Szükséges előismeretek a „Magasabb fokú egyenletek és geometriai szerkeszthetőség” című tárgyhoz

CSOPORTOK

Fogalmak: csoport, részcsoport, normálosztó, generálás, konjugáltság, faktorcsoport, homomorfizmus, szimmetrikus és alternáló csoportok.
Tételek: Lagrange-tétel, homomorfiatétel, izomorfiatételek, megfeleltetési tétel, az alternáló csoportok egyszerűsége.
1. feladat: Legyen V a Klein-féle négyes csoport:

$$V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

Mutassa meg, hogy V normálosztója S_4-nek, és így A_4-nek is. Írja fel az A_4/V faktorcsoport elemeit és a művelettáblázatát. Melyik „ismert” csoporttal izomorf A_4/V?
2. feladat: Jelölje $\ell_{a,b}$ az $x \mapsto ax + b$ lineáris függvényt a valós számok halmazán, és legyen

$$\begin{aligned} G &= \{\ell_{a,b} \colon a, b \in \mathbb{R}, a \neq 0\}, \\ H &= \{\ell_{a,0} \colon a \in \mathbb{R}, a \neq 0\}, \\ N &= \{\ell_{1,b} \colon b \in \mathbb{R}\}. \end{aligned}$$

Ellenőrizze, hogy G csoportot alkot a leképezések szorzásával (kompozícióval). Igazolja, hogy H és N is részcsoportja G-nek, és határozza meg mindkettőhöz a bal- és jobboldali mellékosztályokat. Mutassa meg, hogy N normálosztó, de H nem az. Határozza meg a G/N faktorcsoportot, és állapítsa meg, hogy melyik „ismert” csoporttal izomorf a faktorcsoport.
3. feladat: Írja fel az első izomorfiatételt az előző feladatbeli G csoport H és N részcsoportjaira. Ennek segítségével még egyszer (és kevesebb számolással!) megkapjuk a G/N faktorcsoportot.
4. feladat: Keressen olyan φ szürjektív homomorfizmust a 2. feladatban szereplő G csoportról egy alkalmasan választott csoportra, amelynek magja éppen N. Írja fel a homomorfiatételt erre a φ homomorfizmusra. Így harmadszor is megkapjuk a G/N faktorcsoportot.
5. feladat: Az első izomorfiatétel segítségével igazolja, hogy $S_4/V \cong S_3$. (Keressen S_4-ben egy megfelelő H részcsoportot, majd alkalmazza az első izomorfiatételt a $G = S_4,\ N = V$ szereposztással.)
6. feladat: Határozza meg S_4 összes olyan részcsoportját, amelyik tartalmazza V-t, és rajzolja fel ezen részcsoportok (tartalmazás szerinti) Hasse-diagramját. A megfeleltetési tétel segítségével határozza meg S_4/V összes részcsoportját, és rajzolja fel a Hasse-diagramjukat. (Vesse össze ezt az 5. feladat eredményével.) Keressen S_4-ben olyan részcsoportokat, amelyekre alkalmazható a második izomorfiatétel, és írja is fel a megfelelő izomorfiát.

KLASSZIKUS ALGEBRA
Fogalmak: komplex számokhoz kapcsolódó minden fogalom (különös tekintettel az egységgyökökre), test feletti polinom és polinomfüggvény, maradékos osztás, euklideszi algoritmus, legnagyobb közös osztó, irreducbilis polinom, gyök, többszörös gyök, szimmetrikus polinom, elemi szimmetrikus polinom.
Tételek: komplex számokról minden (különös tekintettel az egységgyökökre), test feletti polinomgyűrű euklideszi gyűrű (és így főideálgyűrű és Gauss-gyűrű is), „diofantoszi" egyenlet test feletti polinomgyűrűben, lnko és közös gyökök kapcsolata, az algebra alaptétele, irreducibilis polinomok $\mathbb{C}$ és $\mathbb{R}$ felett, Schönemann–Eisenstein-féle irreducibilitási kritérium, Rolle tétele a racionális gyökökről, számest feletti irreducibilis polinomnak nincs többszörös gyöke, harmad- és negyedfokú egyenletek megoldása (Cardano, Ferrari), Viète-formulák, a szimmetrikus polinomok alaptétele.
7. feladat: Határozza meg az alábbi polinomok irreducbilis faktorizációját $\mathbb{C}$, $\mathbb{R}$ és $\mathbb{Q}$ felett:

$$f_1 = x^6 + 27;$$
$$f_2 = x^8 - 16;$$
$$f_3 = x^7 + 7x^4 - 8x.$$

8. feladat: Határozza meg az alábbi polinomok irreducibilis faktorizációját $\mathbb{Q}$ felett:

$$f_1 = x^6 + 2x^5 + x^4 + 22x^3 + 55x^2 + 44x + 11;$$
$$f_2 = x^3 + 5x^2 + 6x + 1;$$
$$f_3 = 4x^4 - 7x^2 - 5x - 1.$$

9. feladat: Számítsa ki f és g legnagyobb közös osztóját, és adja meg az $fu + gv = \text{lnko}\,(f, g)$ egyenlet egy megoldását (a $\mathbb{Q}\,[x]$ polinomgyűrűben).

$$f = x^2 + x + 1,\ \ g = x^3 - 2;$$
$$f = x,\ \ g = x^3 - 2x + 2.$$

LINEÁRIS ALGEBRA
Fogalmak: vektortér, altér, generátorrendszer, lineáris függetlenség, bázis, dimenzió, végesdimenziós vektortér.
Tételek: bázis=maximális lineárisan független rendszer=minimális generátorrendszer, végesdimenziós vektortérben bármely két bázis elemszáma ugyanannyi.

GYŰRŰK
Fogalmak: gyűrű, részgyűrű, ideál, főideál, generálás, faktorgyűrű, homomorfizmus, integritástartomány, euklideszi gyűrű, főideálgyűrű, Gauss-gyűrű.
0.1. Tétel: Ha I ideál az R gyűrűben, akkor a $\nu\colon R \to R/I$, $a \mapsto a + I$ leképezés szürjektív homomorfizmus (természetes homomorfizmus). Tehát minden faktorgyűrű homomorf kép.
0.2. Tétel: Ha $\varphi\colon R \to S$ szürjektív gyűrűhomomorfizmus, akkor $\ker \varphi$ ideál az R gyűrűben, és $R/\ker \varphi \cong S$. Tehát minden homomorf kép faktorgyűrű.
0.3. Tétel: Ha R főideálgyűrű, de nem test, akkor az $R/(m)$ faktorgyűrű akkor és csak akkor test, ha m irreducibilis.

TESTEK
Fogalmak: test, karakterisztika, résztest, generálás, testbővítés, algebrai és transzcendens elem, minimálpolinom, egyszerű algebrai és egyszerű transzcendens bővítés.
0.4. Tétel: Legyen $L|K$ egy testbővítés, és legyen $\alpha \in L$ algebrai elem K felett, $m_{\alpha,K}$ minimálpolinommal. Ekkor $m_{\alpha,K}$ irreducibilis K felett; továbbá, ha $f \in K[x]$ irreducibilis főpolinom, melynek α gyöke, akkor $f = m_{\alpha,K}$.
0.5. Tétel: Legyen K test, $f \in K[x]$ irreducibilis n-edfokú polinom. Ekkor az $L = K[x]/(f)$ faktorgyűrű test, amelynek minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in K)$$

„kanonikus” alakban. (Itt a felülvonás a modulo f maradékosztályt jelöli, azaz $\overline{p} = p + (f)$ minden $p \in K[x]$-re.)
0.6. Tétel: Legyen $L = K(\alpha)$ egyszerű algebrai bővítése a K testnek, ahol α minimálpolinomja n-edfokú. Ekkor L minden eleme egyértelműen felírható

$$a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \quad (a_{n-1}, \ldots, a_0 \in K)$$

„kanonikus” alakban.
Megjegyzés: Az utolsó két tétel lényegében ugyanazt a dolgot írja le két különböző nézőpontból.
0.5⟶0.6: Tekintsük először a 0.5 Tételbeli szituációt. Könnyű ellenőrizni, hogy az L testben az $\{\overline{a}\colon a \in K\}$ halmaz egy K-val izomorf résztestet alkot. Azonosítsuk ezt magával a K testtel, vagyis hagyjuk el a felülvonásokat a K-beli elemekről (de csak azokról!). Így K részteste lesz L-nek, azaz egy $L|K$ testbővítést kapunk. Ennek elemei egyértelműen előállnak

$$\begin{aligned}\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} &= \overline{a_{n-1}x^{n-1}} + \cdots + \overline{a_1 x} + \overline{a_0} = \\ &= a_{n-1}\overline{x}^{n-1} + \cdots + a_1\overline{x} + a_0 \quad (a_{n-1}, \ldots, a_0 \in K)\end{aligned}$$

alakban. Ebből látszik, hogy K elemei és az $\overline{x}$ elem együtt generálják az L testet (ráadásul a generálásnál a négy alapműveletből csak az első háromra van szükségünk). Vagyis az $\alpha := \overline{x}$ jelölést bevezetve azt kapjuk, hogy $L = K(\alpha)$. Hátravan még annak megmutatása, hogy α algebrai K felett. Ehhez számoljuk ki az $f \in L[x]$ polinom ($K \subseteq L$ miatt f tekinthető L feletti polinomnak!) $\alpha \in L$ helyen felvett helyettesítési értékét. Legyen $f = b_n x^n + \cdots + b_1 x + b_0$, ekkor

$$\begin{aligned} f(\alpha) &= b_n \alpha^n + \cdots + b_1 \alpha + b_0 = \overline{b_n}\,\overline{x}^n + \cdots + \overline{b_1}\,\overline{x} + \overline{b_0} = \\ &= \overline{b_n x^n + \cdots + b_1 x + b_0} = \overline{f} = \overline{0} = 0. \end{aligned}$$

Tehát α gyöke f-nek, így α algebrai K felett és $L = K(\alpha)$ egyszerű algebrai bővítés. Továbbá a 0.4. Tétel szerint f asszociált $m_{\alpha,K}$-hoz (mert f irreducibilis K felett).

0.6⟶0.5: Induljunk most ki a 0.6. Tételben vázolt szituációból, és tekintsük a $\varphi\colon K[x] \to L$, $p \mapsto p(\alpha)$ gyűrűhomomorfizmust, ami minden $p \in K[x]$ polinomhoz annak α helyen felvett értékét rendeli (ellenőrizzük, hogy ez valóban gyűrűhomomorfizmus!). A 0.6. Tételből következik, hogy φ szürjektív, és így a 0.2. Tétel (gyűrűelméleti homomorfiatétel) szerint $L \cong K[x] / \ker \varphi$. Test feletti polinomgyűrű mindig főideálgyűrű, ezért létezik olyan $f \in K[x]$ főpolinom, amelyre $\ker \varphi = (f)$. A $K[x] / (f)$ faktorgyűrű test (hiszen izomorf az L testtel), tehát a 0.3. Tétel szerint f irreducibilis K felett. Nyilván $f \in \ker \varphi \implies f(\alpha) = 0$, és így a 0.4. Tétel mutatja, hogy $m_{\alpha,K} = f$. Összefoglalva, azt kaptuk, hogy az $L = K(\alpha)$ test izomorf a $K[x]$ polinomgyűrű (f) főideál szerinti faktortestével, ahol f az α elem K feletti minimálpolinomja. Az izomorfizmust konkrétan is felírhatjuk (gondoljuk meg, hogy miért jóldefiniált ez a ψ leképezés):

$$\psi\colon K[x] / (f) \to K(\alpha), \ \overline{p} \mapsto p(\alpha).$$

(Itt a modulo f maradékosztályokat megint felülvonással jelöltük.) Figyeljük meg, hogy $\psi(\overline{a}) = a$ minden $a \in K$ esetén, valamint $\psi(\overline{x}) = \alpha$. Mivel az $\{\overline{a}\colon a \in K\}$ halmaz és az $\overline{x}$ elem együtt generálja a $K[x] / (f)$ testet, az utóbbi két tulajdonság egyértelműen meghatározza a ψ izomorfizmust.

A 0.5. és 0.6. Tételek csak a testek elemeit írják le, azt nem, hogy hogyan kell számolni ezekkel az elemekkel. A számolás gyakoroltatására hivatott a következő két feladat.

10. feladat: Adja meg a $\mathbb{Q}(\alpha)$ test u, v, w elemeit „kanonikus” alakban, ahol $\alpha = \sqrt[3]{2}$, és

$$u = \left(1 + \alpha + \alpha^2\right)\left(2 - \alpha^2\right), \ v = \alpha^{-1}, \ w = \left(1 + \alpha + \alpha^2\right)^{-1}.$$

11. feladat: Adja meg a $\mathbb{Q}(\alpha)$ test u, v, w elemeit „kanonikus” alakban, ahol α gyöke az $x^3 - 2x + 2$ polinomnak, és

$$u = \alpha^7, \ v = \alpha^{-1}, \ w = \alpha^4 + \alpha^{-2}.$$

12. feladat: Határozza meg az alábbi komplex számok minimálpolinomját $\mathbb{C}$, $\mathbb{R}$ és $\mathbb{Q}$ felett:

$$\alpha_1 = \sqrt{3 - \sqrt{6}}, \ \alpha_2 = 2 + i, \ \alpha_3 = i\sqrt[3]{3}.$$