ✓ $\qquad x^2 + 1 = (x + 1)^2$ (tejadék)

Hány polinom van?

Konstans: $0, 1$

Elsőfokú: $x, x + 1$

Másodfokú: $x^2, x^2 + 1, x^2 + x, x^2 + x + 1$ — irred

8 db 3. fokú

x^3, $x^3 + x$, $x^3 + 1$, $x^3 + x + 1$ irred

$x^3 + x^2$, $x^3 + x^2 + x$, $x^3 + x^2 - 1$ irred., $x^3 + x^2 + x + 1$

(4-fokú 2^4 van)

gyök 0 | gyök 1

---

4. fokú, nincs gyöke $\Leftrightarrow$ szorzata $\neq 1$ tagú két páros.

$$x^4 + x^3 + 1$$
$$x^4 + x^2 + 1$$
$$x^4 + x + 1$$
$$x^4 + x^3 + x^2 + x + 1$$

} 4db IRRED??

vem

Példa: $(x^2+1)^2$ Q fölött 4. fokú, nincs gyöke

$\hookrightarrow (x^2 + x + 1)^2$ NEM IRRED

A másik 3 irred.

4. fokú = f · g gr f = gr g = 2

van 1 és 3 elsőfok.

↙ $ax + b$

$-b/a$ gyöke lenne

az eredetinek is.

Most

x	van $x+1$
0	1

gr f = gr g = 2 és f, g-nek nincs gyöke.

$\rightarrow f(x) = g(x) = \boxed{x^2 + x + 1}$

Az eredeti: $(x^2 + x + 1)^2 = x^4 + x^2 + 1$.

HF 5. fokúakat. Pl $x^5 + x + 1 : x^2 + x + 1 = ?$

14 $x^4 + x + 1$ $\mathbb{Z}$ felett, $\mathbb{Q}$ felett

$1 \cdot x^4 + x + 1 = f(x) \cdot g(x)$ $\quad f, g \in \mathbb{Z}(x)$

=

mod 2 $\forall$ együtthatót $\quad f \to \bar{f}$

$u \to 0$ (páros)

$\to 1$ (páratlan) $\quad g \to \bar{g}$

$x^4 + x + 1 = \bar{f}(x) \cdot \bar{g}(x)$

↗ mod (láthatod) $\Rightarrow$ $\bar{f}$ vagy $\bar{g}$ konstans.

$\Rightarrow$ f és g fő együtthatójának szorzata 1

$\Rightarrow$ 2 főegyüttható van

$\Rightarrow$ vagy $f = g$ vagy $f = -g$ $\quad$ vagy $g = -g$.

$\Rightarrow$ $\bar{f}$ konstans $\Rightarrow f$ is $\quad$ így nem

$\bar{g}$ — " — $\Rightarrow g$ is $\quad$ $x^4 + x + 1$ prímitív.

$\mathbb{Z}_2$

$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1

$\mathbb{Z}_5$, $\mathbb{Z}_6$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ora fai: $2 \circ 3 = x$

$\Leftrightarrow 3x = 2$

$x = 4$ $\quad$ $2 \circ 3 = 4$

Unico NULLOMÒDULO.

TEST

(Lin. Ragnucci $3x \equiv 4 \ (7)$)

$\mathbb{Z}_6$, $*_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Nem 0-osztós

$2 \cdot 3 = 0 = 3 \cdot 4$ stb.

$x^2 - x = 0$

gyökei 0, 1, 3, 4

2. fokú, 4 gyök.

Pl. $\mathbb{Z}_8$-ban is $x^2 - 1$ 4 gyök

1, 3, 5, 7

$x^2 - 1 = (x+7)(x+1) = (x+3)(x+5)$

nem elvárt a feltárás!

HF gyöktényező nem euklideszi k.

EGYSZERŰ

Körtési polinom.

$\Phi_n(x)$ n. primitív egységgyök a egyes, minden egyes.

Pl. 4. egy $1, i, -1, -i$

rend $1, 4, 2, 4$

PRIMITÍV

$(x-i)(x+i) = x^2+1 = \Phi_4(x)$.

Tétel: Minden egész együttható

$\Phi_1(x) = x-1$ (1)

$\Phi_2(x) = x+1$ (-1)

Áll: $\prod_{d \mid n} \Phi_d(x) = x^n - 1$.

Példa a számolásra:

$n = 4$

$1, 2, 4 \mid 4$

$\Phi_1(x)\Phi_2(x)\Phi_4(x) = x^4 - 1$

$\underbrace{(x-1)(x+1)}_{x^2-1} \Rightarrow \Phi_4(x) = \frac{x^4-1}{x^2-1} = x^2+1$

$n = 3$

$\Phi_1(x)\Phi_3(x) = x^3 - 1$

$x - 1$

$\frac{x^3-1}{x-1} = x^2 + x + 1 = \Phi_3(x)$

HF p prím $\Phi_p(x) = \frac{x^p-1}{x-1} = 1 + x + x^2 + \ldots + x^{p-1}$

Tábel Ezzel mind ineked.

$\Phi_6(x) = ?$

$1, 2, 3, 6 \mid 6$

$x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6$

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1 \Phi_2 \Phi_3} = \frac{x^6-1}{(x^3-1)(x+1)} =$$

$$= \frac{x^3+1}{x+1} = \boxed{\frac{x^3-1}{x^2-x+1}}$$

$\boxed{\Phi_{16}(x) = ?}$

$\Phi_1 \Phi_2 \Phi_4 \Phi_8 \Phi_{16} = x^{16}-1$

$$\Phi_{16}(x) = \frac{x^{16}-1}{\underbrace{\Phi_1 \Phi_2 \Phi_4 \Phi_8}_{8\text{ alatt: }\, x^8-1}} = \frac{x^{16}-1}{x^8-1} = \boxed{x^8+1}$$

HF Próbáld Φ_{15} explicit.

$\Phi_n(x) = ?$ Visszavezethető n prímtényezőire (csak prím osztók).

$$\Phi_n(x) = \Phi_m\left(x^{n/m}\right)$$

$m \mid n$ $\forall p \mid n$ prím $p \mid m$ " x^2

Pl. $\Phi_{12}(x) = \Phi_6\left(x^{12/6}\right) = x^4 - x^2 + 1$

$m = 6$ $\Phi_6(x) = x^2 - x + 1$

Pl. $\Phi_{16}(x) = \Phi_2\left(x^{16/2}\right) = x^8 + 1$

$m = 2$

$n \to$ négyzetmentesre.

$\phi_{2n}(x) = \phi_n(-x)$

Ha $n > 1$ pár.