2016.02.12

Def. R gyűrű (ring) $(R,+,\cdot)$ műveletek.

$(R,+)$ Abel-csoport $\quad 0\in R,\quad \forall a\in R\ \exists(-a)\in R$

$(R,\cdot)$ asszociatív

$(a+b)c = ac+bc \quad \forall a,b,c\in R$ disztributivitás

$a(b+c) = ab+ac \quad \forall a,b,c\in R$ disztributivitás

Áll. $0\cdot a = a\cdot 0 = 0 \quad \forall a\in R$

B: $0 = 0+0 \qquad a\cdot$

$a\cdot 0 = a\cdot(0+0)$

$a\cdot 0 = a\cdot 0 + a\cdot 0 \qquad +(-(a\cdot 0))$

$0 = a\cdot 0 + 0 = a\cdot 0$ Másik oszlopban. □

Def. Ha $\forall a,b\in R$: $ab = ba \rightarrow R$ kommutatív gyűrű.

Áll. $(-a)b = -ab \quad (1)$

$a(-b) = -ab \quad (2)$

$(-a)(-b) = ab \quad (3)$

B: (1) és (2) $\Rightarrow$ (3)

(1): $0 = (-a)b + a\cdot b = ((-a)+a)b = 0\cdot b = 0$ (2) ugyanúgy □

Def. $e\in R$ balegységelem R-ben, ha $ea = a \quad \forall a\in R$

$e\in R$ jobbegységelem R-ben, ha $ae = a \quad \forall a\in R$

$e\in R$ (kétoldali) egységelem, ha $ae = ea = a \quad \forall a\in R$ (identity)

Észrevétel. Ha e bel., f jel. $\Rightarrow f = ef = e$. $\Rightarrow$ van egyetlen kétoldali egység. $e = f = 1$.

Áll. Ha egyetlen baloegység. van, az kétoldali egység.

Def. Ha $1\in R$ egységelemes gyűrű, $a\in R$-nek $a'\in R$ baliverze, ha $a'a = 1$.

Áll. Ha van bal- és jobbinverz is, az az egyetlen (kétoldali) inverz.

Def. $1\in R$, $a\in R$ egység (unit), ha $\exists a'\in R$: $aa' = a'a = 1$.

Áll. Az egységek csoportot alkotnak (szorzásra), jelük $U(R) = \{a\in R \mid \exists a': aa' = a'a = 1\}$.

Példa: $\mathbb{Z}$ kommutatív egységelemes

K test: $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p$

Def. Test: olyan kommutatív egységelemes gyűrű, amire $U(R) = R\setminus\{0\}$.

Példa: $U(\mathbb{Z}) = \{\pm 1\}$

$U(K) = K\setminus\{0\}$

Def. $R[x]$ az R feletti polinomgyűrű: $R[x] = \left\{\sum_{i=0}^{n} a_j x^j \;\middle|\; a_j\in R\right\}$

Ha $1\notin R \Rightarrow$ veszélyes, $1\cdot x\notin R[x]$

Kérdés: Mik $U(R[x])$ egységei, ha $U(R)$ ismert?

Def. $R[[x]]$ a formális hatványsorok gyűrűje: $R[[x]] = \left\{ \sum_{j=0} a_j x^j \;\middle|\; a_j \in R \right\}$

$R \ni 1$ ajánlatos.
Konvergenciának értelme sincs: topológia kéne hozzá.

Az összeadás és szorzás definíciója természetes.
Minden egyszerűsíthető véges lépésben megkapható.

Áll. $U(R[[x]]) = \left\{ \sum a_j x^j \;\middle|\; a_0 \in U(R) \right\}$ $\quad (1 \in R)$

B: Invertáljuk: $\left(\sum a_j x^j\right)\left(\sum b_\ell x^\ell\right) = 1$

$\Rightarrow \quad a_0 b_0 = 1 \quad \Rightarrow \quad a_0 \in U(R)$.

Ha $a_0 \in U(R) \longrightarrow \exists\, b_0$.
Kell: $a_0 b_1 + a_1 b_0 = 0 \iff a_0 \cdot x = -a_1 \cdot b_0$ megoldható
Ezeket a lépéseket ismételve $\sum b_\ell x^\ell$ előáll.

Példa: $\left(e^x =\right) \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots \in \mathbb{R}[[x]]$ vagy $\mathbb{Q}[[x]]$

$$\frac{e^x - 1}{x} = 1 + \frac{x}{2!} + \frac{x^2}{3!} + \dots$$

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$ inverz definiálva $\longrightarrow$ B_n egyértelműen megadva
Bernoulli-számok

n	B_n
0	1
1	$-\frac{1}{2}$
2	$\frac{1}{6}$
3	0
4	$-\frac{1}{30}$
5	0
6	$\frac{1}{42}$
8	$-\frac{1}{30}$
10	$\frac{5}{66}$
12	$-\frac{691}{2730}$
14	$\frac{7}{6}$
16	$-\frac{3617}{510}$
18	$\frac{43867}{798}$
20	$-\frac{174611}{330}$

„Minden, csak nem szép sima."

Nyilván $B_n \in \mathbb{Q}$.

Minden $2 \nmid n$-re $B_n = 0$. $\quad (n \neq 1)$

$B_{4k} < 0, \quad B_{4k+2} > 0 \quad \forall k$

$\text{nev}(B_{2n}) = \prod_{p-1 \mid 2n} p$, speciálisan $6 \mid \text{nev}(B_{2n})$

A számlálóról fogalmunk sincs.

Észrevétel. R komm. $\Rightarrow$ $R[x]$, $R[[x]]$ komm.

Def. $M_n(R)$ = $n \times n$-es mátrixgyűrű.

Észrevétel. $1 \in R \Rightarrow M_n \ni 1$, de a kommutativitásról álmodni sem érdemes.

Def. $a \in R$ bal oldali nulloszló, ha $\exists\, b \in R \setminus \{0\}$, hogy $ab = 0$.

Def. Ha R-ben $ab = 0 \Rightarrow a = 0$ vagy $b = 0$, akkor R nulloszlómentes.

Példa: testek, $\mathbb{Z}$ nulloszlómentesek.

Példa. $M_n(R)$-ben van nullosztó $\forall n \geq 2$-re.

Def. Legyen A additív Abel-csoport, $\forall a, b \in A$: $ab = 0$. $\rightarrow$ zérógyűrű.

Ha R zérógyűrű $\Rightarrow$ $M_n(R)$ kommutatív, mert zérógyűrű. (De sokan máskor.)

Def. R kommutatív, nullosztómentes $\longrightarrow$ integritási tartomány.
(Hasonlít az egész számokra.)
(Van, aki a definícióba $1 \in R$-et is belevesi.)

Példa. $\mathbb{Z}[\sqrt{d}]$, ahol d négyzetmentes és $0, 1 \neq d$. $\longrightarrow$ $1 \in R$, integritási tart.

Def. $\mathbb{Z}[\sqrt{d}] = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \}$ $0, 1 \neq d$, d négyzetmentes.
A jelölés koherens: lehet úgy gondolni ezekre, hogy $\sqrt{d}$ polinomjai.

Ha $d = -1$ $\longrightarrow$ Gauss-egészek gyűrűje.

Def. Részgyűrű: $R_1 \subseteq R$, R_1 maga is gyűrű ugyanonnan a műveletekre nézve.
Jel: $R_1 \leq R$.

Kell hozzá:
$$\left.\begin{array}{l} a, b \in R_1 \rightarrow a + b \in R_1, \\ 0 \in R_1 \\ a \in R_1 \Rightarrow -a \in R_1 \end{array}\right\} R_1 \text{ részcsoport az összeadásra}$$
$a \cdot b \in R_1$ zárt a szorzásra.

Def. $I \subseteq R$ ideál, ha (részgyűrű) és ha $a \in I$, $r \in R \Rightarrow ar \in I$, $ra \in I$.
$(I, +) \leq (R, +)$ Jel: $I \trianglelefteq R$.

Def. $L \subseteq R$ balideál, ha $(L, +) \leq (R, +)$ és ha $a \in I$, $r \in R \rightarrow ra \in L$.
$J \subseteq R$ jobbideál, ha $(J, +) \leq (R, +)$ és ha $a \in I$, $r \in R \rightarrow ar \in J$

Az ideál felel meg a csoportelméleti normálosztónak.

Def. R_1, R_2 gyűrűk, $\varphi: R_1 \longrightarrow R_2$ hom., ha műveletartó:
$$(a+b)\varphi = a\varphi + b\varphi,$$
$$(ab)\varphi = (a\varphi)(b\varphi) \qquad \forall a, b \in R_1$$

Következik: $0\varphi = 0$, $(-a)\varphi = -(a\varphi)$.

Def. $\operatorname{Ker} \varphi = \{ a \in R_1 \mid a\varphi = 0 \}$

Áll. $\operatorname{Ker} \varphi \trianglelefteq R_1$

B: $(\operatorname{Ker} \varphi, +) \leq (R_1, +)$ és szorzat 0-val 0. $\square$

A megfordítás is igaz lesz.

Def. Faktorgyűrű (maradékosztály-gyűrű): $I \trianglelefteq R$-re $R/I = \{ a + I \mid a \in R \}$.

$(a + I) + (b + I) = (a + b) + I$ $\longrightarrow$ akár reprezentánsként, akár komplexusként
$(a + I)(b + I) = ab + I$ $\longrightarrow$ csak reprezentánsként értelmezendő!

Az R/I valóban gyűrű. Az $R \longrightarrow R/I$, $a \longmapsto a + I$ természetes hom. valóban hom.

$\Rightarrow \forall I \, \exists \varphi$: $\operatorname{Ker} \varphi = I$.

Def. Izomorfizmus: bijektív izomorfizmus.

Tétel. (Homomorfizmustétel). $\varphi: R_1 \to R_2$ -re $\operatorname{Im}\varphi \leq R_2$ -re $\operatorname{Im}\varphi \cong R_1/\operatorname{Ker}\varphi$.

B: Mint csoportoknál.

Def. $R_1, R_2 \leq R \to \langle R_1, R_2 \rangle \leq R$ generált résztyűk.

$X \subseteq R \to \langle X \rangle \leq R$

$$\langle X \rangle = \bigcap_{\substack{R_1 \supseteq X \\ R_1 \leq R}} R_1$$ (Rgy. metszete is at.)

Def. $(X) \lhd R$ generált ideál. Más eseter: (I, J), $(a_1, \dots)$

Ism. Ideálok metszete is ideál; akárhányra.

Áll. $(I, J) = I + J$, ahol $I, J \lhd R$

B: Ha egy ideálban I és J benne van, $I + J$ is.
Kell még, hogy $I + J$ is ideál és $I + J \supseteq I, J$.

$(a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2)$

$r(a + b) = ra + rb$

$I \subseteq I + J$, $a + 0$ alakú elemekkel.

Def. $$I \cdot J = \left\{ \sum_{i=1}^{n} a_i b_j \;\middle|\; a_i \in I,\ b_j \in J \right\}$$ *

(Ez a komplexusszorzat által generált ideál.)

$I \cdot J \lhd R$ felmáll. (a sima komplexusszorzásra nem lenne igaz)

Ism. $IJ \subseteq I \cap J$. (a szorzat kicsi)

Def. Legyen $a \in R$. (a) főideál: 1 elem által gen. ideál.

$$(a) = \left\{ na + ra + as + \sum_{i=1}^{k} r_i a s_i \;\middle|\; n \in \mathbb{Z},\ r, s \in R,\ r_i, s_i \in R \right\}$$

Ezek mind kellenek, és ez más valóban ideál.
$\to$ a főideál ált. alakja nagyon függ R-től.

Ha $1 \in R \to (a) = \left\{ \sum_{i=1}^{k} r_i a s_i \;\middle|\; r_i, s_i \in R \right\}$

Ha R komm. $\to (a) = \{ na + ra \mid n \in \mathbb{Z}, r \in R \}$

Ha $1 \in R$, R komm. $\to (a) = \{ ra \mid R \ni r \} = Ra$ (komplexusszorzat)

Ugyanez elmondható bal- és jobboldalóra is.

Legyen $L_1, L_2 \lhd_b R$. $\Rightarrow$ $L_1 + L_2 \lhd_b R$ és ez a generált baloldalóid

$L_1 \cap L_2 \lhd_b R$ (akárhányra is)

$$L_1 L_2 = \left\{ \sum_{i=1}^{n} a_i b_j \;\middle|\; a_i \in L_1,\ b_j \in L_2 \right\} \lhd_b R$$ (itt elég, hogy $L_2 \leq R$)

Ha $L \triangleleft_b R$, $J \triangleleft_j R$ $\Rightarrow$ $LJ \triangleleft R$. (szellemesen hangzik, de nem rögzült szell

Def. M baloldali modulusa R-nek, ha (baloldali R-mod.)

1) $(M,+)$ Abel

$R \times M \to M$ (r,m) $rm \in M$

2) $(rs)m = r(sm)$

3) $(r+s)m = rm + sm$

$r(m+n) = rm + rn$

Ha $1 \in R$, érdekes hozzávenni: $1m = m$ (unitáris R-modulus)

Mj. Ha csak egységelemes gyűrűt vétnénk, a egy. definíciójában kíne, hogy $1_R \in R$. (ld. gyak. 1/4)

Ez a vektortérre hasonlít: a vektortér test fölötti unitáris modulus. Sokkal izgalmasabb, mint a vektortér.

Egy gyűrűről a moduluszaiból is lehet információt nyerni.

Def. Rismodulus.

Def. Homomorfizmus $(rm)\varphi = r(m\varphi)$ (r a skalár)

Homomorfizmustétel, gen. rismodulus, mag.

Jobboldali ~~rés~~ R-modulus: 2') $m(rs) = (mr)s$ (előbb az elsővel, majd a másodikkal szorozni)

HF: érdekes példákat találni modulusra.

2016.02.18. csütö

Példa: $R = \mathbb{Z}$: $\mathbb{Z}$-modulus $\leftrightarrow$ additívan írt Abel-csoport

$R = K[x]$: az x-szel való szorzás $\leftrightarrow$ lineáris trafó egy K-vektortéren

$\Rightarrow$ a modulus egy K-vektortér egy rögzített lineáris trafóval

${}_RR$, R_R az R fölötti R modulus (bal, jobb)

rétmodulusok: baloldalok / jobboldalok

Def. Modulusok direkt összege: mint csoportokra (belső, külső, 2-re, véges sokra, végtelen sokra)

$\bigoplus_{\alpha \in I} M_\alpha$ (ha I véges: diszjunkt direkt összeg)

Def.

~~Példa~~ $\bigoplus_{\alpha \in I} {}_RR$ szabad modulus.

$$e_\alpha \longrightarrow \bigoplus_R R = \left\{ \sum_{\substack{\alpha \\ \text{véges}}} r_\alpha e_\alpha \;\middle|\; r_\alpha \in R \right\}$$

Legyen D ferdetest (division ring). Bizonyítható, hogy D fölött minden modulus szabad. Sőt: ha minden unitáris modulus szabad $\to R = D$.

Def. M egyszerű, ha csak 0 és M (különbözők) a rétmoduluszai.

Def. R egyszerű, ha az ideáljai $I = 0$ és $I = R$ $(0 \neq R)$

Példa: minden ferdetest egyszerű gyűrű.

Áll. Ferdetestnek nincs nemtrivi baloldali ideálja.

B: $0 \neq a \in D \to Da = D \to (a) = D$.

Def. Gyűrűk direkt összege. $\bigoplus_{\alpha\in I} R_\alpha$

$\longrightarrow$ az egyes direkt összeadandók kétoldali ideálok lesznek.

Tétel. $|R|>1$, $ax=b$ megoldható $\forall a\neq 0,\ b\in R$ (nem kell egyértelműnek lenni)
$\Longrightarrow$ R ferdetest.

B: Először bizonyítjuk a nullosztómentességet.
$0\neq c,d\in R$ tetsz. $\exists x:\ cx=d$
$\exists y:\ dy=x$
$\Rightarrow cdy = cx = d\neq 0 \quad\Rightarrow\quad cd\neq 0.$ ✓

Legyen $0\neq a\in R$. $ax=a$ valamelyik megoldása e.
$ae=a \quad\rightarrow\quad ae^2=ae \qquad a\neq 0 \quad\rightarrow\quad e^2=e$

$t\in R \qquad (t-te)e = te-te^2 = te-te=0, \quad e\neq 0 \quad\Rightarrow\quad t=te$
$\qquad\qquad e(t-et) = et-e^2t = et-e^2t=0, \quad e\neq 0 \quad\Rightarrow\quad t=et$ } egyszerűen

$a\neq 0$, $\exists x:\ ax=e$, $x\neq 0$, mert $e\neq 0$.

$(xa-e)x = xax-ex = xe-ex = 0 \quad\Rightarrow\quad xa=e \quad\rightarrow\quad x$ balinverz is
$\rightarrow$ $\forall$ elemnek van inverze, a^{-1}

Ezzel minden megvan. (És azt is látjuk, hogy $ax=b$-nek egyértelmű a mo.)

Áll. R-ben $\nexists$ balideál $\Rightarrow$ R ferdetest vagy primitív zérógyűrű.
(azaz ${}_RR$ egyszerű)

B: Ezzel jó.

Ha R zérógyűrű $\longrightarrow$ kell, hogy $(R,+)$-nak ne legyen valódi csoportja $\rightarrow (R,+)=\mathbb{Z}_p$.

Ha R nem zérógyűrű: megmutatjuk, hogy NOM.
$\exists a,b\neq 0$, de $ab=0 \longrightarrow$
$0\neq a\in L=\{x\in R \mid xb=0\} \lhd_b R \Rightarrow L=R \Rightarrow \forall x\in R:\ xb=0.$

$0\neq b\in I=\{y\in R \mid Ry=0\}\lhd R \quad\Rightarrow\quad I=R \quad\Rightarrow$ zérógyűrű ↯ ✓

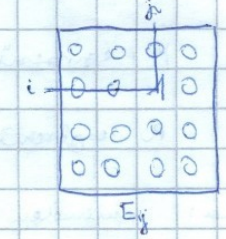
$a\neq 0.\quad Ra=\{xa \mid x\in R\}=R \quad\longrightarrow$ az előző tétel szerint ferdetest.

Köv. R kommutatív, egyszerű $\Rightarrow$ test vagy primitív zérógyűrű.

B: kommutatív ferdetest vagy primitív zérógyűrű.

Áll. Legyen $1\in R$. $I\lhd M_n(R) \iff I=M_n(A)$, ahol $A\lhd R$. (Ez leírja a teljes mátr. ideáljait.)

B: Könnyű látni, hogy ha I ilyen, akkor ideál.



A másik irány a nehezebb. $M=(m_{ij})$. $\quad E_{ij}\,M\,E_{kl} = m_{jk}\cdot E_{il}$,

mert $M=\sum_{j,k} m_{jk}E_{jk}$, $\quad E_{ij}E_{kl}=\delta_{jk}E_{il}$

$A=\{a_{11} \mid (a_{ij})\in I\}\lhd R$

Állítjuk, hogy I a keresett ideál.

$M \in I \to E_{j1} M E_{k1} = m_{jk} E_{11} \Rightarrow m_{jk} \in A$

$\Rightarrow I \subseteq M_n(A)$. Ennek a megfordítása kicsit más.

$(a_{ij}) \in M_n(A) \longrightarrow a_{il} E_{il} \in I$ elég csak ezt belátni.

$M = (m_{ij}) \in I \quad a_{il} = m_{11}$

$j = k = 1$-re: $a_{il} E_{il} = m_{11} E_{il}$

$E_{i1} M E_{1l} \in I$ □

<u>Köv.</u> R egységes $\to M_n(R)$ egységes

Speciálisan $M_n(K)$, $M_n(D)$ egységes.

<u>Def.</u> $a \in R$ nilpotens: $\exists n \geq 1 : a^n = 0$.

<u>Tétel.</u> $1 \in R$, kommutatív, $N(R) = \{ a \in R \mid a \text{ nilpotens} \} \triangleleft R$.
R nilradikálja

B: • a, b nilp. $\Rightarrow a+b$ nilp.

$a^n = b^k = 0 \longrightarrow (a+b)^{n+k-1} = 0$ binomiális tétellel

• $(-a)^n = -a^n = 0$ ✓ $\longrightarrow (N(R), +)$ tört

• $(ra)^n = r^n a^n = 0$ zárt.ág. □

Ellenpélda: ha $R = M_2(K)$: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = 0$, de $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2$ nem nilp.

<u>Megj.</u> $N(R/N(R)) \triangleleft R/N(R)$, ... folytatható, de felesleges: $N(R/N(R)) = 0$.

B: $\bar{x} \in R/N(R) \to \bar{x} = x + N(R)$, $\bar{x}^n = 0$, $x^n \in N(R)$, $(x^n)^k = 0$, $x^{nk} = 0$
$\to x \in N(R) \to \bar{x} = 0$. □

<u>Def.</u> $1 \in R$, kommutatív. $P \trianglelefteq R$ prímideál, ha $x, y \in R$, $xy \in P \Rightarrow x \in P \vee y \in P$.

0 pontosan akkor prímideál, ha R nullosztómentes.

<u>Példa.</u> Legyen $R = \mathbb{Z}$. Ideálok: (n), ahol $n \geq 1$ vagy $n = 0$, $(n) = n\mathbb{Z}$
(n) prímideál $\Leftrightarrow$ n prím vagy $n = 0$.

<u>Példa.</u> $K[x,y]$ (0) prímideál
(x) $\qquad (0) \subset (x) \subset (x,y)$
(x,y) $\longleftrightarrow$ a konstans tag 0

Megj. $K[x_1, \dots, x_n]$-ben legfeljebb n hosszú ideállánc van.

Kritérium. $I \trianglelefteq R$ primideál, $\iff$ R/I NOM. ($1 \in R$, komm.)

B: I nem primideál $\iff \exists x,y \in R \setminus I : xy \in I \iff \exists x,y \in R\setminus I : (x+I)(y+I) = I \iff R/I$ nem NOM

Def. Maximális ideál. $M \trianglelefteq R$: $M \subset A \triangleleft R \to A = R$.

Kritérium. $I \trianglelefteq R$ maximális $\iff$ R/I test. ($1 \in R$, komm.)

B: Komm miatt R/I test $\iff$ nincs nemtriv ideálja. R/I ideáljai $\xleftrightarrow{\text{bij.}}$ R I-t tartalmazó ideáljai.

Mj. Minden maximális ideál prím, mert a testek NOM-ek.
A megfordítás nem igaz: $\mathbb{Z}$-ben (0) prím, de $(0) \subset (p) \trianglelefteq \mathbb{Z}$
(ugyanis: $(k) \subseteq (n) \iff n \mid k$)

Def. Főidéálgyűrű: $1 \in R$ integritási tartomány és benne minden ideál főideál.

Példa: $\mathbb{Z}$, $K[x]$.
Ellenpélda: $K[x,y]$-ban (x,y) nem generálható egyetlen elemmel.

Áll. R főidéálgyűrű $\Rightarrow$ minden nemnulla ideál maximális.

B: $\exists (x) \neq (0)$ primideál. Ha $(y) \supsetneq (x) \Rightarrow x = yz$, $z \in (x)$, $y \notin (x)$.

(x) prím: $\Rightarrow z \in (x) \to z = tx$

$x = ytx \to 1 = yt \Rightarrow (y) = R$ □

Van-e maximális ideál egyáltalán?

Áll. $1 \in R$, $A \trianglelefteq R$ valódi ideál $\Rightarrow \exists M$ maximális id., $A \subseteq M$.

B: $\{I \mid I \triangleleft R, I \neq R, I \supset A\}$ teljesül a Zorn-lemma feltétele, minden lánc uniója A-t tartalmazó ideál.
Miért mindig valódi az unió? Van egységelem: $I \neq R \iff 1 \notin I$.
$\to$ van maximális elem $\to$ az maximális ideál. □

$\forall a \notin U(R)$ $\exists M$ max: $a \in M$, mert $(a) \trianglelefteq R$.

Tétel. $1 \in R$, kommutatív. Ekkor $N(R) = \bigcap_{\substack{P \text{ primideál} \\ R\text{-ben}}} P$.

B: Ha f nilpotens $\to \exists n : f^n = 0 \in P$. $\Rightarrow f \in P$ minden primidéálra. $\Rightarrow \subseteq$

Ha f nem nilpotens: $0 \notin \{f, f^2, \dots\}$

$\{A \triangleleft R \mid A \cap \{f, f^2, \dots\} = \emptyset\}$

P maximális ilyen.

Belátjuk: $f \notin P$: $f^n \in P + (x)$, $x \notin P$. $\quad f^n = p_1 + r_1 x$
$f^k \in P + (y)$, $y \notin P$ $\quad f^k = p_2 + s y$

$f^{n+k} = p_1 p_2 + p_1 s y + p_2 r x + (xy)(rs) \in P$. □

Def. $\mathcal{J}(R) = \bigcap_{\substack{M \text{ max. id} \\ R\text{-ben}}} M \triangleleft R$ Jacobson-radikál

Áll. $a \in R$. $a \in \mathcal{J}(R) \iff 1 - ax \in U(R) \quad \forall x \in R$.

2016.02.26

Ma minden gyűrűre $\boxed{1 \in R}$, és minden modulusra $\boxed{\text{unitárius}}$.

Def

${}_RM$-re teljesül a minimum-feltétel, ha teljesül a következő ekvivalens feltételek bármelyike.

1) M résztermoduluseinak halmazában van minimális (tartalmazásra)
2) $\nexists\, M_1 > M_2 > M_3 > \dots$ szigorúan csökkenő ∞ résztermodulust
2') $M_1 \geq M_2 \geq M_3 \geq \dots \Rightarrow \exists n: \quad M_n = M_{n+1} = \dots$

Ezt másképp artin-modulusnak nevezik (Emil Artin). Az ekvivalenciát egyszerű belátni.
Ugyanígy M_R-re.

Def. ${}_RM$-re teljesül a maximum-feltétel, ha

1) M résztermod. halmazában van maximális
2) $\nexists\, M_1 < M_2 < M_3 < \dots$
2') $M_1 \leq M_2 \leq M_3 \leq \dots \Rightarrow \exists n: \quad M_n = M_{n+1} = \dots$
3) M minden résztermodulusa végesen generált.

1), 2) és 2') ekvivalenciája mint fent.

3) $\Rightarrow$ 2'): $\exists\, M_1 \leq M_2 \leq \dots$, tekintsük $M' = \bigcup_{i=1}^{\infty} M_i \leq M \to$ végesen generált, $M' = \langle a_1, \dots, a_n \rangle$.
$\to a_1 \in M_{i_1}, \dots, a_n \in M_{i_n} \to i = \max(i_1, \dots, i_n)$-re $M_j \ni a_1, \dots, a_n \to M_j = M'$. ✓

2) $\Rightarrow$ 3): $\{ M_0 \leq M$ nem vég gen., $\langle a_1 \rangle = M_0 \to a_2 = M_0 \setminus \langle a_1 \rangle, \dots$
$\to \langle a_1 \rangle < \langle a_1, a_2 \rangle < \langle a_1, a_2, a_3 \rangle < \dots \}$

Más néven noether-modulus (Emmy Noether).

Artin és Noether eszerint eredetileg gyűrűre vonatkozik be: speciálisan ${}_RR$-re

Def. Bal-artin, ha a minimumfeltétel baloldaláldokra teljesül.

Def. Bal-noether, ha a maximumfeltétel baloldaláldokra teljesül.

Nyilván minden véges gyűrű / modulus noether és artin is.

Példa. $\mathbb{Z}$-modulusok között (abel-csoportok):

$\mathbb{Z}_\infty$: $\langle 2 \rangle > \langle 4 \rangle > \langle 8 \rangle > \dots$ nem artin, de noether.

$\mathbb{Z}_{p^\infty}$: $\left\langle e^{\frac{2\pi i}{p}} \right\rangle < \left\langle e^{\frac{2\pi i}{p^2}} \right\rangle < \dots$ nem noether, de artin.

Tétel. (Hopkins–Levitzki) $1 \in R$, R bal-artin $\Rightarrow$ bal-noether. (ugyanígy jobbra is)

Kell, hogy $1 \in R$: ha a $\mathbb{Z}_\infty$-et vagy $\mathbb{Z}_{p^\infty}$-t vesszük mint abel-csoportot a zérógyűrűvel, akkor ellenpéldát kapunk.

Tétel. (Hilbert bázistétele) R egységelemes gyűrű bal-noether $\Rightarrow R[x]$ is balnoether.

B: Balnoether $\iff$ minden baloldaláldok végesen generált. (3))
A bizonyítást kommutatív R-re mondjuk, de könnyű átfogalmazni.

$A \triangleleft R[x]$, $A_n \triangleleft R$, $A_n = \{ a \in R \mid \exists f \in A: \; f - ax^n + \dots \}$ az n-edfokú polinomok főegyütthatói

$a, b \in A_n \to a + b \in A_n$, $(-a) \in A_n$, $ra \in A_n$ $(r \in R)$, az valóban ideál

$A_n \subseteq A_{n+1} \to$ ideálok növekvő lánca.

Noether $\longrightarrow \exists n: A_n = A_{n+1} = \dots$

$A_i = (a_{i_1}, \dots, a_{i_{k_i}})$, $\exists f_{ij}: \quad f_{ij} = a_{ij} x^i + \dots$ (per def.)

Áll. $(f_{01}, \dots, f_{0k_0}, f_{11}, \dots, f_{1k_1}, \dots \dots, f_{n1}, \dots, f_{nk_n}) = A$

Bi. $A \supseteq \langle \dots \rangle$ triviálisan. Legyen $g \in A$, ezt akarjuk felírni f-ekkel.
Indukció $\deg g$ szerint.
$\deg g = 0 \longrightarrow$ def. szerint
$\deg g = j \longrightarrow$ esetek: $j < n$ és $j \geq n$

$g = b x^j + \dots$, $b \in A_j \longrightarrow b = r_1 a_{j1} + \dots + r_j a_{jk_j}$
$f := r_1 f_{j1} + \dots + r_j f_{ej} \in A$

$\Rightarrow g - f \in A$, indukció miatt $j < n$-re megvagyunk. (a vezető tag 0 lesz)

$j \geq n$-re hasonlóan, csak az indexek el vannak eltolva: $g - x^{j-n} f \in A$
(IH a gondolat folytán, leírni nehéz.)
Ezzel a tétel bizonyítását befejeztük.

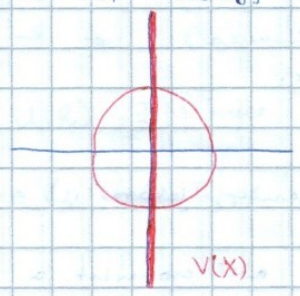
Azért bátris, mert a XIX. században a generátorrendszert listák igy.
Annak idején nagy felzúdulást keltett (1890), az ún. invariánselmélletben

Speciális eset. $K[x_1, \dots, x_n]$ noether.

A bizonyítás nem konstruktív.
Ennek van geometriai interpretációja.
$K^n = \{(a_1, \dots, a_n) \mid a_i \in K\}$ n-dimenziós affin tér

Legyen $X \subseteq K[x_1, \dots, x_n]$. $V(X) = \{(a_1, \dots, a_n) \in K^n \mid f(a_1, \dots, a_n) = 0 \quad \forall f \in X\}$ az X által meghatározott (affin) algebrai halmaz
Algebrai sokaság / varietás: nem bomlik fel kisebb algebrai halmazok unójára.

Példa: $K = \mathbb{R}$, $\mathbb{R}[x,y]$-ban $X = \{f(x,y) = x(x^2+y^2-1)\}$



Nem varietás: $V(X) = V(x) \cup V(x^2+y^2-1)$

$A = (X) \triangleleft K[x_1, \dots, x_n] \Rightarrow V(X) = V(A)$ (a kétoldali tartalmazódás belátásához
$f_i \in X$, g_i tetsz $\longrightarrow g_1 f_1 + \dots + g_k f_k \dots$)

Tekintsük $V(A)$-t. Lehetnek A-n kívüli polinomok, amik mindén eltűnnek rajta.
Határozzuk meg az összest, ami $V(A)$-n eltűnik!
Tfh. K algebrailag zárt, pl. $K = \mathbb{C}$.
(A valamit kitalálni nehézkes, bizonyítani nehéz.)

Mit jelent $K[x_1, \dots, x_n]$-ben a prímideál?

Példa: Minden főidegyűrű Noether (mivelhogy 1 elem generál), például $\mathbb{Z}$.
(De $\mathbb{Z}$ nem artin: $(2) \supset (4) \supset \dots$)

Ismeretlen-e egyáltalán nem véges artin-gyűrűt?

Példa: Legyen D ferdetest. Állítjuk, hogy ekkor $M_n(D)$ balartin-gyűrű.
Ez a következő miatt van:

Tétel: $L \leq_b M_n(D) \iff \exists V \leq_n D$ (a D feletti n-dim balvektortér), hogy $L = \{ V$ sora V-ből való$\}$.

Bi: Az egyik irány könnyű: ha van egy ilyen A-t, akkor TA is ilyen, mert az A sorainak lin. kombja. Ezzel „$\Leftarrow$" beláttatott.

$$\begin{pmatrix} x & & \\ x & & 0 \\ \vdots & & \\ x & & \end{pmatrix} \to (1, 0, \dots, 0)$$

$$\begin{pmatrix} 0 & \overset{i}{x} & 0 \\ & \vdots & \\ & x & \end{pmatrix} \to (0, \dots, \overset{i}{1}, \dots, 0)$$

A mátrix irány beláttatásához konkrétan megadjuk V-t.

V legyen azon vektorok tere, amik 1. sorként előfordulnak L-beli mátrixokban.
Összeadásra zártság triv.
Skalárral szorzás balról: $\begin{pmatrix} r & 0 \cdots 0 \\ & 0 \end{pmatrix} A = \begin{pmatrix} ra_{11} & \cdots & ra_{1n} \\ & \vdots & \end{pmatrix}$

Legyen $A = \begin{pmatrix} \sim\sim \\ \vdots \end{pmatrix}$. $i\text{-}\begin{pmatrix} 0 \\ \sim\sim \\ 0 \end{pmatrix} \in L$, mert $\begin{pmatrix} 0 & & \\ \vdots & & \\ i \to 1 & & 0 \\ \vdots & & \\ 0 & & \end{pmatrix} A$.

Tehát V-beliek L-ben vannak.

Kell még, hogy L-ben minden egyéb elem.

$$\begin{pmatrix} 0 \cdots \overset{i}{1} \cdots 0 \\ 0 \end{pmatrix} \begin{pmatrix} \sim\sim \\ \vdots \end{pmatrix} \in \quad \to \text{ első sorként ott van.}$$

□

Az alterek lánca $\leq n+1$ hosszú $\to$ balartin-gyűrű lesz $M_n(D)$.

Mj.: $\exists R$ balnoether, de nem jobbnoether. (És nyilván fordítva is.) Hasonló kérdés artinra.
Adjunk példákat!

Továbbra is $\boxed{1 \in R}$ és a modulusok $\boxed{\text{unitális balos}}$.

<u>Def.</u> M féligegyszerű modulus, ha $\forall N \leq M \quad \exists N^* \leq M : \quad M = N \oplus N^*$, azaz minden résztermodulus direkt összeadandó.

<u>Áll.</u> M féligegyszerű, $M \geq M_1 \Rightarrow M_1$ féligegyszerű.

B: $N \leq M_1$, $\quad M_1 = N \oplus N^{**}$, $\quad N^{**} = M_1 \cap N^*$ (állítjuk)

Világos, hogy $N, N^{**} \leq M_1$ és diszjunktak, hiszen $N^{**} \subset N^*$, $N^* \cap N = \emptyset$.

Minden elemük: $x = a + b \quad a \in N, \quad b \in N^*$
$b = x - a \in M_1, \quad \longrightarrow b \in N^{**}$

<u>Áll.</u> M féligegyszerű, $N \leq M \Rightarrow M/N$ féligegyszerű.

B: Ujjgyakorlat.

<u>Lemma.</u> Minden féligegyszerű nemnulla modulus tartalmaz egyszerű résztermodulust.

B: M féligegyszerű. $0 \neq m \in M$.

$\{ N_1 \leq M \mid m \notin N_1 \} \neq \emptyset$, mert pl. $N_1 = (0)$.

Teljesül rá a Zorn-lemma feltétele. N a maximális ilyen, $m \notin N$.

$M = N \oplus N^*$. Állítjuk, hogy N^* egyszerű. (Láthatóan $N^* \neq (0)$.)

$\lightning$ $0 < L < N^*$. $\quad N^*$ féligegyszerű $\Rightarrow N^* = L \oplus L^*$. $\quad 0 < L^* < N^*$.

Nézzük $N \oplus L$-et és $N \oplus L^*$-ot! $\quad N \oplus L > N$
$N \oplus L^* > N$

$m = n_1 + l = n_2 + l^*$ (mert N maximális m-et nem tartalmazó volt)

De $\oplus$-ben a felírás egyértelmű $\rightarrow l = l^* \rightarrow l = l^* \in L \cap L^* = 0$
$\Rightarrow m = m_1 = m_2 \in N$ $\lightning$

Tehát N^* egyszerű.

<u>Tétel:</u> M baloldali R-modulus. A következők ekvivalensek:
1) M féligegyszerű.
2) $M = \bigoplus M_\alpha$, $\quad M_\alpha$ egyszerű, $\quad (\alpha \in I)$
3) $M = \sum M_\alpha$, $\quad M_\alpha$ egyszerű. $\quad (\alpha \in I)$

2016.03.04.

B: 1) $\Rightarrow$ 3) $\quad M^* = \sum_{\substack{M_\alpha \leq M \\ M_\alpha \text{ egyszerű}}} M_\alpha \leq M$. $\lightning$ Ha $M^* < M \longrightarrow M = M^* \oplus N$, $\quad N \neq (0)$.

De N f.e. $\longrightarrow N$-ben van egyszerű, de az M^*-ben is benne kell lennie $\lightning$

3) $\Rightarrow$ 1) $\quad M = \sum_{\alpha \in I} M_\alpha$. Legyen $N \leq M$.

$$\left\{ J \subseteq I \;\middle|\; \sum_{\beta \in J} M_\beta \text{ direkt összeg}, \; N \cap \bigoplus_{\beta \in J} M_\beta = 0 \right\}$$

Teljesül a Zorn-lemma, minden lánc uniója is ilyen.

$\rightarrow$ legyen J egy maximális elem.

$M' = N \oplus \left(\bigoplus_{\beta \in J} M_\beta \right)$ Szerintünk: $M' = M$. $\lightning$ Tfh. $M' < M$.

$\rightarrow$ $\exists \alpha : M_\alpha \not\leq M'$. M_α egyszerű, $M_\alpha \cap M' \neq M'$ $\Rightarrow$ $M_\alpha \cap M' = 0$.

$\Rightarrow$ $M' \oplus M_\alpha > M'$ $\rightarrow$ J nem volt maximális $\lightning$

2) $\Rightarrow$ 3) triviális.

3) $\Rightarrow$ 2) A 3) $\Rightarrow$ 1) bizonyítást alkalmazzuk $N = 0$-ra. $\square$

Továbbra is: $\boxed{1 \in R}$, a modulusok $\boxed{\text{unitálisak}}$.

<u>Tétel.</u> R-re ekvivalensek:

1) $\forall$ R-modulus félegyszerű
2) $\forall$ végesen generált R-modulus félegyszerű
3) $\forall$ ciklikus (1 elem által generált) R-modulus félegyszerű
4) ${}_R R$ félegyszerű

<u>Mj:</u> M ciklikus $\Leftrightarrow$ $M \simeq R/L$ $r \longmapsto rm$, homomorfizmustétel erre
$\langle m \rangle = Rm$ cikl.

B: 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 4) triviális. (, provokatíve egy vonal felsorolva")

4) $\Rightarrow$ 1) $M = \sum_{m \in M} Rm$ $\square$

<u>Def.</u> Ha a fentiek bármelyike teljesül, R félegyszerű gyűrű. (bal-félegyszerű)

<u>Áll.</u> D ferdetest, $M_n(D)$ félegyszerű gyűrű $(n \geq 1)$

B: Elég belátni, hogy minimális baloldalok direkt összege.

$\left(\begin{smallmatrix} \circ & \circ \\ \circ & \circ \end{smallmatrix} \right) \oplus \left(\begin{smallmatrix} \circ & \circ \\ \circ & \circ \end{smallmatrix} \right) \oplus \dots \oplus \left(\begin{smallmatrix} \circ & \circ \\ \circ & \circ \end{smallmatrix} \right)$ Ezek minimálisak és valóban kiadják $M_n(D)$-t.
(Használtuk a korábbi tételt a baloldalokról.) $\square$

<u>Mj.</u> R fegyszerű. $\Rightarrow$ $R = L_1 \oplus L_2 \oplus \dots \oplus L_n$ minimális baloldalok

B: $R = \bigoplus_{\alpha \in I} L$. $R \ni 1 = e_1 + \dots + e_n$, $e_i \in L_i \triangleleft_b R$, ezek min. baloldalok.

Állítjuk: $R = L_1 \oplus \dots \oplus L_n$. $\lightning$ $r \in L_\alpha \neq 0$. $r = r \cdot 1 = re_1 + \dots + re_n$, $re_i \in L_i$ $\lightning$

<u>Def.</u> G csoport, $1 \in R$ gyűrű. $RG = \left\{ \sum_{j=1}^{n} r_j g_j \;\middle|\; g_1, \dots, g_n \in G,\ r_1, \dots, r_n \in R \right\}$ csoportgyűrű

Formális összeg, értelmezhetőek benne műveletek (disztributivitás), a csoportelemek felcserélhetőek a gyűrűelemekkel $(rg)(sh) = (rs)(gh)$

RG egységelemes: $1 = 1_R \cdot 1_G$.

<u>Példa.</u> $\mathbb{Z}G$, $\underbrace{KG}_{\text{csoportalgebra}}$. Igazán érdekes, ha $|G| < \infty$, ill. ha R kommut.

<u>Def.</u> A K-algebra, ha A vektortér K felett és A gyűrű. (a két összeadás megegyezik)
$a, b \in A$, $\alpha \in K$: $(\alpha a)b = a(\alpha b) = \alpha(ab)$.

<u>Példa.</u> $M_n(K)$, $K[x]$, KG
$\downarrow$ $\downarrow$ $\downarrow$
$\dim = n^2$ $\dim = \infty$ $\dim = |G|$, ha $|G| < \infty$

Gyakran feltesszük, hogy A is egységelemes.
Ekkor $\alpha \in K \to \alpha \cdot 1 \in A \Rightarrow$ a gyűrű minden ideálja altér.

<u>Tétel</u>. (Maschke) $|G| < \infty$, K test, $\mathrm{char}(K) \nmid G$. $\Leftrightarrow$ KG féligegyszerű.
(A megfordítást nem bizonyítjuk.)

<u>Mj.</u> $U(RG)$-ben $r \in U(R)$, $g \in G$-re $(rg)^{-1} = r^{-1} g^{-1}$. $\therefore$ rg triviális egység.
HF: $\mathbb{Z}\mathbb{Z}_n \simeq \mathbb{Z}[x]/(x^n - 1)$. $n = 3$-ra $U(\mathbb{Z}\mathbb{Z}_3) = \{\pm 1, \pm a, \pm a^2\}$
$\mathbb{Z}_n = \{1, a, \dots, a^{n-1}\}$ $U(\mathbb{Z}\mathbb{Z}_5)$-ben van nemtriviális egység.

B: Elég belátni, hogy KG mint önmaga felett jobbmodulus félegyszerű.
Általánosabban: V KG-modulus (jobboldali), $\dim_K V < \infty$ félegyszerű.

$W \leq V$ tetsz. $\Rightarrow$ $V = W \oplus U_0$. U_0 csak altér, de nem résztmodulus V-ben. (csak K-vektortérre.)
Addig alakítjuk, míg résztmodulus nem lesz.

$\varphi : V \to W$ $v = x + y$, $x \in W$, $y \in U_0$-ra $\varphi(v) = x$. vetítés.
φ lineáris leképezés, de nem modulushomomorfizmus. Csináljunk belőle egyet.

$\vartheta : V \to W$. $\vartheta(v) = \frac{1}{|G|} \cdot \sum_{g \in G} \varphi(vg) g^{-1}$

$v \in V \to vg \in V \to \varphi(vg) \in W \to \varphi(vg) g^{-1} \in W$. Az összeg a feltétel miatt értelmes.
ϑ lineáris leképezés, és ez már modulushomomorfizmus lesz. Ezt most bizonyítjuk.

$\vartheta(va) = \vartheta(v) a$ $\forall a \in KG$ $\longleftarrow$ kell.
Elég: $\vartheta(vh) = \vartheta(v) \cdot h$ $\forall h \in G$ (mert a skalárral felcserélhető)

$$\vartheta(vh) = \frac{1}{|G|} \cdot \sum_{g \in G} \varphi(vhg) g^{-1} = \underbrace{\left(\frac{1}{|G|} \sum_{g \in G} \varphi(vhg) (hg)^{-1} \right)}_{\vartheta(v)} h$$

$\vartheta(v)$, mert amikor g fut, úgy hg is fut G-n.

Tehát ϑ mindomomorfizmus.

$w \in W \Rightarrow wg \in W \to \varphi(wg) g^{-1} = wgg^{-1} = w \Rightarrow \vartheta(w) = w$

$U = \mathrm{Ker}\, \vartheta \leq V$ résztmodulus. Állítjuk: $V = W \oplus U$. Ebből köv, hogy V félegyszerű.
(hiszen ennek W diszjunkt összeadandó)

$\vartheta(\vartheta(v)) = \vartheta(v)$ $\forall v \in V$ (idempotencia)

$$v \in V \to v = \underbrace{\vartheta(v)}_{\in W} + \underbrace{(v - \vartheta(v))}_{\in \mathrm{Ker}\, \vartheta = U}$$

$\vartheta(v - \vartheta(v)) = \vartheta(v) - \vartheta(v) = 0$

Kell még, hogy $W \cap U = 0$.
$w \in W \cap U \to w = \vartheta(w)$ és $\vartheta(w) = 0 \Rightarrow w = 0$. $\square$

Ennek épül a csoportok reprezentációelméletre.

<u>Def.</u> $Z(R) = \{ r \in R \mid rt = tr \quad \forall t \in R \}$ centrum.
A centrum mindig résztgyűrű, de sajnos nem ideál sincs soha. (minden egységelemes nemkommut. gyűrűre nem ideál)
Mi $Z(KG)$?
Nem csak résztgyűrű, hanem résztalgebra is. $\to$ van dimenziója.

$C_1 = \{1\}, C_2, \dots, C_k$ a konjugáltosztályok, $k = k(G)$

$C_j = \sum_{x \in C_j} x \in KG$. Állítjuk, hogy ez bázis: $Z(KG) = \left\{ \sum_{j=1}^{k} \alpha_j C_j \,\middle|\, \alpha_j \in K \right\}$,

Tehát $\dim_K(Z(KG)) = k(G)$

$a = \sum_{g \in G} \alpha_g \cdot g \in Z(KG)$ $\quad h^{-1} a h = a \quad \forall h \in G$

g együtthatója α_g, illetve $\alpha_{hgh^{-1}}$ $\rightarrow$ az azonos konjugáltosztályban levők eltője azonos lesz

Tehát ha centrumbeli, akkor így írható.
És ha így írható, biztosan centrumbeli.

Most legyen $1 \in R$, nem felt. kommutatív.

<u>Def.</u> $J(R) = \bigcap$ maximális baloldali ideálok. (Ez kommutatívra visszaadja az eredeti def.)

<u>Tétel.</u> $a \in R$-re ekvivalensek:

1) $a \in J(R)$
2) $\forall x \in R$: $1 - xa$-nak van balinverze
3) $aM = 0$ $\forall M$ egyszerű modulusra (azaz $\forall m \in M$: $am = 0$)

B: 1) $\Rightarrow$ 2): $\lightning$ $\exists x \in R$: $1 - xa$-nak nincs balinverze: $R(1-xa) \subset_{\triangleleft_b} R$ valódi
$\exists L$ maximális ideál: $1 - xa \in L$. $a \in L \rightarrow xa \in L \rightarrow 1 \in L \rightarrow L$ nem max. $\lightning$

2) $\Rightarrow$ 3): $\lightning$ M egyszerű, de $\exists m \in M$: $am \neq 0$. $\rightarrow$ $Ram = M$, mert M egyszerű.
$\rightarrow$ $\exists x \in R$: $xam = m$ $\rightarrow$ $(1 - xa)m = 0$ $\rightarrow$ $m = 0$ $\lightning$

3) $\Rightarrow$ 1): $L \triangleleft_b R$ maximális $\rightarrow$ $R/L \cong M$ egyszerű modulus.
$\rightarrow$ $a \cdot R/L = 0$ $\Leftrightarrow$ $a \in L$. $\rightarrow$ $a \in J(R)$. $\square$

Eddig csak bal-Jacobsonról beszéltünk. Nyilván ugyanúgy mondjuk jobb-Jacobsonra.
Be tudjuk látni ezek ekvivalenciáját.

2') $1 - xay \in U(R)$ $\forall x, y \in R$. jobb feltétel.

2') $\Rightarrow$ 2): nyilván: $y = 1$-et választva.
1) $\Rightarrow$ 2'): ezt akarjuk belátni

<u>Áll.</u> $J(R) \triangleleft R$ (a bal-Jacobsonra)
B: 3) átfogalmazható. $J(R) = \bigcap_{M \text{ egysz.}} \mathrm{Ann}(M)$

<u>Def.</u> $\mathrm{Ann}(M) = \{ r \in R : rM = 0 \}$ annullátor-ideál

Könnyen látható: $\mathrm{Ann}(M) \triangleleft R$. Ideálok metszete ideál $\rightarrow$ $J(R) \triangleleft R$. $\square$

<u>Áll.</u>
1) $\Rightarrow$ 2'): $a \in J(R) \Rightarrow ay \in J(R)$ (ideál) $\exists u$: $u(1 - xay) = 1$
$xay \in J(R)$ (ideál) $\rightarrow$ $u = \underbrace{1 + u(xay)}_{1 - u(-xay)}$ $\exists$ balinverz: v: $vu = 1$.
$\Rightarrow$ $1 - xay$ szétoldali inverze $u = v$. $\square$

2016. 03. 11.

Most integritási tartományokat és testeket nézünk.

<u>Tétel</u>. R integritási tartomány $\Rightarrow \exists! K$ test, $R \leq K$, $\forall a \in K\ \exists c, d \in R$: $a = \frac{c}{d}$
(Ez nyilván a legszűkebb tartalmazó test.)

B: A gondolat természetes: vegyük a formális hányadosokat.

$$\left\{ (a, s) \;\middle|\; a, s \in R,\ s \neq 0 \right\}$$

$(a, s) \sim (b, t) \iff at = bs$ Az ekvivalencareláció-tulajdonság belátása nélkül.

$(a, s) \sim (b, t)$ és $(b, t) \sim (c, u) \iff at = bs$ és $bu = ct$
$\Rightarrow atu = bsu$ és $bus = cts \Rightarrow (au - cs)t = 0 \Rightarrow au = cs$.
Itt erősen használjuk a NOM-ot. ($\exists$ általánosabb konstrukció is, hányadosgyűrűt ad)

$\overline{(a, s)} = \frac{a}{s}$ jelölés az osztályra.

$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$ és $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ $\rightarrow$ a definíció értelmes és reprezentánsfüggetlen. (nélkül)

$K = \left\{ \frac{a}{s} \;\middle|\; s, a \in R,\ s \neq 0 \right\}$ ezekkel a műveletekkel. $\rightarrow$ gyűrű (nélkül)

$\left(\frac{a}{s}\right)^{-1} = \frac{s}{a}$ $(a \neq 0)$ van inverz

$\frac{as}{s} \leftrightarrow a \Rightarrow R \leq K$. $\square$

<u>Def</u>. K az R hányadosteste.

<u>Példa</u>. $\mathbb{Z} \rightarrow \mathbb{Q}$, $K[x] \rightarrow K(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p, q \in K[x],\ q \neq 0 \right\}$

$K[[x]] \rightarrow$ Laurent-sorok: $\sum_{j=-n}^{\infty} a_j x^j$

<u>Állítás</u>. R tetszőleges gyűrű $\Rightarrow \exists R_1$ egységelemes gyűrű, hogy $R \triangleleft R_1$.

B: A konstrukció itt is természetes: formális $n + a$ alakú elemek.

$$\left\{ (n, a) \;\middle|\; a \in R,\ n \in \mathbb{N} \right\} = R_1 \qquad (n, a) + (k, b) = (n + k, a + b)$$
$$(n, a) \cdot (k, b) = (nk, ka + nb + ab)$$

Rutin: ez valóban gyűrű.
$(1, 0)$ egységelem

$\{(0, a) \mid a \in R\} \cong R$, $\{(0, a) \mid a \in R\} \triangleleft R_1$. $\square$

Ennek – a fentivel szemben – csak elméleti jelentősége van.

Megjegyzés: $\exists$ nemkommutatív NOM gyűrű, ami nem ágyazható be ferdetestbe. (Malcev)
(a NOM nyilván szükséges feltétel)

Most koncentráljunk testekre. Később míg vissza fogunk térni az általános gyűrűre.

<u>Def.</u> $L|K$ testbővítés: $K \leq L$.

Ekkor L automatikusan vektortér K felett.

<u>Def.</u> L mint K-vektortér dimenziója a testbővítés foka: $\dim_K L = (L:K)$.

$\mathbb{C}|\mathbb{Q} \longrightarrow (\mathbb{C}:\mathbb{Q}) = \infty$
$\mathbb{C}|\mathbb{R} \longrightarrow (\mathbb{C}:\mathbb{R}) = 2$

<u>Def.</u> Véges bővítés: $(L:K) < \infty$.

<u>Tétel.</u> (Fokszámtétel) $K \leq L \leq M \Rightarrow (M:K) = (M:L)(L:K)$ (végtelent is beleértve)

B: $(M:L) = n$
$(L:K) = m$
M bázisa L felett $\alpha_1, \dots, \alpha_n$
L bázisa K felett $\beta_1, \dots, \beta_m$
Állítjuk, hogy $\alpha_i \beta_j$ M bázisa K felett.
Ez könnyen láthatóan generátorrendszer.
Lin. füg., mert α-ra rendezve az együtthatók 0-k. $\rightarrow$ □

„Pense le lehet írni, csak miért?

<u>Köv.</u> Primfokú bővítésnek nincs közbülső test. □

Adott $L|K$ bővítés, $\alpha \in L$. $\longrightarrow$ $\exists f(x) \in K[x]$, $f \neq 0$, $f(\alpha) = 0$ (I.)
$\nexists f$ (II.)

<u>Def.</u> Ha $\exists f$, amiben α gyöke, akkor α algebrai K felett.
Különben α transzcendens K felett.

I. $I = \{ g(x) \in K[x] \mid g(\alpha) = 0 \} \trianglelefteq K[x]$, tudjuk, hogy $K[x]$ főtetőgyűrű
$\Rightarrow I = (p(x))$

$p(x)$ egyértelmű konstans szorzó erejéig $\rightarrow$ válasszuk az 1 főegyütt (konvenció)
$\rightarrow p(x) = x^n + a_{n-1} x^{n-1} + \dots + a_0$, $a_i \in K$.

<u>Def.</u> $p(x)$ α kanonikus polinomja.

Automatikus: $p(x)$ irreducibilis $K[x]$-ben. (Fordítva is igaz: az ilyen polinom kanonikus.)

<u>Példa.</u> $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt{2}$. $\rightarrow p(x) = x^2 - 2$ kanonikus polinom.

<u>Jelölés.</u> Ha $L|K$, $\alpha_1, \dots, \alpha_r \in L \longrightarrow K(\alpha_1, \dots, \alpha_r)$ a legszűkebb ezeket tartó bővítés.
($\exists$, mert résztestek metszete résztest)

$K(\alpha)$: α adjunkciója K-hoz.

<u>Áll.</u> $L|K$, $\alpha \in L$ algebrai, $p(x)$ kan. pol. $\Rightarrow K(\alpha) \simeq K[x]/(p(x))$

B: $K[x] \longrightarrow K(\alpha)$
$f \longmapsto f(\alpha)$ homomorfizmus. Homomorfizmustétel.
α polinomjai nyilván $K(\alpha)$-ban vannak. Ennek testet is alkotnak:
$p \nmid f, \rightarrow (f,p) = 1 \longrightarrow f(x)u(x) + p(x)v(x) = 1 \longrightarrow f(\alpha)u(\alpha) = 1$, van inverz. □

Köv. $(K(\alpha):K) = \deg p$, sőt $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ bázis, ahol $n = \deg p$.
$K(\alpha)$-nak K felett

B: $f = pq + r \longrightarrow f(\alpha) = r(\alpha)$, $\deg r < n \longrightarrow$ gyr.
Lineáris, mert p kanonikus.

Def. $L|K$ algebrai, ha $\forall \alpha \in L$ algebrai K felett.

Áll. Minden véges bővítés algebrai.

B: $L|K$, $(L:K) = m < \infty$. $\alpha \in L \rightarrow 1, \alpha, \alpha^2, \dots, \alpha^m$ lin. öf. $\rightarrow \alpha$ algebrai.

Ezzel az is kijött, hogy ha $K \leq K(\alpha) \leq L$, akkor $(K(\alpha):K) \mid m$.

Tétel. $L|K$ adott, $\alpha, \beta \in L$ algebraiak $\Longrightarrow$ $\alpha+\beta$, $-\alpha$, $\alpha\beta$, $\frac{1}{\alpha}$ is algebrai (hányados csak $\alpha \neq 0$)

B: $K(\alpha)|K$ és $K(\beta)|K$ véges bővítés
Felsőfokú: $(K(\alpha\beta):K) = \underbrace{(K(\alpha\beta):K(\beta))}_{(K(\beta)(\alpha):K(\beta)) \leq K(\alpha):K} \cdot \underbrace{(K(\beta):K)}_{\text{véges}}$ } véges.

Többi nyilvánvaló.

Köv. $K_0 = \{\alpha \in L \mid \alpha$ algebrai K felett$\} \leq L$, $K \leq K_0$

Specialisan: $K = \mathbb{Q}$, $L = \mathbb{C} \Rightarrow \mathbb{A} = \{\alpha \in \mathbb{C} \mid \alpha$ algebrai $\mathbb{Q}$ felett$\} < \mathbb{C}$
$\mathbb{A}$ az algebrai számok teste. (más jelölés: $\overline{\mathbb{Q}}$)

Mj. $|\mathbb{A}| = \aleph_0$.

Transcendens: $x \notin \mathbb{A}$. Pl. $\pi, e \notin \mathbb{A}$.

Legyenek $L_1|K$, $L_2|K$ adottak.
Def. $L_1|K \simeq L_1|K$, ha $\exists \varphi: L_1 \longrightarrow L_2$ izomorfizmus, $\varphi|_K = id_K$.

Def. $L|K$ egyszerű, ha $\exists \alpha \in L: L = K(\alpha)$ (egyetlen elem adjunkciója)

Egyszerű bővítések adjunkciója irreduc.

Áll. $\alpha, \beta \in L$, kan. pol. p egyenlő $\Rightarrow K(\alpha)|K \simeq K(\beta)|K$
B: triv

A megfordítás nem igaz! $\sqrt{2}$ kan. pol. $x^2 - 2$
$\sqrt{2}+1$ —"— $x^2 - 2x - 1$,
de $\mathbb{Q}(\sqrt{2})|\mathbb{Q} = \mathbb{Q}(\sqrt{2}+1)|\mathbb{Q}$, nem is csak izomorfizmus!

Hány nem ro transcendens egyszerű bővítés van? Végtelen sok:

Áll. t tr. K felett. $\Rightarrow K(t)|K \simeq K(x)|K$

B: $K[x] \longrightarrow K[t]$ izo, mert t trc. $\longrightarrow$ kiterjed a hányadostestre is.
$f \longmapsto f(t)$

Egyszerű alg bővítés minden eleme algebrai.
Áll. $\alpha \in K(t)$, $\alpha \notin K \Rightarrow \alpha$ trc. K felett.
(HF)

Legyen $f \in K[x]$. $\exists ?\ L \supseteq K$: $\exists \alpha \in L$: $f(\alpha) = 0$.

<u>Tétel.</u> $f \in K[x]$. $\Rightarrow$ $\exists\ L \supseteq K$ $\exists \alpha \in L$ $f(\alpha) = 0$.

B: $f = p_1 \cdots p_n$ irreducibilisek. Tekintsük $K[x] / (p_1(x))$-et!

$(p_1(x))$ maximális ideál $K[x]$-ben $\Rightarrow$ a faktorgyűrű test, ez lesz L.

$\alpha = x + p_1(x) \in L$ $\square$

Ezt kellően továbbvive gyűrűtényezős felbontás is nyerhető.

<u>Tétel.</u> e transzcendens (Hermite 1873)

B: $\lightning$ e algebrai $\rightarrow$ $a_m e^m + \dots + a_1 e + a_0 = 0$, $a_i \in \mathbb{Z}$, $a_m \neq 0$, $a_0 \neq 0$
(ha van rac., van egész eh. polinom is)

$$f(x) = \frac{x^{p-1}(x-1)^p (x-2)^p \cdots (x-m)^p}{(p-1)!}$$ (p prímszám)

$\rightarrow \deg f = mp + p - 1$.

$$F(x) = f(x) + f'(x) + \dots + f^{(mp+p-1)}(x)$$

$$\frac{d}{dx}\left(e^{-x} \cdot F(x)\right) = e^{-x} \cdot \left(F'(x) - F(x)\right) = -e^{-x} \cdot f(x)$$ (itt használjuk ki, hogy e-ről van szó)

$$a_j \int_0^j e^{-x} \cdot f(x)\,dx = a_j \left[-e^{-x} \cdot F(x)\right]_0^j = a_j F(0) - a_j e^{-j} F(j)$$

$$\sum_{j=0}^{m} a_j e^j \int_0^j e^{-x} f(x)\,dx = F(0) \cdot \underbrace{\left(\sum_{j=0}^{m} a_j e^j\right)}_{0} - \sum_{j=0}^{m} a_j F(j) = -\sum_{j=0}^{m} \sum_{i=0}^{mp+p-1} a_j f^{(i)}(j)$$

$f^{(i)}(j) \in \mathbb{Z}$ $(j \neq 0)$ Az általánosított nomatrabány szerint megszondoljuk: $p \mid f^{(i)}(j)$
(ezt sok 0, csak akkor nem 0, amikor a deriválás és a szorzás egyező)

Ha $j = 0$, majdnem ugyanez történik: $i = p-1$-re $(-1)^p \cdot \dots (-m)^p$,
minden másra: 0 vagy $p \mid$.

$\Rightarrow$ $-\sum\sum a_j f^{(i)}(j) = K \cdot p + (-1)^p \cdot \dots (-m)^p$. alkalmas K-ra.

Most megválasztjuk p-t: $p > \max(m, |a_0|)$

Már csak az integrált kell becsülni:

$$|f(x)| \leq \frac{m^{mp+p-1}}{(p-1)!}, \text{ ha } 0 \leq x \leq m \Rightarrow \sum_{j=0}^{m} a_j e^j \int_0^j e^{-x} f(x)\,dx \leq \sum_{j=0}^{m} |a_j| e^j \cdot j \cdot \frac{m^{mp+p-1}}{(p-1)!}$$

$p \to \infty$ a prímszámokon $\Rightarrow$ a felső becslés 0-hoz tart (exp vs. faktoriális),
de ezek nemnulla egész számok $\lightning$ $\square$

A π transzcendenciájának bizonyítása hasonló elvű, de bonyolultabb.

Def. $\alpha \in \mathbb{C}$ algebrai egész, ha $\exists\, f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, hogy $f(\alpha) = 0$.

Algebrai egészek halmaza: Ω

Áll. $\Omega \cap \mathbb{Q} = \mathbb{Z}$

B: $\mathbb{Z} \subset \Omega \cap \mathbb{Q}$ triviálisan: n gyöke $x - n$-nek.

Tfh. p/q gyök $\longrightarrow$ $p^n + a_{n-1}p^{n-1}q + \dots + a_0 q^n = 0$ $\Rightarrow$ $q \mid p^n$ $\rightarrow$ $q = 1$.

Köv. $\Omega \subsetneq \mathbb{A}$ és Ω nem lehet test.

Tétel. Ω gyűrű.

16.03.18.

B: $\alpha \in \Omega \Rightarrow (-\alpha) \in \Omega$

1. lemma. $X = \{\alpha_1, \dots, \alpha_n\} \subset \Omega$, $\Rightarrow \exists S$ gyűrű: $\mathbb{Z} \leq S \leq \mathbb{C}$, $X \subseteq S$, S mint $\mathbb{Z}$-modulus vég. gen.

B: $\alpha_i^{n_i} = f_i(\alpha_i)$ $\quad \deg f_i \leqq n_i - 1$

$\{\alpha_1^{k_1} \dots \alpha_n^{k_n} : 0 \leq k_i < n_i\}$ által generált $\mathbb{Z}$-modulus legyen S

$\rightarrow$ vég. gen., $X \subseteq S$ automatikus

Kell még, hogy S gyűrű.

2. Lemma. S gyűrű, $\mathbb{Z} \leq S \leq \mathbb{C}$, S mint $\mathbb{Z}$-modulus vég. gen. $\Rightarrow$ $\forall \alpha \in S$ algebrai egész $(S \subseteq \Omega)$

B: $Y = \{y_1, \dots, y_n\}$ a $\mathbb{Z}$-modulus generátorrendszere.

$s \in S$. $\rightarrow$ $s \cdot y_i \in S$ $\rightarrow$ $s y_i = \sum_{j=1}^{n} a_{ij} y_j$ $\rightarrow$ $A = (a_{ij})$, $v = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ $\rightarrow$ $sv = Av$

$(sI - A)v = 0$ $\rightarrow$ $\underbrace{\det(xI - A)}_{\downarrow\ 1\ \text{főegyütthatós},\ \mathbb{Z}[x]\text{-beli}} = 0$ - nek gyöke s. $\Big\}\ s \in \Omega$

$\alpha, \beta \in \Omega$ $\Rightarrow$ $\alpha + \beta$, $\alpha\beta \in \Omega$ az 1. és 2. lemma alkalmazásával.

Áll. Ω hányadostesté $\mathbb{A}$.

B: Többet igazolunk: $\forall \alpha \in \mathbb{A}$ $\exists \beta \in \Omega, k \in \mathbb{Z}$: $\alpha = \frac{\beta}{k}$.

$a_n \alpha^n + \dots + a_0 = 0$ $\quad (a_i \in \mathbb{Z})$ $\quad / \cdot a_n^{n-1}$

$(a_n\alpha)^n + a_{n-1} \cdot (a_n \alpha)^{n-1} + a_{n-2}(a_n\alpha)^{n-2} \cdot a_n + \dots + a_0 a_n^{n-1} = 0$

$\rightarrow (a_n \alpha) \in \Omega$ $\rightarrow$ $\alpha = \frac{a_n \alpha}{a_n}$

„Nem kell tűvé tenni az egész polinomgyűrűt."

Áll. $\alpha \in \Omega \iff \alpha$ kanonikus polinomja 1 főegh.-s egész.

B: $\Leftarrow$ triv.

$p(\alpha) = 0$, p 1 főegyütthatós, egész elhós

q α kan. polinomja, 1 főegyütthatós $\Rightarrow$ $p = qr$, $q, r \in \mathbb{Q}[x]$ 1 főegyütthatós

$\exists!\, c_1, c_2 \in \mathbb{Q}$: $c_1 q$, $c_2 r$ primitív polinomok

Gauss: $c_1 c_2 qr$ primitív
p primitív, $p = qr$ $\Big\} \longrightarrow c_1 \cdot c_2 = 1$

c_1 és c_2 egyik kell legyen, az 1 fokú miatt.

Ha $c_1 = c_2 = 1 \to$ jó, ha -1, akkor megújítjuk q-t és r-et. □

Lehetne Ω-n számelméletet csinálni. Helyette előbb általánosabban nézzük.

Legyen $1 \in R$ integritási tartomány.

Def. $a \in R$, $b \in R$. $a | b$, ha $\exists c \in R$: $b = ac$.

$U(R) = \{ a \in R \mid a | 1 \}$ egységcsoport. Ezek triviális nevezőt játszanak.

Def. $a \in R$, $b = au$, $u \in U(R) \to b$ a asszociáltja (b asszociált a-hoz): $b \sim a$.

Áll. $\sim$ ekvivalenciareláció, $a \sim b \iff a | b$ és $b | a$; $a \sim b \iff (a) = (b)$. □

Def. $a \in R$ irreducibilis, ha $a \neq 0$, $a \notin U(R)$, $a = bc \Rightarrow b \in U(R)$ és $a \sim c$ vagy
$c \in U(R)$ és $b \sim a$.

Def. $p \in R$ prím, ha $p \neq 0$, $p \notin U(R)$, $p | ab \Rightarrow p | a$ vagy $p | b$.

Áll. $1 \in R$ ct., $a \in R$ prím $\Rightarrow a$ irreducibilis.

B: $\left.\begin{array}{l} a = bc \Rightarrow a | bc \Rightarrow a | b. \\ \Downarrow \\ b | a \end{array}\right\} \iff a \sim b$ □

A megfordítás nem igaz általában.

Példa. $\mathbb{Z}$-ben igaz az ekvivalencia.

$\mathbb{Z}[\sqrt{-5}]$-ben nem igaz: egyszerűsítés $\mathbb{T}$, $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

$\alpha = a + b\sqrt{-5}$, $\bar{\alpha} = a + \sqrt{-5}$ $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2 = a^2 + 5b^2 \in \mathbb{N} \cup \{0\}$

a norma multiplikatív $\Rightarrow$ ($\alpha | \beta \Rightarrow N(\alpha) | N(\beta)$ $\mathbb{Z}$-ben)

$U(\mathbb{Z}[\sqrt{-5}]) = \pm 1$: tfh. $\alpha | 1 \Rightarrow N(\alpha) | 1 \Rightarrow N(\alpha) = 1 \Rightarrow a = \pm 1$, $b = 0$.

$\to$ a 6-nak két nemtriviális felbontását adtuk, amik lényegesen különböznek

Megmutatjuk, hogy mind a 4 tényező irreducibilis.

$\lightning$ Ha $2 = \underbrace{\alpha\beta}_{\text{nem egységek}} \to 4 = N(2) = N(\alpha)N(\beta) \to N(\alpha) = N(\beta) = 2 \to a^2 + 5b^2 = 2$ $\lightning$

Hasonlóan 3-ra: $9 \neq a^2 + 5b^2$. Hasonlóan $1 \pm \sqrt{5}$-re $N = 6 = 2 \cdot 3$.

Tehát ezek mind irreducibilisek, de nem primek: $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, de $2 \nmid (1 \pm \sqrt{-5})$.

Most térjünk vissza Ω-hoz! Rossz híreink vannak:

<u>Áll.</u> Ω-ban nincs irreducibilis elem

B: <u>Mj.</u> $U(\Omega) = \{ \alpha \in \Omega \mid \alpha$ kar. polinomjának konst. tagja $\pm 1 \}$

$\alpha \notin U(\Omega) \longrightarrow \alpha = \sqrt{\alpha} \cdot \sqrt{\alpha}$

$\downarrow$

nem egység, mert α is ez lenne.

Ehelyett: $K \mid \mathbb{Q}$ véges bővítés, $K \cap \Omega$-n számelmélet.

<u>Áll.</u> $(K : \mathbb{Q}) = 2 \iff K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ négyzetmentes, $(d \neq 0, 1)$

B: Ez másodfokú: $1, \sqrt{d}$ bázis $\mathbb{Q}$ felett.

Ezek nem izomorfak: $d_1 \neq d_2 \Rightarrow \mathbb{Q}(\sqrt{d_1}) \mid \mathbb{Q} \not\cong \mathbb{Q}(\sqrt{d_2}) \mid \mathbb{Q}$.

Mert: $x^2 - d_1$ lineáris faktorokra bomlik az egyikben, de a másikban nem.

$K = \mathbb{Q}(\alpha)$ $\quad \mathbb{Q}\left(\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\right) = \mathbb{Q}(\sqrt{b^2 - 4ac}) = \mathbb{Q}(\sqrt{d})$

<u>Kérdés.</u> $R_d = \mathbb{Q}(\sqrt{d}) \cap \Omega = ?$

Látjuk: $\{ a + b\sqrt{d},\ a, b \in \mathbb{Z} \} \leq R_d$. Hajlamosak lennénk sejteni, hogy csak ennyi.

Legyen $\alpha \in \mathbb{Q}(\sqrt{d})$. $\alpha = \frac{a + b\sqrt{d}}{c}$, $a, b, c \in \mathbb{Z}$, $(a, b, c) = 1$, $c > 0$. $\rightarrow \alpha \overset{?}{\in} \Omega$ miért?

Tfh. $\alpha \in \Omega$

- $b = 0 \longrightarrow c = 1 \longrightarrow \alpha \in \mathbb{Z}$
- $b \neq 0$

$$\alpha c - a = b\sqrt{d}$$
$$\alpha^2 c^2 - 2ac\alpha + a^2 = b^2 d$$
$$\alpha^2 - \frac{2a}{c}\alpha + \frac{a^2 - b^2 d}{c^2} = 0$$

$\alpha \in \Omega \iff c \mid 2a,\ c^2 \mid a^2 - db^2$

$m = (a, c)$ $\quad m^2 \mid a^2,\ m^2 \mid c^2 \mid a^2 - db^2 \longrightarrow m^2 \mid db^2$ (d négyzetmentes)

$\iff m^2 \mid b^2 \iff m \mid b$.

$\longrightarrow m = 1$ kell legyen, mert $m \mid (a, b, c) = 1$.

$\Rightarrow c = 1$ vagy $c = 2$. Ha $c = 1 \rightarrow \alpha = a + b\sqrt{d}$, ezt már ismerjük.

Ha $c = 2$: $4 \mid a^2 - db^2$, a páratlan. $\Rightarrow b$ páratlan, $d \equiv 1 \ (4)$

Ekkor is algebrai egészt kapunk.

$$\Rightarrow R_d = \begin{cases} \{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \} & \text{ha } d \equiv 2, 3 \ (4) \\ \{ a + b\sqrt{d} \mid \text{vagy } a, b \in \mathbb{Z}, \text{ vagy } a - \frac{1}{2}, b - \frac{1}{2} \in \mathbb{Z} \} & \text{ha } d \equiv 1 \ (4) \end{cases}$$

R_{-5}-öt már néztük. $R_{-1} = \mathbb{G}$ is volt már.

R_{-3} érdekesebb eset: ezek az Eisenstein-egészek, de ettől függetlenül gyakran hívjuk őket úgy, hogy Euler-egészek.

$\omega = \frac{\sqrt{d}-1}{2} \in R_d$ jelöléssel $a + b\omega$ 1. fajtájú, ha b páros,
2. fajtájú, ha b páratlan

$\rightarrow$ a $d \equiv 1$ eset ebben $\mathbb{Z}[\omega]$.

Az igazi vágynunk a számelmélet alaptétele.

<u>Def</u> UFD (unique factorisation domain): igaz benne a SzAT. (R EIT)

Mj. PID: principal ideal domain = főidéálgyűrű ($\rightarrow$ automatikusan IT)

Láttuk, hogy R_{-5} nem UFD, mint már láttuk.

<u>Tétel</u>. R EIT UFD $\Longleftrightarrow$ 1) főidéálokra teljesül a maximumfeltétel. ÉS
2) $\forall$ irreducibilis elem prím.

B: $\Rightarrow$: $(a_1) \subsetneq (a_2) \subsetneq \dots$ ideálok sorozata, mig. nő

a_1 felbontható véges sok irred. szorzatára.

$\rightarrow a_2$-ben kevesebb faktor van. $\rightarrow$ előbb-utóbb véget ér.

$p \mid ab$, $ab = pc$ vesszük az irred. felbontást ✓

$\Leftarrow$: a_1: ha nem irred: $a_1 = a_2 c_2$. Ezt folytatjuk.

$\rightarrow (a_1) \subset (a_2) \subset (a_3) \subset \dots$

$\Rightarrow$ $\forall$ elem felbontható irreducibilisek szorzatára.

$a_1 \dots a_n = b_1 \dots b_k$ $\rightarrow$ sorban toppantjuk mindkét oldal irred. faktorait (amik prímszerűek szintén) □

<u>Tétel</u>. Minden főidéálgyűrű UFD. (PID $\Rightarrow$ UFD)

B: 1) $(a_1) \subseteq (a_2) \subseteq \dots$ $\longrightarrow \bigcup (a_i) = (a)$ ideál $\longrightarrow \exists j: a \in (a_j) \rightarrow$ a j-edik lépésben stabilizálódik.

2) Állítjuk, hogy van lnko.
$a, b \in R$. $(a, b) = (d)$. Ez lesz a lnko.

$ax + by = d$ Ha $c \mid a$, $c \mid b$ $\Rightarrow$ $c \mid d$. Tehát d lnko.

$(cd) = (ca, cb)$ fennáll.

Legyen p irreducibilis, $p \mid ab$, $p \nmid a$. $(p, b) = \begin{cases} (p) \rightarrow p \mid b. \\ (1) \end{cases}$ ✓

Ha $(p, b) = (1)$ $\rightarrow (pa, ab) = (a)$ $\longrightarrow p \mid a$ ↯. □

2016. 04. 01.

Tétel (NB). R UFD $\Rightarrow$ $R[x]$ UFD

Köv. $K[x,y]$ UFD, mert $K[x,y] = K[x][y]$, és $K[x]$ UFD.

Példa. R UFD $\not\Rightarrow$ $R[[x]]$ UFD (NB)

Def. R euklideszi gyűrű (euclidean domain): EIT, $\exists \varphi: R\setminus\{0\} \to \mathbb{Z}_{(\geq 0)}$ és $\forall a,b \in R$, $b \neq 0$: $\exists q,r \in R$: $a = bq + r$ és $\varphi(r) < \varphi(b)$ vagy $r = 0$.

Tétel. Euklideszi gyűrű $\Rightarrow$ főideálgyűrű.

B: $I \triangleleft R$.

Ha $I = 0$ $\to$ $I = (0)$.

Ha $I > 0$ $\to$ $b \in I$ olyan, hogy $\varphi(b)$ minimális I-ben.

$(b) \subset I$ triviális.

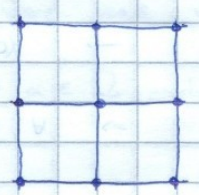
Legyen $a \in I$. $r = a - bq \in I$ $\to$ $r = 0$ $\to$ $a = bq$ $\Rightarrow$ $(b) \supset I$.

Tehát $I = (b)$. □

Példa.
- $\mathbb{Z}$-ben $\varphi(n) = |n|$,
- $K[x]$-ben $\varphi(f) = \deg f$.
- $G = R_{-1}$-ben $\varphi(\alpha) = N(\alpha)$: $\alpha, \beta \in G$ $\exists \gamma, \rho \in G$: $\alpha = \beta\gamma - \rho$ és $N(\rho) < N(\beta)$ kell.

G hányadosteste $\mathbb{Q}(i)$ $\to$ γ „körülbelül" α/β lesz.

$\frac{\alpha}{\beta} = a + bi$ $\exists a_0, b_0$: $|a_0 - a| \leq \frac{1}{2}$, $|b_0 - b| \leq \frac{1}{2}$, $a_0, b_0 \in \mathbb{Z}$



$\to$ $\gamma := a_0 + b_0 i \in G$, $\rho = \alpha - \beta\gamma \in G$

$N\left(\frac{\alpha}{\beta} - \gamma\right) = (a_0 - a)^2 + (b_0 - b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$ ($\mathbb{Q}(i)$-ben is van N)

$\Rightarrow N(\alpha - \beta\gamma) < N(\beta)$, a feltét β-val monozva.

Áll. $R_{-2} = \mathbb{Z}[\sqrt{-2}]$ euklideszi.

B: Ugyanúgy, mint G-re, $N(a + b\sqrt{-2}) = a^2 + 2b^2$, a számolás működik. □

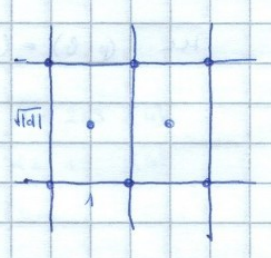
R_{-3}-ra ez már nem megy: lehet egyszerűség is < 1 helyett, így az euklideszi algoritmus, azaz a maradékos osztás megdöglik.

De $\mathbb{Z}[\sqrt{-3}]$ nem lesz UFD, vissza R_{-3} az.

Tétel. R_d (d négyzetmentes, $d \neq 0, 1$, $d < 0$) euklideszi, ha $d = -1, -2, -3, -7, -11$

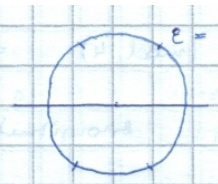
B: Fent négyzetrácsban dolgoztunk, általánosan ez téglarács; a csúcsoktól vett távolságot nézzük.

$d \equiv 1$-re nem csak a csúcsok, hanem a középpontok is jótevnek: $\frac{1}{4} + \frac{|d|}{16} < 1$ kell a kulcsegyenlőtlenségben.



Ez $d = -15$-re már nem jó. □

$\mathcal{U}(R_d) = ?$ Tudjuk: $\mathcal{U}(R_{-1}) = \{\pm 1, \pm i\}$



Áll. $\mathcal{U}(R_{-3}) = \{\pm 1, \pm \varepsilon, \pm \varepsilon^2\}$

B: Ezek jók. Más nem lehet, mert 1 normájú kell legyen. (sőt az elég is)
$N(a + \sqrt{-3}\, b) = a^2 + 3b^2 = 1$ □

Áll. $d \neq -1, -3$ -ra $\mathcal{U}(R_d) = \{\pm 1\}$ ($d<0$, négyzetmentes)

B: Nagyobb a normából. □

Meglepő: $d > 0$-ra (négyzetmentes): $|\mathcal{U}(R_d)| = \infty$
Pell-egyenlet: $x^2 - dy^2 = 1$
$\longrightarrow$ van ∞ megoldás: a triviális és ha (x_1, y_1) minimális olyan, hogy $x_1 > 1$ és $y_1 > 0$ megoldás:
$(x_1 + y_1\sqrt{d})^n = x_n + y_n\sqrt{d}$ $n = 2, 3, \dots$ -ra új megoldáspárt ad
(sőt ezek megfelelő negálfjai is)
Újdonság: lehet negatív norma! Ha az $x^2 - dy^2 = -1$ Pellnek van megoldása. (nem mindig van). Ha van: ennek a minimális megoldásainak páros kitevős hatványai adják a $+1$-es megoldásait.

Tétel. (NB) $d<0$, R_d euklideszi $\Leftrightarrow$ $d = -1, -2, -3, -7, -11$.

Tétel. (NB) $d<0$, R_d UFD $\Leftrightarrow$ $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

Tétel. (NB) $d>0$, R_d euklideszi $\Leftrightarrow$ $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

Sejtés: $d>0$, R_d UFD végtelen sok d-re. (Megoldatlan.)

$x^2 + x + 41$ $x = 0, 1, 2, \dots 39$ -ra prímet ad

$x^2 + x + p$ $x = p$-re nem prím, sőt $(p-1)$-re sem: $p^2 - 2p + 1 + p - 1 + p = p^2$.

Tétel. (NB) $x^2 + x + p$ prímszám $x = 0, 1, \dots, p-2$ -re $\Leftrightarrow$ $R_{-(4p-1)}$ UFD.

IMO 1987/6. (Kuba) $n \geq 2$ $x^2 + x + n$ értéke $0 \leq x \leq \sqrt{\frac{n}{3}}$ prím $\Rightarrow$ értéke $0 \leq x \leq n-2$ prím.

Tétel. $d \neq 0, 1$ négyzetmentes. $\mathbb{Z}[\sqrt{d}]$-ben 2 nem prím soha.

B: $2 \mid d \cdot (d-1) = d^2 - d = (d + \sqrt{d}) \cdot (d - \sqrt{d})$, de $2 \nmid (d + \sqrt{d})$, $2 \nmid (d - \sqrt{d})$. □

Köv. Ha $d \leq -3$, akkor $\mathbb{Z}[\sqrt{d}]$ nem UFD.

B: 2 nem prím. Elég belátni, hogy 2 irreducibilis.
$2 = \alpha\beta \longrightarrow N(2) = N(\alpha)N(\beta) \longrightarrow 4 = N(\alpha)N(\beta)$. $4 = 1 \cdot 4 = 2 \cdot 2$. egység
$\longrightarrow N(\alpha) = N(\beta) = 2. \longrightarrow a^2 + |d|\, b^2 = 2$, ez nem oldható meg $d \leq -3$-ra. □

Köv. $d \equiv 1 \pmod 4 \Rightarrow \mathbb{Z}[\sqrt{d}]$ nem UFD. (d lehet pozitív is)

B: Ugyanígy bizonyítunk. $a^2 - db^2 = 2$

$\Rightarrow a^2 - b^2 \equiv 2 \quad (4)$, ennek nincs megoldása. □

Térjünk vissza az első ellenpéldához!

$\mathbb{Z}[\sqrt{-5}]$-ben $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

Írhatjuk így is:

$$(6) = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$$

Mj: $1 \in R$, kommutatív, noether:

$$(a_1, \dots, a_n)(b_1, \dots, b_k) = (a_1b_1, a_1b_2, \dots, a_1b_k, \dots, a_nb_k)$$

$$\begin{cases} P_1 = (1+\sqrt{-5}, 2) = (1-\sqrt{-5}, 2) \\ P_2 = (1+\sqrt{-5}, 3) \\ P_3 = (1-\sqrt{-5}, 3) \end{cases}$$

$$(2) \cdot (3) = (1+\sqrt{-5})(1-\sqrt{-5})$$

$$P_1^2 \cdot P_2P_3 = P_1P_2 \cdot P_1P_3$$

Ezek prímideálok:

pl. $\mathbb{Z}[\sqrt{-5}]/P_2 = \mathbb{F}_3$

Ezeknek a prímideáloknak az „árnyéka" a nem egyértelmű felbontás. (Kummer)

Def. Dedekind-gyűrű: minden ideál egyértelműen előáll prímideálok szorzataként.

Példa (nem memorizálandó)

$x^2 - 67y^2 = 1 \longrightarrow x = 48\,842, \quad y = 5967$ minimális

$66 \longrightarrow \dots \quad y = 8$

$68 \longrightarrow \dots \quad y = 4$

$x^2 - 1141y^2 = 1 \longrightarrow x \approx 1{,}037 \cdot 10^{27}, \quad y \approx 3{,}069 \cdot 10^{25}$

Ennyit az IT-ok számelméletéről.

Testekkel folytatjuk.

volt: $f \in K[x] \Rightarrow \exists L \geq K \quad \exists \alpha \in L \quad f(\alpha) = 0.$ $f = p_1 \cdots p_k$, p_i irreducibilis,

$K[x]/(p_1(x))$: $\alpha = x + (p_1(x))$

$\exists L$: $L[x]$-ben $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. $\alpha_1, \dots, \alpha_n \in L$.

<u>Def.</u> L f felbontási teste K felett: f gyöktényezőire bomlik L felett és $L = K(\alpha_1, \dots, \alpha_n)$.

<u>Áll.</u> A felbontási test lényegében egyértelmű: ha $L_1 | K$ és $L_2 | K$ felb. testek, akkor $L_1 | K \cong L_2 | K$.

B: $(x - \alpha_1) \dots (x - \alpha_n)$ $(x - \beta_1) \dots (x - \beta_n)$ gyt. felbontások

$K(\alpha_1) | K \simeq K(\beta_1) | K$, indukció. □

<u>Def.</u> $L|K$ normális bővítés, ha algebrai és ha $p(x) \in K[x]$ K-irreducibilis és van gyöke L-ben, akkor $p(x)$ gyöktényezőire bomlik L-ben.

<u>Tétel</u> Tfh. $L|K$ véges. Ez normális $\Leftrightarrow$ L felb. test, azaz $\exists f \in K[x]$, amiben L a felb. teste.

<u>Mj.</u> Minden elsőfokú bővítés normális: $L = K$-ra L felb. teste x-nek.
Minden másodfokú bővítés normális: $L = K(\alpha)$, $\alpha \in L \setminus K$ minőségképpen (formula tétel)
$\rightarrow$ L a kanonikus polinom felbontási teste.
Semmilyen magasabb fokúra nincs ilyen:
$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, $L|K$ harmadfokú
$x^3 - 2$ irreducibilis, de nem bomlik lineáris tényezőkre (gyökei megadhatók)
Ez nyilván minden $n \geq 3$-ra működik.

2016.04.0

Bt. ① Felb. test $\Rightarrow$ normális.
Felb. test: $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ $\alpha_i \in L$,
$L = K(\alpha_1, \dots, \alpha_n)$
$\beta \in L$, $p(\beta) = 0$ p K-irreducibilis

$\Rightarrow \beta = g(\alpha_1, \dots, \alpha_n)$, ahol $g \in K[x_1, \dots, x_n]$

Ötlet: $h(x) = \prod_{S_n} \left(x - g(\alpha_{i_1}, \dots \alpha_{i_n})\right)$, deg $h = n!$,

állítjuk, hogy $h \in K[x]$. Az α-k permutálásával h önmagába megy át. $\rightarrow$ ez szimmetrikus polinom.
Sőt az α-k elemi szimm. polinomjaival polinomjai.
$\Rightarrow$ az ekkor előállnak mint K-beliek polinomjai.

$(x - \beta) \mid h(x)$ $\Rightarrow (p, h) \neq 1$, de p irreducibilis $\Rightarrow p | h$. ✓

② Normális $\Rightarrow$ felb. test. $L = K(\alpha_1, \dots, \alpha_n)$ véges bővítés.
α_i algebraiak, p_i kan. polinom, mindegyik lin. tényezőkre bomlik.
$f = p_1 \cdots p_n$ is lin. tényezőkre bomlik, a gyökeit K-hoz adjungálva L-et kapjuk $\rightarrow$ L f-nek a felbontási teste. ✓ □

Példa. $\mathbb{R}$ felett x^2+1 f. teste $\mathbb{C}$,
$\mathbb{Q}$ felett x^2+1 f. teste $\mathbb{Q}(i)$
$\mathbb{Q}$ felett x^n-1 f. teste: elég valamelyik prim. egységgyököt adjungálni, például $\varepsilon = \exp\left(\frac{2\pi i}{n}\right)$-et, tehát a f. test $\mathbb{Q}(\varepsilon)$.

$$(\mathbb{Q}(\varepsilon):\mathbb{Q}) = \varphi(n), \qquad \Phi_n(x) = \prod_{\substack{\eta\ n\text{-edik}\\ \text{primitív}}} (x-\eta) \in \mathbb{Z}[x]$$

Algebra 1:

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \qquad \frac{x^n-1}{\prod_{\substack{d|n\\ d\neq n}} \Phi_d(x)} = \Phi_n(x) \longrightarrow \Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1$$

SzhE p-vel $x+1$-re $\to$ irreducibilis

Tétel. $\Phi_n(x)$ irreducibilis $\mathbb{Z}$ felett $\forall n \geq 1$-re.

B: $\varepsilon \in \Omega \to$ kan. polinomja $f \in \mathbb{Z}[x]$, f főegyütthatója 1.
Látjuk, hogy $f \mid \Phi_n$.

Legyen $p \nmid n$ prímszám, legyen g az ε^p pr. egységgyök kan. polinomja.
Belátjuk: $f = g$.
Tfh $f \neq g$. $f, g \mid x^n - 1$, $\mathbb{Q}[x]$-en egyértelmű a felbontás irreducibilisekre

$$x^n - 1 = f(x)\cdot g(x)\cdot k(x) \quad \text{valamely } h\text{-ra.} \qquad h \in \mathbb{Z}[x]$$

$$g(x^p) = f(x)\cdot k(x), \quad \text{mert } g(\varepsilon^p) = 0. \qquad k \in \mathbb{Z}[x]$$

$$g(x^p) \equiv (g(x))^p \pmod p$$

Ez egyszerű látni bin. tétellel, vagy $(a+b)^p \equiv a^p + b^p \pmod p$ alapján.

$$g(x)^p = f(x)\,k(x) \quad (p)$$

$\downarrow$ $\varphi(x)$ mod p irred. faktor ($\mathbb{F}_p$ felett vagyunk)

$\downarrow$

$\varphi(x) \mid f(x) \quad (p)$,
$\varphi(x) \mid g(x) \quad (p)$,
$\varphi(x)^2 \mid x^n - 1 \quad (p)$,
$\varphi(x) \mid nx^{n-1}$ $\lightning$

Ezt az eljárást folytatjuk. $\longrightarrow$ előbb-utóbb kiderül, hogy f-nek az összes n-edik prim. egységgyök gyöke $\longrightarrow$ $f = \Phi_n$. $\square$

Def. $\mathbb{Q}(\varepsilon)$ az n-edik körosztási test.

Legyenek $K \leq L \leq M$ véges bővítések.

1) $M|K$ normális $\Rightarrow$ $L|K$ normális? nem
2) $M|K$ normális $\Rightarrow$ $M|L$ normális? igen
3) $L|K$ és $M|L$ norm. $\Rightarrow$ $M|K$ normális? nem

2) Igaz, mert nagyobbra a polinom, ami K felett van M-ben, jó L-ben is.

1) $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$ ω harmadik egy.
3) $\mathbb{Q} < \mathbb{Q}(\sqrt[4]{2}) < \mathbb{Q}(\sqrt[4]{2})$

$\downarrow$ másodfokú bővítés

Lehet-e irreducibilis polinomnak a felbővítési testben többszörös gyöke?

Áll. Nem lehet.

„B": $p(x) \in K[x]$ irreducibilis. $\exists\, \alpha$ többszörös gyök, $x-\alpha \mid p(x)$
$x-\alpha \mid p'(x)$

$\Rightarrow x-\alpha \mid (p, p') \Rightarrow (p,p') = p$, $p \mid p'$, de $\deg p' < \deg p$ $\lightning$ □

Ez nem stimmel: baj van, ha $p' = 0$. $\Leftrightarrow p(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots = g(x^p)$
ahol p a char, és $kp \cdot a_{kp} = 0$. (tk p kétféle értelemben áll.)
De az az igazi kérdés, hogy van-e ilyen kívánt irreducibilis polinom.

Def. $p(x) \in K[x]$ irred., p separábilis, ha minden gyöke egyszeres.

Def. $L|K$, $\alpha \in L$ algebrai. α separábilis, ha a kan. polinomja az.

Def. $L|K$ algebrai bőv. separábilis, ha $\forall \alpha \in L$ separábilis.

$g(y)$-nak is van felb. teste. $g(y) = (y-\beta_1) \dots (y-\beta_k)$

$p(x) = (x^p - \beta_1) \dots (x^p - \beta_k)$

$\downarrow$

ennek a faktorai $\Longrightarrow x^p - \alpha_1^p = (x-\alpha_1)^p \dots (x-\alpha_k)^p$
α_1 gyöke alk. testben
$\alpha_1^p = \beta_1$

Tehát ha egy irred. polinom inseparábilis, akkor $\forall$ gyöke legalább p-szeres.

Def. K perfekt test, ha minden algebrai bővítése separábilis, azaz $\forall p(x) \in K[x]$ irreducibilis separábilis.

Áll. char $K = 0 \Rightarrow$ perfekt.

Áll. char $K = p$-re K perfekt $\Leftrightarrow K$ $\forall$ elemének van p-edik gyöke K-ban.

B: $a_0 + a_p x^p + a_{2p} x^{2p} + \dots = \Longrightarrow a_{lp} = b_l^p$ van p-edik gyök

$= b_0^p + b_1^p x^p + b_2^p x^{2p} + \dots = (b_0 + b_1 x + b_2 x^2 + \dots)^p$. ✓ perfekt.

Legyen $a \in K$ olyan, hogy nincs p-edik gyöke K-ban.
Állítjuk, hogy $x^p - a \in K[x]$ inseparábilis. irreducibilis.

$\alpha^p = a$, $x^p - \alpha^p = (x-\alpha)^p$

$f \mid x^p - a = (x-\alpha)^p$

$f = (x-\alpha)^l$ valy $l \geq 1$-re $l \geq p$

Tehát ez olyan irred. polinom, ami insep., tehát nem perfekt. ✓ □

Példa. $\mathbb{F}_p(t) = K$ nem perfekt. (t tr.c. $\mathbb{F}_p$ felett)

B: $x^p - t \in K[x]$ irreducibilis, de van többszörös gyöke.
Ezt az előbb mint végiggondoltuk, csak az kell, hogy t-nek nincs p-edik gyöke.

$$\exists \quad t = \frac{f(t)^p}{g(t)^p}$$

$$t \cdot g(t)^p - f(t)^p = 0. \quad \text{De } t \text{ transcendens. } \lightning$$

Ugyanezt a $\exists$ kérdést, amit normálisra feltettünk, meg lehet kérdezni separábilisra is. $K \leq L \leq M$ véges bővítések.

1) Triv igaz.
2) az L feletti kar. polinom osztja a K fölöttit. $\longrightarrow$ igaz.
3) Triviálisabb, HF.

Véges testek

Legyen F véges test.

Tétel. $|F| = q = p^f$, ahol p prím, $f \geq 1$.

B: F véges $\Rightarrow$ char $F = p$ véges. $\Rightarrow$ $\mathbb{F}_p \leq F$, vektortér felette.

$\dim_{\mathbb{F}_p} F = f \quad \rightarrow \quad |F| = p^f.$

Tétel. $q = p^f \quad \Rightarrow \quad \exists F : |F| = q.$

B: $x^{p^f} - x \in \mathbb{F}_p(x)$. Legyen ennek a felb. teste F.

$\downarrow$
nincs többszörös gyöke: $p^f \cdot x^{p^f - 1} - 1 = 0 - 1$ a derivált, ennek igy nem tud közös gyöke lenni.

Ha $a^{p^f} = a$ és $b^{p^f} = b$ gyökök.

$$\Rightarrow (a+b)^{p^f} = a^{p^f} + b^{p^f} = a + b,$$

$$(a \cdot b)^{p^f} = a^{p^f} \cdot b^{p^f} = a \cdot b,$$

tehát a gyökök már magukat résztestet alkotnak, igy ez maga a felbővítési test $\longrightarrow$ p^f db gyök van, $|F| = p^f$.

($\mathbb{F}_p$ elemei ebben Kis-Fermat miatt benne vannak.)

Tétel. $\forall q = p^f$-re csak egy q elemű test van.

B: Legyen $|F| = p^f = q$. $\quad |F^*| = p^f - 1$ a mult. csoport.

$0 \neq a \in F^*$-ra $\quad a^{p^f - 1} = 1 \quad$ (Lagrange-tétel)

gyöke $x^{p^f - 1} - 1$-nek $\Rightarrow$ $x^{p^f} - x$-nek F minden eleme.

Tehát $x^{p^f} - x = \prod_{\alpha \in F} (x-\alpha)$, tehát F ennek a felb. teste $\mathbb{F}_p$ felett. $\square$

Tehát a véges testek $\xleftrightarrow{1:1}$ primhatványok.

<u>Tétel.</u> $|F| = p^f = q$: $(F,+) \simeq (\mathbb{Z}_p)^f$ $\quad (F^*, \cdot) \simeq \mathbb{Z}_{q-1}$

B: Van p elemű bázis, az additív struktúra triviális látnivaló.
A multiplikatív a következő erősebb tételből jön ki. $\square$

<u>Tétel.</u> K <u>tetszőleges test</u>, $G \leq K^*$, $|G| < \infty$ $\Rightarrow$ G ciklikus
kommut.

<u>Mj.</u> Ferdetestre ellenpélda: $\mathbb{H}$-ben $\{\pm 1, \pm i, \pm j, \pm k\}$ nem ciklikus.

B: $|G| = n$ $\quad \forall\, d \mid n$-re $\psi(d) :=$ (hány d rendű elem van G-ben),

$\psi(d) \geq 0$. Állítjuk: $\psi(d) \neq 0 \Rightarrow \psi(d) = \varphi(d)$.

[$a \in G$, $o(a) = d$ $\rightarrow$ $x^d - 1$-nek ez gyöke, és a többi d rendű olyan, hogy a-val d-hez rel. prím kitevőjű hatványa.]

$$\sum_{d \mid n} \psi(d) = n = \sum_{d \mid n} \varphi(d).$$

De $\psi(d) \leq \varphi(d)$ $\forall d$
$\Rightarrow$ $\psi(d) = \varphi(d)$ $\forall d$
$\Rightarrow$ van $d = n$ rendű elem
$\Rightarrow$ ciklikus. $\square$

<u>Tétel.</u> $|F| = p^f = q$. $\quad \mathrm{Aut}(F) \simeq \mathbb{Z}_f$

B: Vegyük észre, hogy $\varphi: x \mapsto x^p$ automorfizmus. Ez a korábbi számolásból látszik, hogy műveletartó. Kell még, hogy injektív:
$a^p = a_1$, $b^p = b_1$ $\longrightarrow$ $(a-b)^p = a_1 - b_1$ miatt.
Így bijekció is. Ez az ún. Frobenius-aut.

Ez hatványozható: $x \mapsto x^{p^2}, \dots, x \mapsto x^{p^f} = x$.
Ennek f a rendje, különben $x^{p^2} - x$-nek gyöke lenne.

Állítjuk, hogy nincs más. $F = \mathbb{F}_p(\alpha)$, ahol α a mult. csoport generátora. $\longrightarrow$ α kar. polinomja f fokú
$\longrightarrow$ α f helyre mehet, mert a kar. polinomja egyszer gyökébe kell menjen.
$\Rightarrow$ $|\mathrm{Aut}(F)| = f$. $\square$

<u>Jel.</u> $|F| = p^f = q \longrightarrow F = GF(q)$

2016. 04. 15

„Ismerjük a véges testeket, hát felét ismerjük, de mindenre rákent valamit."

Tétel (Wedderburn) Minden véges ferdetest test.

B: (Witt) Legyen D véges ferdetest. (division ring, skew field) Legyen $F = Z(D)$.

Könnyen ellenőrizhetően F rést-ferdetest: azt tudjuk, hogy résszgrűű,
$ax = xa \quad (a \neq 0) \quad \Rightarrow \quad xa^{-1} = a^{-1}x$, tehát, $a \in F \Rightarrow a^{-1} \in F$.
Tehát F véges test, $|F| = q$.
D automatikusan vektortér F felett, $|D| = q^n$ ($n \geq 1$ dimenzió)
Elég lenne: $n = 1$.

Tekintsük D^*-ot! $|D^*| = q^n - 1$ csoport.
Felírjuk az osztályegyenletet:

- az 1 elemének alkotják a centrumot: $q-1$ db (0 kivétel)
- ha $a \in D \setminus F$: $C_{D^*}(a) \cup \{0\} = C_D(a)$

$x, y \in C_D(a) \Rightarrow x+y,\ xy,\ x^{-1} \in C_D(a)$ miatt, tehát ez is rést-ferdetest, résztestek valódi.

$\Rightarrow F \leq C_D(a) \lneq D$, $C_D(a)$ is vt, q^k elemszámú, $k < n$.

az a^{D^*} konjugáltosztály elemszáma $\dfrac{q^n - 1}{q^k - 1}$ (a centralizátor indexe),

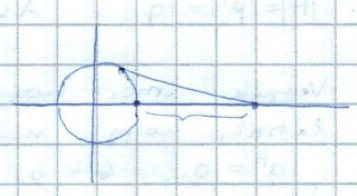
Emlék: $m^k - 1 \mid m^n - 1 \iff k \mid n$ (euklideszi algoritmus)

tehát $k \mid n$.

$$|D^*| = (q-1) + \sum_{\substack{k \mid n \\ k < n}} \underbrace{\frac{q^n - 1}{q^k - 1}}_{\Phi_n(q)},$$

ahol a ' azt jelzi, hogy egy k akár többször, akár 0-szor is lehet

$$\Phi_n(q) = \frac{q^n - 1}{\prod\limits_{\substack{d \mid n \\ d < n}} (q^d - 1)}, \quad |D^*| = q^n - 1 \quad \Rightarrow \quad \Phi_n(q) \mid q - 1$$



Ebből $n = 1$ következik. □

Némi kárpótlást jelent, ha az egyik disztributivitást is elhagyjuk a kommutativitás mellett, olyanok vannak, sőt osztályozva is vannak (Zassenhaus)
→ majdnemtest, near-field, Fastkörper.

Most visszatérünk a separábilis bővítésekhez.

Tétel. $L|K$ véges bővítés és separábilis $\Rightarrow$ $L|K$ egyszerű bővítés

Spec.: $\mathbb{Q}$ minden véges bővítése egyszerű (ezt másodfokúra már láttuk), ez char $\mathbb{Q} = 0$ miatt van.

B: Világos, hogy L véges sok elem adjunkciójával kapható.
Elég lenne belátni, hogy 2 elem adjunkciója kiegészíthető 1-gyel, felhasználva, hogy sep. bővítés minden résztestje is az.
Kell tehát: $K(\alpha, \beta) = K(\vartheta)$.

α kan. polinomja $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ a felbontási testben, az alfák különbözők a separábilitás miatt.

Ugyanígy β-hoz $g(x) = (x-\beta_1)\dots(x-\beta_k)$. Legyen $\alpha = \alpha_1$, $\beta = \beta_1$ a jelölésben.

$\alpha_i + z\beta_j = \alpha + z\beta$ fennállhat-e, ha $j \neq 1$, z tetszőleges?

$\longrightarrow$ $z = \dfrac{\alpha - \alpha_i}{\beta - \beta_j}$, ez egyszerűen z-re igen. fix i, j mellett

- Tfh. K végtelen. $\longrightarrow$ csak véges sok z-t zárunk ki, $\exists c$: $\alpha_i + \beta_j c \neq \alpha + c\beta$
$\longrightarrow \vartheta := \alpha + c\beta$.

Könnyű látni: $K(\vartheta) \subset K(\alpha, \beta)$.

A másik irányhoz elég lenne, hogy $\alpha, \beta \in K(\vartheta)$, sőt elég, ha $\beta \in K(\vartheta)$, mert akkor $\alpha = \vartheta - c\beta$.

Tek. az $f(\vartheta - cx)$-et. $f(\vartheta - c\beta) = f(\alpha) = 0$,
$g(\beta) = 0$.

Állítjuk, hogy $f(\vartheta - cx)$-nek és $g(x)$-nek nincs más közös gyöke:
$f(\vartheta - c\beta_j) = 0 \Rightarrow \vartheta - c\beta_j = \alpha_i$ valamely i-re, de ez nem lehet.

$\Rightarrow \big(f(\vartheta - cx), g(x)\big) = (x - \beta)$, de az euklo is a testből van
$\Rightarrow \beta \in K(\vartheta)$. ✓

- Ha K véges: mivel a multiplikatív csoport ciklikus, elég annak a generátorelemét adjungálni. □

Legyen $\varphi: K \to L$ homomorfizmus. $\ker\varphi \triangleleft K \longrightarrow \ker\varphi = 0$ vagy K.

Tehát minden nemtriviális homomorfizmus monomorfizmus,
így nemtriv. bijektív homomorfizmus izomorfizmus.

<u>Def.</u> $L|K$, $M|K$, $\varphi: L \to M$ K-homomorfizmus, ha $\varphi|_K = \mathrm{id}_K$.

<u>Def.</u> $L|K$-ra $\mathrm{Gal}(L|K) = \{\varphi \in \mathrm{Aut}(L) \mid \varphi|_K = \mathrm{id}_K\}$ Galois-csoport.

<u>Példa.</u> $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$-ra $\mathrm{Gal}\big(\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}\big) = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$.

Az automorfizmust meghatározza az, hogy $\sqrt[3]{2}$-t hova viszi.
$\sqrt[3]{2}$ csak $x^3 - 2$ valamely gyökébe mehet, de a másik kettő gyök nincs a testben

<u>Példa.</u> $\mathrm{Gal}(\mathbb{R} \mid \mathbb{Q}) = \{\mathrm{id}_{\mathbb{R}}\}$, pedig $\mathbb{R}|\mathbb{Q}$ kontinuum fokú.

Ugyanis minden a racionálisokat megtartó automorfizmus rendezéstartó,
mert pozitív pozitívba fog menni.
Rendezéstartás miatt pedig csak $\mathrm{id}_{\mathbb{R}}$ lehet.

<u>Def.</u> $L|K$ Galois-bővítés, ha véges,
normális,
separábilis.

Tétel. $L|K$ Galois $\Rightarrow$ $|Gal(L|K)| = (L:K)$.

B. $L = K(a)$, mert Gal-bővítés.
Normális, f-nek a gyöke L-ben $\rightarrow$ $f = (x-a_1)\dots(x-a_n)$, $a_i \in L$, egymásra gyökök
Legfeljebb n aut. lehet, mert csak $a \mapsto a_i$ lehet.
$a \mapsto a_i$ kiterjed automorfizmussá.

Lemma. (Dedekind) $\lambda_1, \dots, \lambda_n : K \rightarrow L$ különböző monomorfizmusok $\Rightarrow$ lin. ftlenek, azaz $\sum_{i=1}^{n} a_i \lambda_i = 0$, $a_i \in L$, 0 a konstans nulla fv. $\Rightarrow \forall a_i = 0$.

B: $\lightning$ $\sum a_i \lambda_i = 0$ nemtriv lin. kombináció, ezek közül választunk azt, ahol minimális a nemtriv elemek száma (legalább 2)
Nyilván elég csak esetet kizni: $n \geq 2$, $\forall a_i = 0$

$$a_1 x^{\lambda_1} + a_2 x^{\lambda_2} + \dots + a_n x^{\lambda_n} = 0 \quad \forall x \in K$$

(később valamit jól meg)
$c \in K$, $c \neq 0$. Szorzunk c^{λ_n}-nel:

$$\begin{cases} a_1 x^{\lambda_1} c^{\lambda_n} + a_2 x^{\lambda_2} c^{\lambda_n} + \dots + a_n x^{\lambda_n} c^{\lambda_n} = 0 \\ a_1 (cx)^{\lambda_1} + a_2 (cx)^{\lambda_2} + \dots + a_n (cx)^{\lambda_n} = 0 \end{cases}$$

$\longleftarrow$ az eredeti egyenlet $x \leftarrow cx$-szel

$$\rightarrow a_1 (c^{\lambda_1} - c^{\lambda_n}) x^{\lambda_1} + a_2 (c^{\lambda_2} - c^{\lambda_n}) x^{\lambda_2} + \dots + a_{n-1} (c^{\lambda_{n-1}} - c^{\lambda_n}) = 0$$

$\Rightarrow$ $a_1 \cdot (c^{\lambda_1} - c^{\lambda_n}) = 0$ $\Rightarrow$ $c^{\lambda_1} = c^{\lambda_n}$, de c választható úgy, hogy ez ne álljon fenn. $\lightning$

Tétel.
Legyen $G \leq Aut(K)$, $|G| = \infty$. Legyen $K_0 = \{a \in K : a^g = a\} \leq K$ a fixtest.
Ekkor $(K : K_0) = |G|$.

B: Számolós. Feltételek: $|G| = \{\lambda_1, \dots, \lambda_n\}$, $(K : K_0) = m$. Kell, hogy $n = m$. Indirekt.

① $\lightning$ $m < n$. Vegyük K bázisát K_0 felett $\rightarrow$ $x_1, \dots, x_m$

$$\left.\begin{matrix} x_1^{\lambda_1} y_1 + x_1^{\lambda_2} y_2 + \dots + x_1^{\lambda_n} y_n = 0 \\ \vdots \\ x_m^{\lambda_1} y_1 + x_m^{\lambda_2} y_2 + \dots + x_m^{\lambda_n} y_n = 0 \end{matrix}\right\}$$

$y_1, \dots, y_n$ ismeretlenek homogén lin, van nemtriv megoldás, mert $m < n$.

Legyen $x \in K$. $\longrightarrow$ $x = a_1 x_1 + \dots + a_m x_m$, $a_i \in K_0$ felírás.
A k-adik egyenletet a_k-val szorozzuk. Vegyük észre: $a_k = a_k^{\lambda_1} = \dots = a_k^{\lambda_n}$.

$$\rightarrow (a_k x_k)^{\lambda_1} y_1 + (a_k x_k)^{\lambda_2} y_2 + \dots + (a_k x_k)^{\lambda_n} y_n = 0$$

Összeadás: $x^{\lambda_1} y_1 + \dots + x^{\lambda_n} y_n = 0$, y_i nem mind 0 $\rightarrow$ $\lambda_1, \dots, \lambda_n$ lin. öf, ez ellentmond a Dedekind-lemmának. $\lightning$

② $\lightning$ $m > n$. $\rightarrow$ Van $n+1$ lin ftl. elem: $x_1, x_2, \dots, x_{n+1} \in K$ linfüggenek K_0 felett.

$$\left.\begin{matrix} x_1^{\lambda_1} y_1 + x_2^{\lambda_1} y_2 + \dots + x_{n+1}^{\lambda_1} y_{n+1} = 0 \\ \vdots \\ x_1^{\lambda_n} y_1 + x_2^{\lambda_n} y_2 + \dots + x_{n+1}^{\lambda_n} y_{n+1} = 0 \end{matrix}\right\}$$

Van nemtriv mo., a lehető legkevesebb nem 0.

$\longrightarrow$ $y_1, \dots, y_r \neq 0$, $y_{r+1} = \dots = y_{n+1} = 0$, r minimális, $r \geq 1$.

(*) $x_1^{\lambda_i} y_i + x_2^{\lambda_i} y_2 + \dots + x_r^{\lambda_i} y_r = 0$ $(i = 1, 2, \dots, n)$

$\Rightarrow$ $x_1^{\lambda_i \lambda} y_i^{\lambda} + x_2^{\lambda_i \lambda} y_2^{\lambda} + \dots + x_r^{\lambda_i \lambda} y_r^{\lambda} = 0^{\lambda} = 0.$ Valamely λ-ra, fix. $(i = 1, \dots, n)$

$\to$ $\lambda_i \lambda$ végigfut G elemein

(**) $x_1^{\lambda_i} y_1^{\lambda} + x_2^{\lambda_i} y_2^{\lambda} + \dots + x_r^{\lambda_i} y_r^{\lambda} = 0$ $(i = 1, 2, \dots, n)$

$(*) \cdot y^{\lambda} - (**) \cdot y$: $x_1^{\lambda_i} \underbrace{(y_1 y^{\lambda} - y_1^{\lambda} y)} + x_2^{\lambda_i} (y_2 y^{\lambda} - y_2^{\lambda} y) + \dots + x_r^{\lambda_i} (y_r y^{\lambda} - y_r^{\lambda} y) = 0$

$(i = 1, \dots, n)$

$y := y_1 \neq 0 \longrightarrow 0$ $\Rightarrow$ $\forall$ más elem. is 0, mert r minimális.

$y_k^* = y_k y^{\lambda} - y_k^{\lambda} y = 0.$ $(k = 1, 2, \dots, r)$

$(y_k y^{-1})^{\lambda} = y_k y^{-1}$ λ tetszőleges volt $\Rightarrow$ $\underbrace{y_k y^{-1}}_{a_k \neq 0} \in K_0.$

$\Rightarrow$ $y_k = a_k y.$

$x_1 y_1 + \dots + x_r y_r = 0$ $(\lambda_i = id \in G$ -re$)$

$y(a_1 x_1 + \dots + a_r x_r) = 0$ $\longrightarrow$ az x-ek nem lineárisan ↯ $\square$

„Itt mindenek Galois a neve, és teljes joggal."

<u>Def.</u> Részben rendezett halmaz: $(H, \leq)$ (poset)

1) $a \leq a$ $(\forall a \in H)$ reflexív

2) $a \leq b$, $b \leq c$ $\Rightarrow$ $a \leq c$ tranzitív

3) $a \leq b$, $b \leq a$ $\Rightarrow$ $a = b$ antiszimmetrikus

<u>Példa.</u> $(\mathcal{P}(\mathbb{R}), \subseteq)$

$(\mathbb{N}, \mid)$

$(\mathcal{P}(X), \subseteq)$

„Ezt nevezni fogjátok, mert nagyon könnyű."

Ha H véges: Hasse-diagram. Csak a fedéseket ábrázoljuk.

<u>Def.</u> $a \prec b$ (a fedi b-t), ha $a < b$ és $\nexists x$: $a < x < b$

A rajzos fogalmak bevezethetők (izomorfizmus stb.)

Némely végtelenek is: $\mathbb{Z}$

(ezért lánc a teljesen rendezett)

<u>Kérdés.</u> Hány 4 elemű poset van?

<u>Def.</u> $(H, \leq)$ poset háló, ha ($a, b \in H$-re c a és b alsó korlátja, ha $c \leq a, b$)

$\forall a, b \in H$-ra van legnagyobb alsó korlát: $a \wedge b$, és

(a és b felső korlátja c, ha $a, b \leq c$)

$\forall a, b \in H$-ra van legkisebb felső korlát: $a \vee b$.

$\wedge$ és $\vee$ résztelmezésben a $\cap$ és az $\cup$ lesz.

$(H, \wedge, \vee)$-ra

1) $a \vee a = a, \quad a \wedge a = a$ — idempotencia

2) $a \vee b = b \vee a, \quad a \wedge b = b \wedge a$ — kommutatív

3) $a \vee (b \vee c) = (a \vee b) \vee c$

$a \wedge (b \wedge c) = (a \wedge b) \wedge c$ — asszociativitás

4) $(a \wedge b) \vee a = a$

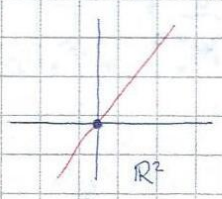
$(a \vee b) \wedge a = a$ — abszorpciós tulajdonság.

Könnyű ellenőrizni, hogy ha ezeket követeljük meg, az eredeti definíciót kapjuk, tehát a két megfogalmazás ekvivalens. (gyak)

2016.04.22.

Gyakorlaton: moduláris hálók, disztributív hálók (vizsgaanyag: 1., 3–6.)

Legyen K test, $P_n(K)$ n-dim proj. tér, $A_n(K)$ n-dim affin tér. (K^n alterei és azok eltolt(ai))



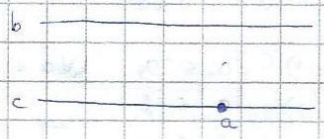
$P_n(K) = K^{n+1}/K$

$\downarrow$

ez maga is háló $\subseteq$-ra a részhalmazokon (metszet, generált részhalmaz)

Áll. $P_n(K)$ moduláris háló, (HF).

Példa. $A_2(\mathbb{R})$ nem moduláris.



$a \leq c$, de $a \vee (b \wedge c) = a$,

$(a \vee b) \wedge c = c$. (Ugyanez az okoskodás bármely $A_2(K)$-ra elmondható).

Megj. $\forall L$ hálóban $a \leq c \Rightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$. (tehát összehasonlíthatók is)
(Metaállítás: minden állítás unió $\leq$ metszet alakú, nem fordítottan.)

Def. L moduláris, ha $a, b, c \in L$, $a \leq c$-re: $a \vee (b \wedge c) = (a \vee b) \wedge c$.

Példa. Csoport normálosztóinak hálója moduláris. (gyak)

Áll. M modulus résmodulusai mod. háló (NB: innen nőnevük az elnevezés)

B: Elég: $A, B, C \leq M$, $A \leq C \Rightarrow A \vee (B \wedge C) \geq (A \vee B) \wedge C$.

Modulus-jelölésekkel: $A + (B \cap C) \supseteq (A + B) \cap C$.

$a + b = c$

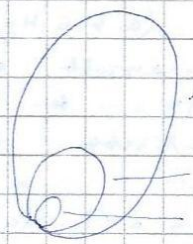
$\Rightarrow b = c - a \in C$, mert $A \leq C$

Tehát az $a + b = c$ alakú elemek a bal oldalon is ott vannak. $\square$

Jel. $L(G)$ G résztcsoport-hálója.

Áll. A Abel $\Rightarrow L(A)$ moduláris.

Tétel (BN): $L(G)$ disztributív $\Longleftrightarrow$ G lokálisan ciklikus.

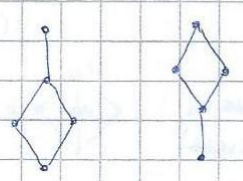


Def. G lokálisan T, ha $\forall$ végesen generált résztcsoportja T.

Mj. Véges csoport lok. ciklikus $\iff$ ciklikus.

Köv. Speciálisan minden nem Abel-csoport nem distributív.

Metamegjegyzés. Minden tétel duálisa is igaz, mert az axiómarendszer önduális. (Ezt ne írtuk fel.)



duális háló (a Hasse-diagram fejjel lefelé fordítása, $\wedge$ és $\vee$ felcserélődik)

Vizsgáljuk behatóbban $L(G)$-t!

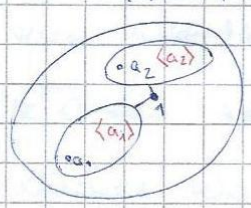
Tétel. $L(G)$ véges $\iff$ G véges.

B: $\Leftarrow$: triviális.

$\Rightarrow$: $|G| = \infty$-re ha $o(a) = \infty$, akkor $\langle a \rangle$-nak ∞ sok részcsoportja van. $|G| = \infty$, és torziócsoportra kell még belátni.

Sorban lehet nem generált elemeket venni: $\langle a_1 \rangle, \langle a_2 \rangle, \dots$

$\rightarrow$ ∞ sok res. van. $\square$



Mi a háló és $L(G)$ kapcsolata (milyen a hatványrendelés?

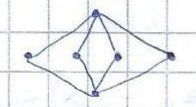
Példák. 1) $L(G) =$ $\iff$ $G \simeq Z_p$ (nincs valódi résztcsoport)

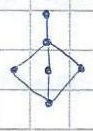
2) $L(G) =$  $\iff$ $G \simeq Q$

1b) $L(G) =$  $\iff$ $G \simeq Z_{p^2}$

1b: Ez nyilván jó. Másrészt műszeglelppen p-csoport, mert különben lenne benne Z_p és Z_q is, ha $p \cdot q \mid |G|$. És műszeglelppen a középső elem minimalitása miatt az Z_p. Sylow miatt p^2 rendű $\rightarrow$ Z_{p^2} vagy $Z_p \times Z_p$, de utóbbi nem jó.

2: p-csoport kell legyen, mert egyetlen elem fedi $\langle 1 \rangle$-et.
Akárhány p^2, legfeljebb egy p^3 rendű csoport van.
Általánosított Sylow: p^k rendűek száma $\equiv 1$ (p).
$3 \equiv 1$ (p) $\rightarrow$ $p = 2$. $\rightarrow$ 8 rendű csoport, azokat ismerjük.

3) $L(G) =$  $\Leftarrow$ $G \simeq Z_3 \times Z_3$, S_3 (HF: nincs több)

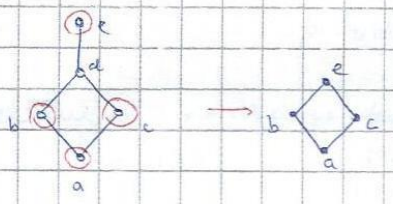
4) $L(G) =$  : nincs ilyen G csoport. A következő lemma miatt:

Lemma $|G| < \infty$, pontosan 1 maximális résztcsoportja van $\rightarrow$ $G \simeq Z_{p^n}$

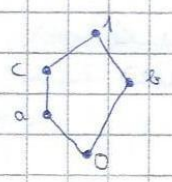
B: Ezek jók: láncot alkotnak 

Bármely M-en kívüli elem generálja G-t $\rightarrow$ ciklikus.
p-csoport kell legyen, különben több max. lenne. $\square$

Def. Résztháló: zárt $\vee$-ra és $\wedge$-re.



résztalmat, ami háló, nem feltétlenül résztháló
Itt $b \vee c = d$, ami nincs benne.



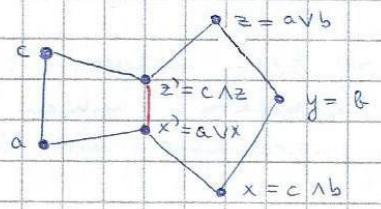
N_5

$a \vee (b \wedge c) = a \vee 0 = a$
$(a \vee b) \wedge c = 1 \wedge c = c$

$\longrightarrow$ nem moduláris.
(nb. ez a legkisebb)

Tétel. L háló moduláris $\iff$ nincs N_5-tel izomorf résztháló-ja.

B: Ha moduláris, akkor $\forall$ résztháló moduláris, így nem lehet N_5 résztháló. ✓
Megmutatjuk, hogy ha nem moduláris, akkor van N_5.
Tfh. L nem mod.: $a, b, c \in L$, $a \leq c$, $a \vee (b \wedge c) < (a \vee b) \wedge c$.
Tfh. $a < c$: ha $a = c$, abszorpció miatt nem igaz a fenti.



Itt a vonal nem fedés, csak $\leq$.

Állítjuk: $x' < z'$. Valóban:
$x' = a \vee (b \wedge c) < (a \vee b) \wedge c = z'$.

Ezzel megvan, hogy miből adunk, hogy N_5.
Kell: nem egyenlőek és résztháló.

x, y, z valóban láncot alkotnak, és x, x', z', z is lánc.
Kéne: $z' \wedge y = x' \wedge y = x$, $z' \vee y = x' \vee y = z$, ezzel a résztháló meglesz.

$x' \vee y = (a \vee x) \vee y = a \vee (b \wedge c) \vee b = a \vee b = z$ ✓
$z' \vee y \leq z$, $z' \vee y \geq x' \vee y \implies z' \vee y = z$ ✓

$z' \wedge y = c \wedge z \wedge y = c \wedge (a \vee b) \wedge b = c \wedge b = x$ ✓
$x' \wedge y \geq x$, $x' \wedge y \leq z' \wedge y = x \implies x' \wedge y = x$ ✓

Belátjuk, hogy ez tényleg 5 elemet ad.

$\lightning$ $x = y$. $\iff b \wedge c = b \iff b \leq c$
Ekkor $x' \wedge y = x' \wedge x = x = y$.
$x' \vee y = x'$
De $x' \vee y = z$ $\implies x' = z$, de $x' < z' \leq z$ $\lightning$

Dualisan $z \neq y$.

$\lightning$ $z' = z \implies y \vee z' = z = z' \implies y \leq z'$
$y \wedge z' = y$
De $y \wedge z' = x$ $\longrightarrow$ $x = y$ $\lightning$

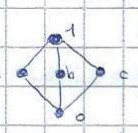
Dualisan $x \neq x'$.

$\lightning$ $x' = y \Rightarrow x = x' \wedge y = y \wedge y = y$ $\lightning$.

Duálisan $z' \neq y$.

Ezzel az N_5-öt kizártuk megtalálhatóra. $\square$

Tétel. (BN) L háló distributív $\iff$ nincs se N_5-tel, se M_5-tel izomorf részhálója.

Példa. 

M_5 rendisztributív, de moduláris: nincs benne N_5

Észr. $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ mindig fennáll

JH nem áll fen a distr.: $a \vee (b \wedge c) = 0$, de
$(a \vee b) \wedge (a \vee c) = 1$.

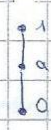
Def. Korlátos háló: van legnagyobb (mindenél nagyobb) és legkisebb eleme. Ezek jele $0, 1$.

Észr. Véges háló korlátos.

Példa. $(\mathbb{Z}, \leq)$ nem korlátos.

Észr. Korlátossá tevő: legfelülre és legalulra 1-1 elem hozzávétele.

Def. L korlátos hálóra $b \in L$ komplementuma $a \in L$-nek, ha $a \wedge b = 0$,
$a \vee b = 1$.

Nem mindig van: 

a-nak nincs komplementuma.

0 és 1 egymás komplementumai.

Lehet több is: M_5-ben a-nak b és c is komplementuma.

Áll. Distributív L hálóban ha $a \in L$-nek van komplementuma, akkor az egyértelmű.

B: $\lightning$ a-nak a' és a'' komplementumai.

$$a' = a' \wedge 1 = a' \wedge (a \vee a'') \underset{D_1}{=} (a' \wedge a) \vee (a' \wedge a'') = 0 \vee (a' \wedge a'') = a' \wedge a''$$

Fordítva $a'' = a' \wedge a''$. $\Rightarrow a' = a''$. $\square$

Def. Boole-algebra: korlátos distributív háló, melyben minden elemnek van komplementuma. Jel.: a komplementuma a'.

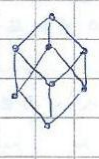
Def. Komplementumos háló: $\forall$ elemnek van komplementuma.

Példa. $\mathcal{P}(H)$ Boole-algebra, $A \in \mathcal{P}(H)$-ra $A' = H \setminus A$.

$|H| = 0$ 

$|H| = 1$ 

$|H| = 2$ 

$|H| = 3$ 

$|H| = n \longrightarrow n$-dimenziós kocka.

Tétel. (BN). Véges Boole-algebrák mind $\mathcal{P}(H)$ alakúak.

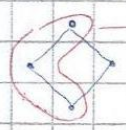
Példa: $|H| = \aleph_0$ véges és kovetges részhalmazok megad. Boole-algebrát adnak.

2016. 04. 29.

Def. $\langle B; \wedge, \vee, ', 0, 1 \rangle$ Boole-algebra (bővebb axiómarendszerrel):

$$1 \wedge x = x,$$
$$0 \wedge x = 0,$$
$$x \wedge x' = 0,$$
$$x \vee x' = 1.$$

Ez azért szerencsésebb def., mert a rács-Boole-algebra fogalma egyszerűbb.



→ rácsháló, de nem rács-Boole-algebra

Def. $\mathcal{P}(H)$ rács-Boole-algebrája: halmaztest.

Tétel. (Stone) Minden Boole-algebra izomorf egy halmaztesttel.

Mivel ez csak bebizonyíthatóságról szól, ez nem annyira erős, mint amilyen látszik.

Def. $\mathcal{P}(H)$ rácsháló: halmazgyűrű.

Tétel. Minden disztributív háló izomorf egy halmazgyűrűvel.

Mj. Boole-algebrák $\longleftrightarrow$ egységelemes Boole-gyűrűk

① $a + b = (a' \wedge b) \vee (a \wedge b')$
$ab = a \wedge b$
$\langle B, \wedge, \vee, ', 0, 1 \rangle \longrightarrow (B, +, \cdot)$ egységelemes (nulla)

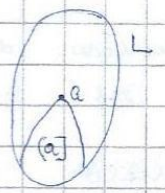
② $(B, +, \cdot)$ egységelemes $\longrightarrow \langle B, \wedge, \vee, ', 0, 1 \rangle$ (nulla)
$a \vee b = ab + a + b$
$a \wedge b = ab$

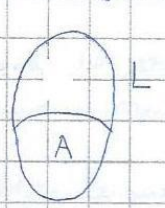
Észr. $(a \vee b)' = a' \wedge b'$; $(a \wedge b)' = a' \vee b'$ De Morgan-azonosság, fennáll minden B-algebrában.

Def. $A \subseteq L$ ideál L-ben $(A \triangleleft L)$, ha $a, b \in A \Rightarrow a \vee b \in A$,
$a \in A,\ x \in L,\ x \leq a \Rightarrow x \in A$ (erős: $a \in A, y \in L \Rightarrow a \wedge y \in A$)

Def. Generált ideál, főideál.

Ntl. $(a] = \{ x \in L : x \leq a \}$





Def. Duális ideál $B \subseteq L$: $a, b \in B \Rightarrow a \wedge b \in B$,
(filter, szűrő) $a \in B,\ x \in L,\ x \geq a \Rightarrow x \in B$.

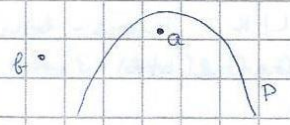
Def. $\emptyset \neq P \subsetneq L$ prímideál: ideál és $a, b \in L,\ a \wedge b \in P \Rightarrow a \in P$ vagy $b \in P$.

Def. $\emptyset \neq P^* \subsetneq L$ duális prímideál: ideál és $a, b \in L,\ a \vee b \in P^* \Rightarrow a \in P^*$ vagy $b \in P^*$.
(ultrafilter, ultraszűrő)

Észr. Ideál prím $\Leftrightarrow$ halmazelméleti komplementuma duális ideál.

Tétel (Stone) Legyen L disztributív háló. Ekkor bármely két különböző elem elválasztható primideállal; pontosabban ha $b \not\leq a$, akkor $\exists P$ primideál, hogy $a \in P$, $b \notin P$.

(Sincs ideál, amiben benne: $b \notin (a]$.)



B: $X \triangleleft L$, $\underbrace{X \ni a}_{X \supseteq (a]}$, $X \not\ni b$ tipusúakat nézzük.

Teljesül az X-re a Zorn-lemma feltétele. Láncok uniója is tartalmazza a-t, b-t nem.

Legyen P maximális ilyen. Elég, hogy P primideál.
Legyen $x, y \notin P$. Be kell látni, hogy $x \wedge y \notin P$.

$U = \{ u \mid \exists p \in P \,.\, u \leq x \vee p \}$. $P \subseteq U$, hiszen $p \leq x \vee p$.

Másrészt $x \in U$: $x \leq x \vee p$. $\Rightarrow$ $P \subsetneq U$.

Továbbá $U \triangleleft L$: $u_1 \leq x \vee p_1$, $u_2 \leq x \vee p_2$-re: $u_1 \vee u_2 \leq x \vee \overbrace{(p_1 \vee p_2)}^{\in P}$,
és nyilván minden $\leq u_1$ elem U-beli.

P maximális volt $\Rightarrow$ $b \in U$, azaz $\exists p_1 \in P$: $b \leq x \vee p_1$.

Ugyanez elvégezhető y-nal is x helyett $\longrightarrow$ $b \leq y \vee p_2$.

$p = p_1 \vee p_2 \in P$-re $\quad b \leq x \vee p_1 \leq x \vee p$,
$\qquad\qquad\qquad\qquad b \leq y \vee p_2 \leq y \vee p$.

$\Rightarrow$ $b \leq (x \vee p) \wedge (y \vee p) \underset{\text{disztributivitás}}{=} (x \wedge y) \vee p$ $\quad$ Ha $x \wedge y \in P \Rightarrow (x \wedge y) \vee p \in P$
$\Rightarrow b \in P$, ami $\lightning$
Így $x \wedge y \notin P$. $\square$

Most bebizonyítjuk a két korábbi reprezentációs tételt.

B: Legyen D disztributív háló. $H := \{ D$ duális primideáljai$\} \neq \emptyset$ a fenti tétel miatt

$x \in D \longrightarrow H(x) = \{ P^* \mid P^*$ duális primideál, $x \in P^* \}$ a fenti tétel miatt $\neq \emptyset$

- Ha D Boole-algebra: $H(1) = H$, mert $\forall$ d.p.i.-ben benne van 1.
  $H(0) = \emptyset$, mert d.p.i. nem lehet a teljes D.
- Kell, hogy $x \neq y \rightarrow H(x) \neq H(y)$, hogy tényleg beágyazást kapjunk, pontosan ezt mondja ki a fenti tétel.
- Kell: $H(x) \cap H(y) = H(x \wedge y)$. Gyűrűk módszere.
  $\supset$ $x \wedge y \leq x, y$ miatt
  $\subset$ ami a bal oldalon van, tartalmazza x-et és y-t $\longrightarrow$ d.i. miatt $x \wedge y$-t is.
- $H(x) \cup H(y) = H(x \vee y)$:
  $\supset$ felhasználva, hogy d.p.i. (csak itt használjuk, hogy d. prím)
  $\subset$ $x \leq x \vee y$ miatt.
- Ha D Boole-algebra: $H(a') = H \setminus H(a)$ kell.

Ez két dolgot jelent: $H(a) \cap H(a') = \emptyset$, mert $a \wedge a' = 0$
$H(a) \cup H(a') = H$, mert $a \vee a' = 1$ és d. prim □□

Most visszakanyarodunk a testbővítésekhez.

Legyen $L|K$ Galois-bővítés. Tekintsük a bővítés közbenső testeit. $\longrightarrow$ háló $\cap, \langle \cdot, \cdot \rangle$-re.
Legyen $G = Gal(L|K)$ $\longrightarrow$ $L(G)$ háló

<u>A Galois-elmélet alaptétele.</u> $L(G)$ és a közbenső testek hálója dualisan izomorfak (egyik izomorf a másik dualisával).

„Mama még absztrakt vizeken evezünk."

Legyen $L|K$ bővítés (egyelőre általános, valóban érdemes végeset nézni).

$$K \leq M \leq L \longmapsto M^* = \{\varphi \in G \mid x^\varphi = x \quad \forall x \in M\} \leq G$$

$$1 \leq H \leq G \longmapsto K \leq H^\circ = \{x \in L \mid x^\varphi = x \quad \forall \varphi \in H\} \leq L.$$

Világos, hogy H° test, $K \leq H^\circ$ a Gal-csoport elfixje miatt és $H^\circ \leq L$. triv.

Ha $H_1 \leq H_2 \leq G \Rightarrow H_1^\circ \geq H_2^\circ$.
Ha $M_1 \leq M_2 \leq L \Rightarrow M_1^* \geq M_2^*$ } definícióból

$H^{\circ *} \geq H$; $M^{*\circ} \geq M$ (definícióból), $\Rightarrow H^{\circ * \circ} \leq H^\circ$

Most már feltesszük, hogy $L|K$ Gal-bővítés. (Egy darabig még megjelenik ennek, de így egyszerűbb)

<u>Áll.</u> $H \leq G$-re $(H^\circ : K) = \dfrac{(L:K)}{|H|}$.

B: $(L:K) = (L:H^\circ)\cdot(H^\circ : K)$ fokszámtétel. Elég, hogy $(L:H^\circ) = |H|$
Ezt pedig véges csoportokra tudjuk. (fixtestes tétel) A'

<u>Áll.</u> $L|K$ Galois $\Rightarrow G^\circ = K$. (Ez az alaptétel egy nagyon speciális esete, és már önmagában is erős állítás)

B: $(L:G^\circ) = |G|$ (fixtestes tétel)
$|G| = (L:K)$ $K \leq G^\circ$
$\Rightarrow$ fokszámtétel szerint G° foka K felett 1 $\rightarrow G^\circ = K$. A'

Most már tényleg ráfordulunk az alaptétel bizonyítására.

Elegendő belátni, hogy $*$ és $\circ$ egymás inverzei. Ekkor nyilvánvaló műveleptép kölcs. egyértelműek. És nyilván a rendezéstartás és a háttérműveletek tartása nem ekvivalens, de kölcsönösen egyértelműek az.

<u>Áll.</u> $M^{*\circ} = M$.

B: $L|M$ nyilvánvalóan, mert felső ötöros.
$M^* = Gal(L|M)$.
Az előző állítás igazolja, hogy $M^{*\circ} = M$. A'

Áll. $H^{o*} = H$.

B: $M = H^o \Rightarrow H^{o*o} = H^o$ az előző szerint.

$|H| = (L : H^o)$ (ez minden végessre igaz)

$|H^{o*}| = (L : H^{o*o})$ Tehát $H = H^{o*}$, mert egyik része a másiknak és a fokszámuk egyezik. A

Ezzel az alaptétel bizonyítása kész. □

Köv. Galois-bővítésre a kölcsönös testek halmaza véges.

De nincs nem mintaj Galois-bővítésnek lenni:

Tétel. $L|K$ véges bővítés egyszerű $\Leftrightarrow$ közbülső testek halmaza véges.

B: $\Leftarrow$: Ha K (és így L is) véges, akkor a bővítés valóban egyszerű, mert a mult. csoport ciklikus.
Legyen tehát $|K| = \infty$.

$L = K(\alpha_1, \dots, \alpha_n)$, kiír a bővítés véges. Indukció n szerint.
$n = 1$: épp az kell. TFH. $(n-1)$-ig már megvan, $n \geq 2$.

$K(\alpha_1, \dots, \alpha_{n-1}) = K(\beta)$ indukció miatt.
$L = K(\alpha_n, \beta)$.
Legyen $a \in K$. $M_a = K(\alpha_n + a\beta) \longrightarrow K \leq M_a \leq L$
K végtelen, de csak véges sok közb. test van.
$\Rightarrow \exists\, a, a' : M_a = M_{a'} = M$.

$$\left.\begin{array}{l} \beta = \dfrac{(\alpha_n + a\beta) - (\alpha_n + a'\beta)}{a - a'} \in M \longrightarrow \beta \in M. \\ \alpha_n = (\alpha_n + a\beta) - a\beta \in M \longrightarrow \alpha_n \in M \end{array}\right\} \Rightarrow L \leq M \Rightarrow L = M,$$

tehát $L = K(\alpha_n + a\beta)$ ✓

$\Rightarrow$: Legyen $L = K(\alpha)$. α kar. polinomja K felett p. (irreducibilis)
Legyen $K \leq M \leq L$. α — " — M felett q

Szükségképp $q(x) \mid p(x)$. Legyen $q(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in M[x]$.

$M_0 = K(a_0, \dots, a_{n-1}) \leq M$. α kar. polinomja M_0 felett $s(x)$.

$q \in M_0[x]$. $\Rightarrow s(x) \mid q(x)$.

Tekintsük $(L : M)$-et: $(L : M) = \deg q$, mert a bővítés egyszerű.
$\deg q \geq \deg s = (L : M_0)$.
Fokszámtétel: $(L : M_0) = (L : M)(M : M_0) \Rightarrow (L : M) = (L : M)(M : M_0)$

$\Rightarrow (M : M_0) = 1. \Rightarrow M = M_0$. L felett nincs p-nek csak véges sok osztója lehet. □

2016. 05. 13.

Tekintsük $\mathbb{Q}$ felett x^4-2 felbontási testét.

$K = \mathbb{Q}$

$L = \mathbb{Q}(\sqrt[4]{2}, i)$, mert a polinom gyökei $\mathbb{C}$-ben $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$.

$(L:K) = 8$, mert $\sqrt[4]{2}$ fokú 4, i fokú 2. $\longrightarrow$ véges bővítés

A bővítés normális, mert felbontási test, és separabilis, mert char $= 0$.

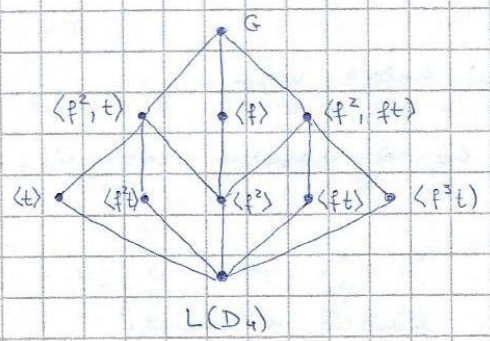
$G = Gal(L|K) \longrightarrow |G| = 8$.

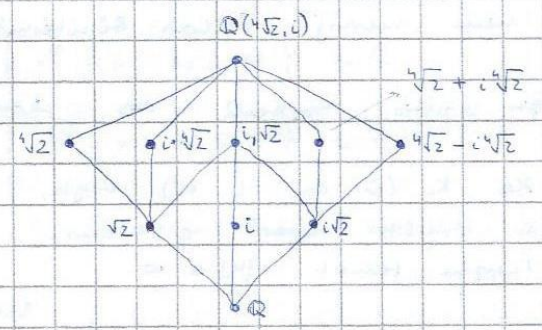
Legyen $f: \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \quad i \mapsto i \quad \Rightarrow \quad f$ rendje 4

$t: \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad i \mapsto -i \quad \Rightarrow \quad t$ rendje 2

$t^{-1} f t = f$

Dyck-tétel: $G \simeq D_4$





Galois-feladat: a D_4-et jellemzi a résztestcsoportrácsja.

Itt a bővítések minden egymenőzőt is felismerhetők lesznek (véges separabilis bőv.)

— o —

Gyökjelekkel való megoldhatóság

Def. $f \in K[x]$-re legyen L a K feletti felb. test. $L|K$ véges és normális automatikusan.
A technikai nehézségek elkerülése végett tfh. char $K = 0 \longrightarrow$ separabilitás.
Ekkor $Gal_K(f) = Gal(L|K)$.

Azon permutációkat vesszük itt, amik megtartják a gyökök közti összefüggéseket.

Pl. $\alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = i\sqrt[4]{2}, \quad \alpha_3 = -\sqrt[4]{2}, \quad \alpha_4 = -i\sqrt[4]{2}. \longrightarrow \alpha_1 + \alpha_3 = \alpha_2 + \alpha_4$ fennáll.
A fenti Galois-csoport $Gal_{\mathbb{Q}}(x^4-2)$.

A többszörös gyökök rendelkezése elkerülése végett tfh. f irreducibilis.

Áll. G tranzitív permutáció-csoport.

B: $\deg f = n$, $G \leq S_n$.
Bármely gyök átírható egy másikba, és ez kiterjeszthető testautomorfizmussá. □

Def. $L|K$ radikálbővítés, ha $\exists \alpha_1, \dots, \alpha_n \in L$: $L = K(\alpha_1, \dots, \alpha_n)$, $\forall k \; \exists n(k)$:
$\alpha_k^{n(k)} \in K(\alpha_1, \dots, \alpha_{k-1})$.

Mj. minden radikálbővítés véges. Nullkarakterisztikában vagyunk, így separabilis.
A normalitás nem feltételnek áll fenn.

Def. $f \in K[x]$ megoldható gyökjelekkel, ha a felbontási teste beágyazható radikálbővítésbe, azaz ha L a felb. test, akkor $\exists R|K$ r.bővítés, hogy $K \leq L \leq R$.

Tétel. (BN) $f \in K[x]$-re $\exists R$, hogy $K \leq L \leq R$, ahol L a felb. test $\iff$ $Gal_K(f)$ feloldható.

A bizonyítás standard anyag, Kiss, Fried, Fuchs jegyzetében elolvasható (és érdemes!).

Tétel. $x^5 - 6x + 3$ nem oldható meg gyökjelekkel. (Mint $\mathbb{Q}[x]$ feletti polinom.)

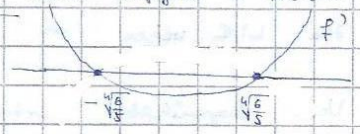
B. $f(x) = x^5 - 6x + 3$ irreducibilis: Schönemann – Eisenstein $p = 3$.

$G = Gal_{\mathbb{Q}}(x^5 - 6x + 3)$ tranzitív. Megmutatjuk, hogy S_5.

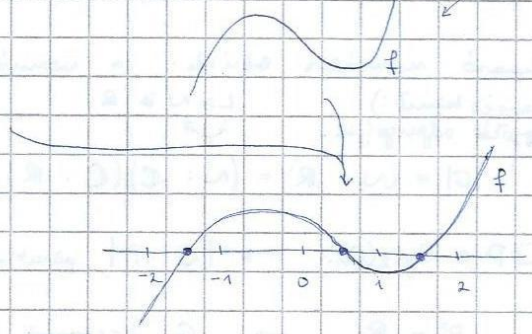
$5 \mid |G|$, $G \leq S_5$. $\longrightarrow$ ftm. $(12345) \in G$, mert kell legyen 5 rendű elem.

mert G tranzitív

$f'(x) = 5x^4 - 6$



x	$f(x)$
-2	-17
-1	8
0	3
1	-2
2	23



Van két komplex gyök, amik így egymás konjugáltjai kell legyenek. A komplex konjugálás megmutatása a felbontási testre automorfizmus.

$\Rightarrow$ átrámozással elérhető, hogy $(12), (12345) \in G$.

Tehát $G = S_5$, amiből kapjuk, hogy nem oldható fel. $\square$

Def. K algebrailag zárt, ha $\forall f \in K[x]$, $\deg f \geq 1$ $\exists \alpha \in K$: $f(\alpha) = 0$.
$\iff$ $\forall f \in K[x]$ gyöktényezőire bomlik $\iff$ ha $L|K$ algebrai bővítés, akkor $L = K$.

Def. L a K test algebrai lezártja, ha $L|K$ algebrai bővítés és L algebrailag zárt.

Tétel. (BN) $\forall K$: $\exists L$ algebrai lezárt, és ha L_1, L_2 alg. lezártak, akkor $L_1|K \cong L_2|K$.
(A bizonyítás a Zorn-lemma alapul.)

Jel. Az algebrai lezárt $\overline{K}$.

Példa. $\overline{\mathbb{Q}} = \mathbb{A}$, $\overline{\mathbb{R}} = \mathbb{C}$

$\overline{\mathbb{F}_p}$ az összes p^n elemű testet tartalmazza valamely módon, végtelen test, de az nem nyilvánvaló, hogy miféle.
$\overline{\mathbb{F}_p} = \overline{\mathbb{F}_{p^n}}$.

Tétel. $\mathbb{C}$ algebrailag zárt. (Az „algebra alaptétele!")

Bi: **Liouville-tétel:** (BN) $f: \mathbb{C} \to \mathbb{C}$ egész fv. (mindenütt differenciálható) korlátos $\Rightarrow$ konstans.

Legyen $f \in \mathbb{C}[x]$, $\deg f \geq 1$. $\lightning$ Tfh. f-nek nincs gyöke. $\Rightarrow \frac{1}{f}$ egész függvény.

$\frac{1}{f}$ korlátos (mert $|z| \to \infty$ mellett $|f(z)| \to \infty$, így $\exists K$: $|z| > K \Rightarrow \left|\frac{1}{f}\right| \leq 1$,

és $|z| \leq K$ kompakt, így ezen $\frac{1}{f}$ korl.) $\Rightarrow \frac{1}{f}$ konstans. $\lightning$

B_2: <u>Áll.</u> $\mathbb{R}$ felett minden pt. fokú polinomnak van gyöke.

B: Bolzano-Weierstrass.

Ekvivalens: $\mathbb{R}$-nek nincs önmagától különböző pt. fokú bővítése (kihasználjuk a nullkarakterisztikából következő separábilitást)

<u>Áll.</u> Minden komplex számnak van négyzetgyöke.

Ekvivalens: $\mathbb{C}$-nek nincs másodfokú bővítése.

Ez a két állítás az, amik kihasználjuk, hogy miszerint $\mathbb{R}$ és $\mathbb{C}$.

<u>Áll.</u> $L|\mathbb{C}$ véges $\Rightarrow$ $L = \mathbb{C}$.

B: Ha $L|\mathbb{C}$ véges $\Rightarrow$ $L|\mathbb{R}$ is véges, de nem felt. normális.

Van legszűkebb tartalmazó normális bővítés: a normális lezárt, $N|\mathbb{R}$.
(A normális lezárt egyértelmű:) $L \geq N \geq \mathbb{R}$.
a konstans polinomok összes gyökét odajegyezzük.

$Gal(N|\mathbb{R}) = G$. $\rightarrow$ $|G| = (N:\mathbb{R}) = (N:\mathbb{C})(\mathbb{C}:\mathbb{R}) = 2(N:\mathbb{C})$,

tehát $2 \mid |G|$. $\rightarrow$ $\exists P \in Syl_2(G)$. $\rightarrow$ $|G:P|$ páratlan.

$|G:P| = (P^\circ:\mathbb{R}) \xrightarrow{\text{1. áll.}} P^\circ = \mathbb{R}$ $\rightarrow$ G 2-csoport.

$Gal(N|\mathbb{C}) \leq Gal(N|\mathbb{R})$ $\rightarrow$ $Gal(N|\mathbb{C})$ is 2-csoport.

$\lightning$ $Gal(N|\mathbb{C}) \neq 1$. $\rightarrow$ legyen M 2 indexű részcsoport. (Sylow-tétel)

$\Rightarrow (M^*:\mathbb{C}) = 2$, de ilyen bővítés nincs. $\lightning$
(2. áll.)

— o —

<u>Geometriai szerkeszthetőség</u> (nem vizsgaanyag)

Minden konvertálható szakasszá: szög helyett a szinusza. Egységszakasz adott.

Egységszakasz $\longrightarrow$ $\mathbb{Q}$ kosszal megvannak.

Ehhez Galois-elmélet nem kell, csak a bővítéstétel.

A szerkeszthetőt mind másodfokú algebrai számok (a megfordítás nem igaz!)

<u>Kocka megkettőzés.</u> $\sqrt[3]{2}$ nem szerkeszthető meg.

<u>Szögharmadolás.</u> $\cos 20^\circ$ nem szerkeszthető meg ($\cos(3x)$ alapján harmadfokú)

<u>Körnégyszögesítés.</u> $\sqrt{\pi}$ nem algebrai, mert π sem az.

<u>Szabályos n-szög:</u> akkor és csak akkor szerkeszthető, ha $n = 2^a \cdot p_1 \cdots p_k$,
ahol $a \geq 0$ és $p_1, \dots, p_k$ különböző Fermat-prímek.

Az ismert Fermat-prímek: $F_n = 2^{2^n} + 1$, ahol $n = 0, 1, 2, 3, 4$.