TRNAVSKÁ UNIVERZITA
PEDAGOGICKÁ FAKULTA

ÚVOD DO ŠTÚDIA GALOISOVEJ TEÓRIE

Milan Paštéka

Recenzovali:
Prof. RNDr. Štefan Porubský, DrSc.
Prof. RNDr. Jozef Širáň, DrSc.

ISBN 978-80-568-0206-9 EAN 9788056802069

1 Úvod

Úvod. Tento text si kladie za cieľ sprostredkovať čitateľovi niektoré základné poznatky o riešení polynomických rovníc. Sú to rovnice tvaru

$$f(x) = a_n x^n + \cdots + a_0 = 0, \tag{1}$$

kde $a_n, \ldots, a_0$ sú prvkami nejakého poľa F. Vieme, že takáto rovnica má vždy korene v nejakom nadpoli poľa F. Otázka je ako tieto korene nájsť , alebo presnejšie povedané vypočítať. Vzorec na výpočet koreňov kvadratickej rovnice je všeobecne známy a nepoznáme jeho objaviteľa. Pravdepodobne ich je viac, nezávislých na sebe. S istou mierou poézie sa hovorí , že tento vzorec je súčasťou matematického folklóru. Až v 16. storočí boli objavené formule na výpočet koreňov kubickej rovnice. Najznámejšia sa volá Cardanov vzorec. Jeho objavenie sa pripisuje matematikovi menom Tartaglia, ktorý ho údajne predal Jeromovi Cardanovi. Šestnáste storočie bolo obdobím súbojov. Mimo iných sa odohrávali aj matematické súboje. Súperi si zadávali úlohy. Každý mohol zadať iba takú úlohu, ktorú vedel sám riešiť. Traduje sa, že Cardano zaviazal Tartagliu mlčanlivosťou a to mu umožnilo víťaziť pomocou kubických rovníc. Výhodou matematických súbojov bolo tiež to, že pri nich neboli mŕtvi.

Trochu neskôr Cardanov žiak Ferarri objavil formulu pre korene polynómu 4. stupna. Úpravami previedol tento problém na kvadratickú a kubickú rovnicu. Samozrejme nasledovali snahy na objavenie metódy výpočtu koreňov rovnice piateho stupňa. Tieto však boli dlhodobo neúspešné. Jeden zo spôsobov pri tomto výskume spočíval vo využití tzv. Vietovych vzorcov. To sú formule, ktoré vyjadrujú koeficienty daného polynómu pomocou jeho koreňov. Teda v našom prípade vyjadrujú známe veličiny pomocou neznámych. Cieľom bolo rôznymi úpravami dosiahnuť opak : vypočítať nezmáme pomocou známych. Ako sme už spomínali nepodarilo sa. Napriek tomu táto práca prínos mala. Vietove vzorce sú symetrické, to znamená že sa nemenia pri prehadzovaní poradia koreňov, ináč povedané pri permutáciach. To viedlo k objaveniu grúp permutácií . Začiatkom 19. storočia objavili nezávisle na sebe nór Niels Henrik Abel a francúz Evariste Galois metódu pomocou ktorej priradili danej polynomickej rovnici istú grupu permutácií , ktorá sa dnes nazýva Galoisova grupa tejto rovnice. Rovnice ktoré sa dajú riešit pomocou vzorcov ktoré obsahujú odmocniny majú túto grupu pomerne jednoduchú. Rovnice, ktorých grupa je zložitá sa pomocou odmocnín riešiť nedajú. Okrem iného to aj objasňuje prečo vyššie uvedený výskum nepriniesol očakávané výsledky.

Evariste Galois nemal štastný osud. Narodil sa 1811, koncom napoleonských vojen , zomrel 1832 ako dvadsaťro-

čný - pri súboji. Nepodarilo sa mu ani zoznámiť ma- tematikov tej doby so svojimi výsledkami. Okrem iného to bolo aj dôsledkom nestabilnej situácie vo vojnami zbedačeného Francúzska.

O trochu vačšie sťastie mal Niels Henrik Abel (1802-1829), podarilo sa mu nadviazať kontakty s inými učencami svojej doby. Aj on však zomrel mladý. Dostal zápal pľúc - vtedy neexistovali antibiotiká a ústredné kúrenie bolo veľmi zriedkavé. Komutatívne grupy sa na jeho počesť nazývajú aj Abelove grupy.

Na začiatku si pripomenieme niektoré o polynómoch. Budeme študovať rozšírenia polí o korene polynómov a ich galoisove grupy. Ukážeme ako súvisia s rozšíreniami o korene binomických rovníc. Bude nás zaujímať hla- vne to či sú komtatívne resp. cyklické. Dokážeme o istej množine poly- nómov, že ich korene sa nedajú vyjadriť pomocou odmocnín. Medzi také polynómy patrí aj polynóm $x^5 - 10x - 5$.

Jednoduchším probémom je otázka euklidovských geometrických konštrukcií , pravítkom a kružidlom, ktorú už dobre poznáme - postupná adjunkcia druhých odmocnín.

Galoisova teória dnes patrí medzi veľmi rozvinuté časti algebry so širokými aplikáciami napríklad v informatike.

Text sa snažíme viesť čo najskôr ku Galoisovym gru-

pám. V časť doplnky sú niektoré dolpňujúce poznatky. Pre úplnosť je na začiatku doplnkov uvedená Zornova lema a dôkaz jej ekvivalencie s Axiomou výberu.

Chcel by som poprosiť prípadných čitateľov o zhovievavosť k jazykovej úrovni textu. Spôsob jeho prípravy a vydania neumožnil urobiť dôkladnú jazykovú korektúru.

Touto cestou by som chcel poďakovať recenzentom za podporu a veľmi cenné pripomienky k textu. Rovnako vyjadrujem vďaku aj pani RNDr. Zuzane Václavíkovej, PhD. z Ostravskej Univerzity za predbežné prečítanie taextu a jej pripomienky.

Označenia. Budeme označovať $\mathbb{C}$ - množina komplexných čísel, $\mathbb{R}$ - množina reálnych čísel, $\mathbb{Q}$ - množina racionálnych čísel, $\mathbb{Z}$ - množina celých čísel, $\mathbb{N}$ množina prirodzených čísel, $F[x]$ okruh polynómov neurčitej x nad poľom F, $\mathbb{Z}[x]$ množina polynómov s celočíselnými koeficientami, $\mathbb{Z}_m$ - množina zvyškových tried modulo m, $\mathbb{Z}_m^*$ - množina zvyškových tried modulo m, ktoré sú nesúdeliteľné s m, $\mathbf{S}_n$ bude označovať množinu všetkých permutácií množiny $\{1, \ldots, n\}$. Symbol $[M]$ bude označovať najmenšiu podgrupu danej grupy obsahujúcu množinu M. Ďalej budeme označovať zjednodušene $[\{a_1, \ldots, a_j\}] =$
$= [a_1, \ldots, a_j]$. Ak S je konečná množina tak symbol $|S|$ bude znamenať počet jej prvkov. Niekedy sa táto hodnota označuje aj $\mathbf{c}ard(S)$. My však s priestových dôvodov tento symbol používať nebudeme. Z kontextu bude vždy jasné, že ide o množinu a teda sa to nebude mýliť s absolútnou hodnotou čísla. Ak a je kladné reálne číslo tam symbolom $\sqrt[n]{a}$ budeme označovať kladný koreň polynómu $x^n - a$, teda hodnotu ktorá má tiež oznečenie $a^{\frac{1}{n}}$, pre $n \in \mathbb{N}$. Ak a ľubovoľný iný tak $\sqrt[n]{a}$ bude jeden ale v danom kontexte pevne daný koreň polynómu $x^n - a$.

1.1 Základné pojmy

Stručne pripomenieme definície a vlastnosti algebrických štruktúr ktoré budeme používať.

Usporiadaná dvojica $(G, \circ)$ sa nazýva **grupa** ak G je množina a $\circ$ je asociatívna binárna operácia na G, ktorá má neutrálny prvok a ku každému prvku G existuje inverzný prvok. Neutrálny prvok zvykneme označovať e. Ak G je grupa bijekcií na nejakej množine tak neutrálny prvok, teda identické zobrazenie, označujeme id. Ak používame aditívnu symboliku, teda $(G, +)$, neutrálny prvok nazývame aj **nulový prvok** a označujeme ho ako obvykle 0. [1]

Usporiadanú trojicu $(R, +, \cdot)$ na nazývame **komutatívny okruh s jednotkou** ak $(R, +)$ je komutatívna grupa, operácia $\cdot$ je asociatívna a komutatívna na R, má neutrálny prvok a

$$a(b + c) = ac + bc$$

pre všetky $a, b, c \in R$.

Neutrálny prvok operácie $\cdot$ sa v tomto prípade zvykne označovať 1, nazývame ho aj **jednotkový prvok**.

Komutatívny okruh s jednotkou R sa nazývam **obor**

[1] Pojem grupy vznikal postupne pri štúdiu množín permtácií koreňov polynómov. V roku 1900 pravdepodobne James de Pierpoint definoval grupu ako množinu s operáciou ktorá spĺňa tri aximomy - tak ako ju poznáme dnes. De Pierpoit pochadzal z USA, narodil sa v 16. júna 1866 v štáre Connecticut. Matematiku študoval v Európe, v Berlíne a vo Viedni. Tam aj získal doktorát. Neskôr pôsobil v USA na univerzite Yale. Zomrel 9. decembra 1938.

integrity práve vtedy keď

$$ab = 0 \iff a = 0 \vee b = 0$$

pre každé $a, b \in R$.

Usporiadané trojica $(F, +, \cdot)$ sa nazýva **pole** ak je to komutatívny okruh s jednotkou a $(F \setminus \{0\}, \cdot)$ je grupa. V tomto prípade $(F, +)$ sa nazýva aditívna grupa poľa F a $(F \setminus \{0\}, \cdot)$ sa nazýva multiplikatívna grupa poľa F.

Okruh polynómov jednej alebo viacerých neurčitých nad poľlom F je príkladom oboru integrity. Príkladom poľa je napríklad množina racionálnych čísel, reálnych čísel a komplexných čísel.

Hovoríme, že pole F má **konečnú charakteristiku** práve vtedy ak existuje $n \in \mathbb{N}$ také, že

$$n \times 1 := 1 + \cdots + 1 = 0$$

kde 1 sa sčíta n krát. Najmenšie také n sa nazýva charakteristikou poľa F. Ľahko sa ukáže, že $(n_1 \times 1)(n_2 \times 1) = n_1 n_2 \times 1$. Z minimality charakteristiky potom vyplýva

Veta 1. Ak má pole konečnú charakteristiku tak jeho charakteristika je prvočíslo.

Veta 2. Pole charakteristiky p obsahuje podpole izomorfné s poľom $\mathbb{Z}_p$, kde p je ľubovoľné prvočíslo.

Dôkaz. Je to podpole $\{0, 1, 2 \times 1, \ldots, (p-1) \times 1\}$. $\square$

Ak $(V, +)$ je komutatívna grupa a F je pole hovoríme, že V je **vektorový priestor** nad F ak existuje operácia $\cdot : F \times V \to V$ ktorá spľňa nasledujúce podmienky:
1) $1 \cdot v = v$ pre $v \in V$,
2)$(ab)v = a \cdot (b \cdot v)$ pre $v \in V, a, b \in F$,
3) $(a + b) \cdot v = a \cdot v + b \cdot v$ pre $v \in V, a, b \in F$ a
4) $a \cdot (v_1 + v_2) = a \cdot v_1 + a \cdot v_2$ pre $a \in F, v_1, v_2 \in V$.

Prvky množiny V budeme nazývať **vektory** aj keď nemusia mať geometrický význam. Pre stručnosť budeme namiesto $a \cdot v$ písať iba av. Ak
$v_1, \ldots, v_n \in V$ a $a_1, \ldots, a_n \in F$ tak vektor

$$v = a_1 v_1 + \cdots + a_n v_n$$

budeme nazývať **lineárnou kombináciou** vektorov $v_1, \ldots, v_n$. Symbolom $\mathcal{L}(v_1, \ldots, v_n)$ budeme označovať množinu všetkých lineárnych kombinácií vektorov $v_1, \ldots, v_n$. Je zrejmé, že aj táto množina tvorí vektorový priestor nad F. Hovoríme tiež, že tento priestor je **generovaný** vektormi $v_1, \ldots, v_n$.

Vektorový priestor V sa nazýva **konečnorozmerný** ak existuije taká konečná postupnosť $v_1, \ldots, v_n \in V$, že $V = \mathcal{L}(v_1, \ldots, v_n)$. V takomto príp- ade sa postupnosť s najmenším počtom vektorov, ktoré generujú vektorový priestor V nazýva **báza** tohoto priestoru. Počet jej prvkov nazývame **dimenziou** V, označuje sa ako $dimV$.

Vektory $v_1, \ldots, v_n$ sa nazývajú **lineárne nezávislé** práve vtedy, keď platí

$$a_1 v_1 + \cdots + a_n v_n = 0 \Longleftrightarrow a_1 = 0, \ldots, a_n = 0. \quad (2)$$

Veta 3. Ak vektory $v_1, \ldots, v_n$ sú bázou V tak sú lineárne nezávislé.

Dôkaz. Ak by v rovnosti (2) platilo napríklad $a_n \neq 0$ tak vektor v_n by sa dal vyjadriť ako lineárna kombinácia $v_1, \ldots, v_{n-1}$ a z toho by sme po jednoduchých úpravách dostali $V = \mathcal{L}(v_1, \ldots, v_{n-1})$ a to je spor s minimalitou n. □

Veta 4. Ak vektory $v_1, \ldots, v_n$ sú bázou V tak každý vektor z V sa dá vyjadriť jediným spôsobom ako ich lineárna kombinácia.

Rovnako sa dá dokázať : Ak $v_1, \ldots, v_n$ vektory tvoria bázu V a $v = a_1 v_1 + \cdots + a_n v_n$ a $a_1 \neq 0$ tak aj vektory $v, v_2, \ldots, v_n$ tvoria bázu V. Pomocou toho faktu sa dá odvodiť

Veta 5. Postupnosť lineárne nezávislých vektorov vektorového priestoru dimenzie n nemôže obsahovať viac ako n prvkov. Ak takáto postupnosť má n prvkov tak tvorí bázu daného vektorového priestoru.

1.2 Konečné polia

Dôležitú úlohu hrajú konečné polia. Medzi ne patria tiež polia zvyškových tried modulo prvočíslo. Konečné pole má konečnú charakteristiku. Ak p je charakteristika daného poľa tak podľa vety 2 obsahuje podpole izomorfné s poľom $\mathbb{Z}_p$. Ked si uvedomíme, že každé pole je vektorový priestor nad svojím podpoľom dostávame podľa vety 4

Veta 6. Konečné pole má p^k prvkov, kde p je jeho charakteristika a k je vhodné prirodzené číslo.

Dokážeme jednu významnú vlastnosť konečných polí . V Doplnkoch sa nachádza definícia pojmu cyklickej grupy, ktorý budeme študovať .

Veta 7. Multiplikatívna grupa konečného poľa je cyklická.

V dodatkoch je tiež pripomenutý rád prvku v grupe. Dôkaz vety 7 začneme nasledovným tvrdením:

Veta 8. Nech F je konečné pole a $|F|-1 = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ je kanonický rozklad. Potom pre každé $j = 1, \dots, s$ existuje v $F \setminus \{0\}$ prvok rádu $p_j^{\alpha_j}$.

Dôkaz. Nech j je pevne dané. Uvažujme množinu M všetkých prvkov tvaru

$$a^{\frac{|F|-1}{p_j^{\alpha_j}}}, \ a \in F \setminus \{0\}.$$

Je zrejmé, že pre každé $b \in M$ platí

$$b^{p_j^{\alpha_j}} = 1.$$

Preto rády prvkov z tejto množiny sú p_j^ℓ kde $\ell \leq \alpha_j$. Ak by ani jeden z jej prvkov nemal rád rovný $p_j^{\alpha_j}$ tak pre každý prvok $b \in M$ platí

$$b^{p_j^{\alpha_j - 1}} = 1.$$

To znamená, že pre každý prvok $a \in F \setminus \{0\}$ plati

$$a^{\frac{|F|-1}{p_j}} = 1.$$

Teda polynóm $x^{\frac{|F|-1}{p_j}} - 1$ by mal $|F| - 1$ koreňov a teda viac koreňov ako je jeho stupeň, tým sme dostali spor. □

Veta 9. Nech G je grupa a $a, b \in G$ sú také prvky, že $ab = ba$. Ak rád prvku a je m_1 a rád prvku b je m_2 a $(m_1, m_2) = 1$ tak rád prvku ab je $m_1 m_2$.

Dôkaz. Určite platí

$$(ab)^{m_1 m_2} = e$$

a teda ak m je rád prvku ab tak $m | m_1 m_2$. Ukážeme, že to platí aj opačne. Z definície m dostávame

$$a^m b^m = e$$

a teda

$$e = (a^m b^m)^{m_1} = a^{mm_1} b^{mm_1} = b^{mm_1}.$$

Preto $m_2 | mm_1$ a z podmienky $(m_1, m_2) = 1$ dostávame $m_2 | m$. Rovnako sa dokáže $m_1 | m$. □

Dôkaz vety 7. Nech $|F| - 1 = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. Označme a_j prvok rádu $p_j^{\alpha_j}$. Podľa vety 9 prvok

$$a = a_1 \dots a_s$$

má rád $|F| - 1$ a teda generuje celú grupu $F \setminus \{0\}$. □

2 Rozšírenia polí

2.1 Algebrické prvky

Nech F je pole a E je jeho nadpole. Prvok $\alpha \in E$ za nazýva **algebrický** nad F práve vtedy ak je koreňom nejakého polynómu z $F[x]$ stupňa aspoň 1. V takom prípade normovaný polynóm $f(x) \in F[x]$ najnižšieho stupňa taký, že $f(\alpha) = 0$ sa nazýva **minimálny polynóm** prvku α. Prvok E ktorý nie je algebricý nad F sa nazýva **transcendentný** nad F. Komplexné čísla ktoré sú algebrické nad poľom racionálnych čísel sa nazývajú **algebrické čísla**. Tie ktoré

sú transcendetné nad poľom $\mathbb{Q}$ sa nazývajú **transcendetné čísla**. [2]

Veta 10. Ak α je algebrický prvok na pobm F a $f(x)$ je jeho minimálny polynóm, tak pre kazdý polynóm $g(x) \in F[x]$ platí

$$g(\alpha) = 0 \Longleftrightarrow f(x)|g(x).$$

Dôkaz. Jedna implikácia je zrejmá na prvý pohľad. Nech $g(\alpha) = 0$. Polynóm $g(x)$ môžeme deliť so zvyškom a dostávame

$$g(x) = f(x)q(x) + r(x)$$

kde stupeň $r(x)$ je menší ako stupeň $f(x)$. Po dosadení do poslednej rovnosti dostávame $r(\alpha) = 0$. Ak by $r(x)$ bol nekonštantný polýnóm dostali by sme spor s minimalitou stupňa $f(x)$. Teda $r(x)$ je konštantný polynóm preto $r(x) = 0$. □

Veta 11. Ak α je algebrický prvok nad poľom F tak normovaný polynóm $f(x) \in F[x]$ je minimálny polynóm α práve vtedy ak $f(x)$ je polynóm ireducibilný nad poľom F a $f(\alpha) = 0$.

[2] Otázkam transcendentnosti čísel sa venuje veľká časť výkumu. Je dokázané, že čísla π a e sú transcendentné. V roku 1934 Theodor Schneider a Alexander Geľfond dokázali nezávisle na sebe, že v prípade keď $a \neq 0, 1$ je algebrické číslo a b je iracionálne číslo tak a^b je transcendentné číslo.

Dôkaz. Ak $f(x) = f_1(x)f_2(x)$ a $f(\alpha) = 0$, tak $f_1(\alpha) = 0$ alebo $f_2(\alpha) = 0$. Teda ak $f(x)$ je minimálny polynóm α tak z minimality stupňa $f(x)$ vyplýva že obidva polynómy $f_1(x)$, $f_2(x)$ nemôžu mať stupeň menší ako $f(x)$. Teda $f(x)$ nemá vlastné delitele a teda je ireducibilný.

Nech $f(x)$ ireducibilný a $f(\alpha) = 0$. Ak $f_0(x)$ je minimálny polynóm prvku α tak z vety 10 vyplýva, že $f_0(x)|f(x)$. Preto $f(x) = cf_0(x)$, teda aj $f(x)$ je minimálny polynóm prvku α. □

Príklad 1. Minimálny polynóm $\sqrt{2}$ nad poľom $\mathbb{Q}$ je x^2-2.

2.2 Separabilné polynómy

Polynóm patriaci do $F[x]$ sa nazýva **separabilný** práve vtedy ak v žiadnom nadpoli nemá násobné korene.

Príklad 2. Polynóm x^2+1 je separabilný. Polynóm $(x^2+1)^2$ separabilný nie je, pretože má v $\mathbb{C}$ dvojnásobné korene $i, -i$.

Veta 12. Ak ireducibilný polynóm z $F[x]$ má nenulovú formálnu deriváciu tak je separabilný. [3]

[3] Ak $a(x) = a_n x^n + \cdots + a_0$ tak symbolom $a'(x)$ označujeme tzv. formálnu deriváciu polynómu $a(x)$ kde

$$a'(x) = na_n x^{n-1} + \cdots + a_1.$$

Dôkaz. Ak $f(x) \in F[x]$ je ireducibilný polynóm a jeho derivácia je nenulový polynóm tak sú nesúdeliteľné. Teda existujú polynómy $h_1(x), h_2(x) \in \mathbb{Q}[x]$ také, že

$$1 = h_1(x)f(x) + h_2(x)f'(x). \tag{3}$$

Ak by mal $f(x)$ v nejakom nadpoli násobný koreň tak

$$f(x) = (x - \alpha)^2 f_1(x)$$

a teda

$$f'(x) = 2(x - \alpha)f_1(x) + (x - \alpha)f_1'(x).$$

Ak by sme α dosadili do (3) dostali by sne $1 = 0$ a to je spor. □

2.3 Rozšírenie poľa, Galoisova grupa.

Ak $F \subset E$ sú polia, hovoríme , že pole E je rozšírením poľa F. V takom prípade sa izomorfizmus $\varphi : E \to E$ spĺňajúci podmienku $\varphi(a) = a$ pre každé $a \in F$ nazýva F -**automorfizmus poľa** E. Množinu všetkých F - automorfizmov budeme označovať $G(E : F)$. Je zrejmé že

Ako vidíme ide o rozšírenie derivácie tak ako ju poznáme z diferencialneho počtu na polynómy nad ľubovoľým poľom. Úpravami sa dá preveriť, že súčet a súčin sa derivuje štandartným spôsobom.

táto množina tvorí grupu vzhľadom na operáciu skladania zobrazení . Budeme ju nazývať **Galoisova grupa** poľa E nad poľom F. Istý význam tohto pojmu pre štúdium koreňov polynómov je vidieť z nasledujúceho jednoduchého faktu:

Veta 13. Nech $f(x) \in F[x]$ **a** $\varphi \in G(E : F)$**. Potom pre každé** $b \in E$ **platí**

$$f(b) = 0 \Longleftrightarrow f(\varphi(b)).$$

Dôkaz. Ak $f(x) = a_n x^n + \cdots + a_0$ tak pre $b \in E$ máme

$$\varphi(f(b)) = \varphi(a_n b^n + \cdots + a_0) =$$

$$= \varphi(a_n)\varphi(b^n) + \cdots + \varphi(a_0) = a_n\varphi(b^n) + \cdots + a_0$$

$$f(\varphi(b)).$$

Pretože $\varphi(f(b)) = 0$ práve vtedy keď $f(b) = 0$ dostáveme tvrdenie. □

Príklad 3. Ak uvažujeme $\mathbb{R}$ pole reálnych čísel a jeho nadpole $\mathbb{C}$ komplexných čísel, tak veľmi známym príkladom $\mathbb{R}$ automorfizmu je zobrazenie $z \to \overline{z}$, komplexnému číslu sa priradí komplexne združené. Aký bude minimálný polynóm čísla $1 + 2i$ nad $\mathbb{R}$? Koreňom takého polynómu musí byť aj $1 - 2i$ a teda to je polynóm

$$(x - (1 + 2i))(x - (1 - 2i)) = x^2 - 2x + 5.$$

Príklad 4. Uvažujme pole $\mathbb{Q}(\sqrt{2})$. Ak $\varphi \in G(\mathbb{Q}(\sqrt{(}2) : Q)$ tak $\varphi(a + b\sqrt{2}) = a + b\varphi(\sqrt{2})$. Je zrejme, že $(\varphi(\sqrt{2}))^2 = \varphi(2) = 2$. Teda $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Teda grupa $G(\mathbb{Q}(\sqrt{(}2) : Q)$ obsahuje iba dva prvky $\varphi_0 = id$ a φ_1 kde $\varphi_1(a+\sqrt{2}) = a - b\sqrt{2}$. Z toho vidiet, že táto grupa je izomorfná s aditivnou grupou $\mathbb{Z}_2$.

Hovoríme, že pole E je konečné rozšírenie poľa F práve vtedy keď E je konečnorozmerný vektorový priestor nad F. V tomto prípade dimenziu E nad F označujeme $[E : F]$ a táto hodnota sa nazýva **stupeň rozšíenia** E nad F.

Ak $\alpha \in E$, tak symbolom $F(\alpha)$ budeme označovať najmenšie podpole poľa E, ktoré obsahuje F aj α. Je to teda množina, ktorá obsahuje práve všetky súčiny, súčty, podiely s nenulovým menovateľom prvkov množiny $F \cup \{\alpha\}$. Hovoríme tiež, ž k polu F sme **adjungovali** prvok α. Ak $\beta \in E$ tak označujeme $F(\alpha)(\beta) := F(\alpha, \beta)$.

Príklad 5. Pole $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ obsahuje prvok $\sqrt{3}+\sqrt{2}$. Teda $\mathbb{Q}(\sqrt{3} + \sqrt{2}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{2})$. Pole $\mathbb{Q}(\sqrt{3} + \sqrt{2})$ obsahuje aj prvok $\frac{1}{\sqrt{3}+\sqrt{2}} = \sqrt{3} - \sqrt{2}$. Sčítanía odčítaním dostávame $\sqrt{3}, \sqrt{2} \in \mathbb{Q}(\sqrt{3}+\sqrt{2})$. To znamená $\mathbb{Q}(\sqrt{3}, \sqrt{2}) \subset \mathbb{Q}(\sqrt{3}+\sqrt{2})$. Teda $\mathbb{Q}(\sqrt{3} + \sqrt{2}) = \mathbb{Q}(\sqrt{3}, \sqrt{2})$.

Príklad 6. Ak uvažujeme galoisovu grupu $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : Q)$ tak vidíme, že pre každý jej prvok φ platí $(\varphi(\sqrt{2}))^2 = 2, (\varphi(\sqrt{3}))^2 = 3$. Táto grupa má preto štyri prvky $\varphi_0 = id$,

φ_1, kde $\varphi_1(\sqrt{2}) = -\sqrt{2}$ $\varphi_1(\sqrt{3}) = \sqrt{3}$, φ_2, kde $\varphi_2(\sqrt{2}) = \sqrt{2}$ $\varphi_2(\sqrt{3}) = -\sqrt{3}$ a φ_3, kde $\varphi_3(\sqrt{2}) = -\sqrt{2}$ $\varphi_3(\sqrt{3}) = -\sqrt{3}$. Teda táto grupa je izomorfná s $Z_2 \times Z_2$.

Príklad 7. Môžeme sa opýtať aký bude minimálny polynóm čísla $\sqrt{2}+\sqrt{3}$ z predošlého príkladu. Koreňom tohoto polyńomu musia byť všetky hodnoty $\varphi_j(\sqrt{2} + \sqrt{3}), j = 0, 1, 2, 3$. Dostávame takto, že je to polynóm

$$(x - (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))\cdot$$
$$\cdot(x - (-\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3})) =$$
$$= x^4 - 10x^2 + 1.$$

Polynóm ktorý má štyri korene musí byť aspoň štvrtého stupňa. Z toho vyplýva, že daný polynóm je minimálny polynóm prvku $\sqrt{2} + \sqrt{3}$.

Veta 14. Nech $f(x) \in F[x]$ je ireducibilný polynóm stupňa $m \geq 1$ a $\alpha \in E$ je jeho koreň.
i) Prvky $1, \alpha, \ldots, \alpha^{m-1}$ sú lineárne nezávisé nad poľom F.
ii) $F(\alpha)$ je vektorový priestor nad F s bázou $1, \alpha, \ldots, \alpha^{m-1}$.
iii) V takom prípade platí $[F(\alpha) : F] = m$.

Dôkaz. Polynóm $f(x)$ je minimálnym polynómom prvku α preto tento prvok nemôže byť koreňom polynómu nižšieho stupňa. Z toho vyplýva i).

Označme V vektorový priestor generovaný prvkami $1, \alpha, \ldots, \alpha^{m-1}$ nad poľom F. Je zrejmé že $V \subset F(\alpha)$. Na to aby sme dokázali opačnú inklúziu stačí dokázať , že V je pole, teda že s každými dvomi prvkami obsahuje ich súčin a s každým nenulovým prvkom osahuje aj jeho inverzný prvok. Ak $a, b \in V$ tak $a = g_1(\alpha), b = g_2(\alpha)$ pre nejaké $g_1(x), g_2(x) \in F(x)$. Potom $g_1(x)g_2(x) = q(x)f(x) + r(x)$ kde $q(x), r(x) \in F[x]$ a stupeň $r(x)$ je menší ako m. Preto $ab = r(\alpha) \in V$. Ak $a \neq 0$ tak $g_1(x)$ je nenulový polynóm. Z ireducibility vyplýva že $f(x)$ a $g_1(x)$ sú nesúdeliteľné polynómy a teda existujú polynómy $g_3(x), g_4(x), g_5(x)$ také že stupeň $g_3(x)$ je menší ako m a

$$1 = g_1(x)g_3(x) + g_4(x)f(x),$$

a teda $ag_3(\alpha) = 1$.

Bod iii) vyplýva automaticky z toho že $F(\alpha)$ má m prvkovú bázu. □

Príklad 8. Polynóm $x^3 - 2$ je ireducibilný nad $\mathbb{Q}$. Preto $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$,

Príklad 9. Aká je galoisova grupa $G(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$? Nech $\varphi \in G(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$. Potom $\varphi(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\varphi(\sqrt[3]{2}) + c(\varphi(\sqrt[3]{2})^2)$. Prvok $\varphi(\sqrt[3]{2})$ patrí do poľa $\mathbb{Q}(\sqrt[3]{2})$. Polynóm $x^3 - 2$ má dva korene komplexné a jeden reálny. Toto pole obsahuje iba ten reálny a teda $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$.

Preto grupa $G(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ má jediný prvok a to identické zobrazenie.

Príklad 10. Číslo

$$\frac{1}{(\sqrt[3]{2})^2 + \sqrt[3]{2} + 1}$$

je prvkom poľa $\mathbb{Q}(\sqrt[3]{2})$. Môžeme ho upraviť tak aby odmocniny neboli v menovateli. Vyjadríme ho v tvare

$$\frac{1}{(\sqrt[3]{2})^2 + \sqrt[3]{2} + 1} = A(\sqrt[3]{2})^2 + B\sqrt[3]{2} + C$$

a po vynásobení dostaneme lineárne rovnice pre A, B, C. Táto úprava sa nazýva usmerňovanie zlomkov.

Veta 15. Ak E je konečné rozšírenia poľa F a H je konečné rozšírenie poľa E tak H je konečné rozšírenie poľa F a platí

$$[H : F] = [H : E] \cdot [E : F].$$

Dôkaz. Ak prvky $\alpha_1, \ldots, \alpha_j$ tvoria bázu E nad F a $\beta_1, \ldots, \beta_k$ tvoria bázu H nad E tak prvky

$$\alpha_1\beta_1, \ldots, \alpha_1\beta_k, \alpha_2\beta_1, \ldots, \alpha_2\beta_k, \ldots$$

tvoria bázu H nad F. □

Príklad 11. Podľa príkladu 8 vidíme, že $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$ lebo v takom prípade by $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[3]{2})$ a teda $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ to je spor pretože $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ a 2 nie je deliteľom 3.

Príklad 12. Je zrejmé, že $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Teda polynóm $x^2 - 3$ je ireducibilný nad $\mathbb{Q}(\sqrt{2})$. Teda $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Príklad 13. Ukážeme, že $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. V opačnom prípade by $\sqrt{5} = A + B\sqrt{3}$ kde $A, B \in \mathbb{Q}(\sqrt{2})$, teda $5 = A^2 + 3B^2 + 2AB\sqrt{3}$. Je zrejmé, že $A \neq 0, B \neq 0$. Preto $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ - spor. Teda $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$. Podobne ako v príklade 6 sa dá dokázať, že galoisova grupa $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q})$ je izomorfná s $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Matematickou indukciou sa dá dokázať , že pre rôzne prvočísla $p_1, \ldots,$
p_k platí :

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k. \tag{4}$$

Príklad 14. Môže patriť koreň polynómu $x^3 + x + 1$ do poľa $\mathbb{Q}(\sqrt{2}, \sqrt{3})$?

Z dôkazu vety 15 hneď dostávame:

Veta 16. Ak F je pole a $\alpha_1, \ldots, \alpha_n$ sá prvky algebrické nad F, tak každý prvok poľa $F(\alpha_1, \ldots, \alpha_n)$ sa dá vyjadriť v tvare $r(\alpha_1, \ldots, \alpha_n)$ kde $r(x_1, \ldots, x_n)$ je polynóm n neurčitých nad F.

Veta 17. Ak $F \subset E$ sú polia tak množina všetkých prvkov E, ktoré sú algebrické nad F tvorí pole.

Dôkaz. Označme symbolom F' množinu všetkých prvkov E, ktoré sú algebrické nad F. Ak $\alpha \in F'$ tak $\alpha \in F(\alpha)$. Ak $\alpha \neq 0$ tak $\frac{1}{\alpha} \in F(\alpha)$. Ale $F(\alpha)$ konečno rozmerný vektorový priestor nad F a teda musí existovať $n \in \mathbb{N}$ také, že prvky $1, \frac{1}{\alpha}, \ldots, (\frac{1}{\alpha})^n$ sú lineárne závislé. Teda $\frac{1}{\alpha}$ je koreňom polynómu z $F[x]$ preto $\frac{1}{\alpha} \in F'$. Podobne ak $\beta \in F'$ tak $\alpha+\beta, \alpha\cdot\beta \in F(\alpha, \beta)$ čo je tiež konečno rozmerný vektorový priestor nad F a teda z rovnakých dôvodov $\alpha + \beta, \alpha \cdot \beta \in F'$. □

Adjunkcia algebrických prvkov k nejakému poľu sa dá tiež predstaviť ako pridávanie abstraktných symbolov a pravidllá pre ich násobenie. Pri odmocninách sú tie pravidlá jednoduché, pri koreňoch niektorých polynómov môžu byť komplikovanejšie.

Príklad 15. Nech α_1 je koreňom polynómu x^3+x+1 a α_2 je koreňom polynómu x^2+x+1. Ako by sme zjednodušili $(\alpha_1^2\alpha_2 + 1)^2$?

Veta 18. Ak $F \subset E$, E, F sú polia, tak množina všetkých prvkov E, ktoré sú algebrické nad F tvorí pole.

Dôkaz. Ak α, β sú algebrické nad F tak $[F(\alpha, \beta) : F] < \infty$. Položme $m = [F(\alpha, \beta) : F]$, Prvky $\alpha + \beta, \alpha\beta$

patria do $F(\alpha, \beta)$ a preto postupnosti $(\alpha+\beta)^n, (\alpha\beta)^n, n = 0, 1, 2, \ldots$ nemôžu obsahovať viac ako m prvkov ktoré sú linearne nezávislé nad F. Z toho vyplýva, že obidvaa tieto prvky sú koreňom nejakého polynómu nad F, ktorého stupeň neprevyšuje $m + 1$. To isté platí aj pre $\frac{1}{\alpha}$ ak $\alpha \neq 0$. □

Príklad 16. Ľahko sa dá ukázať, že ak $\alpha \neq 0$ je koreňom polynómu $a_n x^n + \cdots + a_0$ tak $\frac{1}{\alpha}$ je koreňom polynómu $a_0 x^n + \cdots + a_n$.

Veta 19. Ak $a_0, \ldots, a_n$ sú algebrické prvky nad poľom F a α je koreňom polynómu $a_n x^n + \cdots + a_0$ tak ak α je algebrický nad poľom F.

Dôkaz. Za týchto predpokladov je α algebrický prvok nad poľom $F(a_0, \ldots, a_n)$. To znamená, že $[F(a_0, \ldots, a_n, \alpha) : F(a_0, \ldots, a_n)] < \infty$. Je zrejmé, že $[F(a_0, \ldots, a_n) : F] < \infty$ a teda aj $[F(a_0, \ldots, a_n, \alpha) : F] < \infty$. Pretože $F(\alpha) \subset F(a_0, \ldots, a_n, \alpha)$ dostávame $[F(\alpha) : F] < \infty$. □

2.4 Hlavná veta algebry

Problém existencie koreňov polynómov nad poľom racionálnych, reálnych a komplexných čísel úplne rieši **Hlavná veta algebry:**

Veta 20. Každý polynóm s komplexnými koeficientami stupňa aspoň 1 má komplexný koreň.

Na dôkaz použijeme nasledujúcu lemu:

Lema 1. Ak $f(x)$ je polynóm s komplexnými koeficientami tak množina

$$M = \{|f(x)|; x \in \mathbb{C}\}$$

obsahuje minimum.

Dôkaz. Ak polynóm $f(x)$ je konštantný tak tvrdenie je zrejmé. Nech stupeň tohoto polynómu ja aspoň 1. Položme

$$m = \inf M.$$

Z definície infima dostávame, že pre každé $k \in \mathbb{N}$ existuje komplexné číslo z_k takém, že

$$m \leq |f(z_k)| \leq m + \frac{1}{k}.$$

Teda

$$\lim_{k\to\infty} |f(z_k)| = m. \tag{5}$$

Ak n je stupeň $f(x)$ tak tento polynóm sa dá pre $x \neq 0$ vyjadriť v tvare

$$f(x) = x^n\Big(a_n + \frac{a_{n-1}}{x} + \ldots \frac{a_0}{x^n}\Big).$$

Preto ak by postupnosť $\{z_k\}$ bola neohraničená pre nejakú jej podpostupnosť $\{z_{k_j}\}$ by platilo

$$\lim_{j\to\infty} |f(z_{k_j})| = \infty$$

a to je spor s (5). Teda $\{z_k\}$ je ohraničená postupnosť a preto obsahuje konvergentnú podpostupnosť [4] $\{z_{\ell_s}\}$. Ak $w = \lim_{s\to\infty} z_{\ell_s}$ tak podľa (5) dostávame

$$m = |f(w)|.$$

□

Dôkaz vety 20. Nech $f(x)$ je polynóm s komplexnými koeficientami stupňa $n \geq 1$. Položme rovnako ako v dôkaze predchádzajúcej lemy

$$m = \min\{|f(z)|; z \in C\} = f(w).$$

Stačí dokázať $m = 0$.

Polynóm $f(w + t)$ premennej t je tiež stupňa n. Nech

$$f(w + t) = a_n t^n + \cdots + a_1 t + a_0.$$

[4] Tento fakt je dôsledkom rovnakej vlastnosti reálnych čísel. Pole reálnych čísel je zostrojené tak aby každá jeho ohraničená neprázdna podmožina mala supremum a infimum. Z toho po istých 'uvahách vyplýva, že každá ohraničená postupnosť obsahuje konvergentnú podpostupnosť.

Je zrejmé $a_0 = f(w)$. Predpokladajme, že $a_0 \neq 0$. Polynóm $f(w+t)$ potom môžeme vyjadriť v tvare

$$f(w+t) = a_0\Big(\frac{a_n}{a_0}t^n + \cdots + \frac{a_1}{a_0}t + 1\Big).$$

Označme $r = \min\{j \geq 1; a_j \neq 0\}$. Potom

$$f(w+t) = a_0\Big(\frac{a_n}{a_0}t^n + \cdots + \frac{a_{r+1}}{a_0}t^{r+1} + \frac{a_r}{a_0}t^r + 1\Big).$$

Ak definujeme

$$g(t) = \frac{a_n}{a_0}t^{n-r} + \cdots + \frac{a_{r+1}}{a_0}t$$

dostávame vyjadrenie

$$f(w+t) = a_0\Big(t^r g(t) + \frac{a_r}{a_0}t^r + 1\Big)$$

a

$$\lim_{t\to 0} g(t) = 0. \tag{6}$$

Nech T je také komplexné číslo, že $T^r = -\frac{a_0}{a_r}$. Potom pre každé δ platí

$$f(w+\delta T) = a_0\Big(-\delta^r \frac{a_0}{a_r} g(\delta T) - \delta^r + 1\Big).$$

Pre $\delta > 0$ to znamená

$$|f(w+\delta T)| \leq |a_0|\Big(\delta^r \Big|\frac{a_0}{a_r} g(\delta T)\Big| + |-\delta^r + 1|\Big).$$

Podľa (6) existuje $\delta \in (0,1)$ také, že $|\frac{a_0}{a_r} g(\delta T)| < 1$. V tomto prípade dostávame

$$|f(w + \delta T)| < |a_0|(\delta^r - \delta^r + 1) = |a_0|,$$

to je spor s minimalitou $m = |a_0|$. □

Z hlavnej vety algebry bezprostredne vyplýva:

Veta 21. Každé algebrické rozšírenie poľa $\mathbb{Q}$ je podpole poľa komplexných čísel.

Príklad 17. Pomocou Hlavnej vety algebry sa dá dokázť, že polynómy ireducibilné nad poľom reálnych čísel sú iba lineárn a kvadratické so záporným diskriminantom.

[5] Ako autori tohoto dôkazu sú uvádzaní Jean le Rond d'Alembert (1717 -1783) a Johann Karl Friedrich Gauss (1777 - 1855). d'Alemebert bol francúzsky filozof, matematik, fyzik a astronóm a predovšetkým pokrokový mysliteľ. Napísal úvod encyklopédie, v ktorom sa zamýšľal nad vznikom vied a významom technického pokroku. Žil v Paríži. Zastával názor nezávislosti tela a ducha. Gauss patrí k zakladateľským osobnostiam modernej matematiky. Jeho prínos je tak obsiahly, že nie je tu dostatok miesta ho popisovať. Bol genialne dieťa. Pochadzal z rodiny remeselníka. Miestny kurfirst (niečo ako knieža) sa o ňom dozvedel a udelil mu štipendium, ktoré mu umožnilo študovať.

2.5 Algebrický uzáver poľa

Pole E sa nazýva **algebricky uzavreté** práve vtedy keď pre každý polynóm $f(x) \in E[x]$ stupňa aspoň 1 existuje $a \in E$ také, že $f(a) = 0$. Pole $\tilde{F} \supset F$ sa nazýva **algebrický uzáver** poľa F práve vtedy keď je algebricky uzavreté a každý jeho prvok je algebrický nad F.

Na dôkaz toho, že pole komplexných čísel ja algebricky uzavreté teda vety 20, sme použili vlastnosti usporiadania reálnych čísel, konkrétne vetu o infime a skutoňosť, že každá hraničená postupnosť reálnych čísel obsahuje konvergentú podpostupnosť. Vo všeobecnosti pole nemusí byť usporiadané tak aby dané usporiadanie súviselo s operáciami ako to poznáme u poľa reálnych čísel. Stačí uvážiť napríklad polia zvyškových tried.

V tejto časti dokážeme, že ku každému poľu existuje algebrický uzáver.

Veta 22. Nech R je komutatívny okruh s 1 a $J \subset R$ je ideal. J je maximálny ideal práve vtedy keď faktorový okruh R/J je pole.

Dôkaz. Nech J je maximálny ideal a $a + J \in R/J$ je nenulový prvok. Potom $a \notin J$ a teda $J + (a) = R$. To znamená, že pre vhodné $b \in R$ platí $ab + c = 1$ kde $c \in J$. Preto $(a + J)(b + J) = 1 + J$. Inými slovami k prvku $a + J$ existuje inverzny prvok.

Nech R/J je pole. Ak J' je vlastný nadideál J tak existuje $a_1 \in J'$ take, že $a_1 \notin J$. Teda $a_1 + J$ je nenulový prvok R/J. Podľa predpokladu inverzný. Nech $(a_1+J)(b_1+J) = 1 + J$. Potom $a_1 b_1 - 1 \in J$ a teda $1 \in J'$. □

Veta 23. Nech F je pole a $p(x)$ je polynóm stupňa aspoň 1 ireducibilný nad F. Potom hlavný ideál $(p(x))$ je maximálny.

Dôkaz. Ak $I \supset (p(x))$ je vlastný nadideál tak existuje polynóm $h(x) \in I$, ktorý nie je deliteľný $p(x)$. Z ireducibilty $p(x)$ dostávame, že $h(x)$ a $p(x)$ sú nesúdeliteľné a teda pre vhodné polynómy $f(x)$ a $g(x)$ platí

$$1 = f(x)p(x) + g(x)h(x.)$$

Preto $1 \in I$. Z toho vyplýva, že ideál I obsahuje všetky násobky 1 a teda celý okruh $F[x]$. □

Príklad 18. Inverzný prvok k $2x + 1 + (x^2 + 2)$ v poli $\mathbb{Z}_5[x]/(x^2 + 2)$ môžeme nájsť v tvare $ax + b + (x^2 + 2)$.

Pretože každý polynóm stupňa aspoň 1 je deliteľný nejakým ireducibilným polynómom dostáveme bezprostredne z predoslej vety

Veta 24. Každý polynóm nad nejakým poľom stupňa aspoň 1 má koreň v nejakom konečnom rozšírení daného poľa.

Príklad 19. Keď uvažujeme polynóm $x^2 + x + 1$ nad $\mathbb{Z}_5$ tak tento má koreň v nadpoli $\mathbb{Z}_5[x]/(x^2 + x + 1)$.

Príklad 20. Pole komplexných čísel je vlastne pole $\mathbb{R}[x]/(x^2 + 1)$. Triedu $x + (x^2 + 1)$ tradične označujeme i. Triedy $a + (x^2 + 1)$ označujeme jednoducho a pre reálne číslo a.

Ďalej využijeme pri tom nasledejúce tvrdenie známe pod názvom **Krullova veta**: [6]

Veta 25. Nech R je komutatívny okruh s 1. Ak $I \subset R$ je netrivialny ideál tak existuje maximálny ideál J taký, že $I \subset J$.

Dôkaz. Vetu dokážeme za predpokladu, že okruh R je spočítateľný. Ak množina $R \setminus I$ je konečná okruh tak systém nadidealov I je konečný a tvrdenie je teda jasné. Nech množina $R \setminus I$ je nekonečná spočítateľná. Označme

$$R \setminus I = \{r_n, n \in \mathbb{N}\}.$$

Definujme postupnosť ideálov: $I_0 = I$ a $I_{n+1} = I_n + (r_n)$ ak $1 \notin I_n + (r_n)$ a $I_{n+1} = I_n$ v opačnom prípade. Je zrejmé,

[6] Wolfgang Krull, 26. augusta 1899 – 12. april 1971, bol nemecký matematik, ktorého práca priniesla zásadné výsledky v teórii okruhov. Špecialny typ okruhov nesie na jeho počesť názov Krullove okruhy.

že $I_n \subset I_{n+1}, n \in \mathbb{N}$. Preto množina

$$J = \bigcup_{n=0}^{\infty} I_n$$

je ideál a $1 \notin J$. Nech J' je vlastný nadideál J. Potom existuje $r \in J'$ také, že $r \notin J$. Potom $r \notin I$. Teda existuje $k \in \mathbb{N}$ také že $r = r_k$. Ale $r_k \notin I_{k+1}$ teda $1 \in I_k + (r)$. Je zrejmé, že $I_k + (r) \subset J'$ a teda $1 \in J'$ preto $J' = R$. □

Pre ľubovoľný komutatívny okruh s 1 vyplýva Krullova veta z tzv. Zornovej lemy. Je to tvrdenie ekvivalentné Axiome výberu.

Zornova lema: Nech $(M, \leq)$ **je taká čiatočne usporiadaná množina, že každá jej lineárne uporiadaná podmožina je zhora ohraničená. Potom pre každý prvok** $a \in M$ **existuje maximálny prvok** $m \in M$ **taký, že** $a \leq m$**.**
[7]

Nech M je množina všetkých vlastných ideálov okruhu R usporiadaná množinovou inklúziou a obsahuje aspoň jeden ideál I. Ak $H \subset M$ je jej lineárne usporiadaná podmnožina tak aj $\cup H$ je vlastný ideál a teda $\cup H \in M$. Vyplýva to z toho, že žiaden prvok H neobsahuje 1 a teda

[7] O tom ako súvisí Zornova lema s axiomami teórie množín, konkrétne s Axiomou výberu, ktorá je ľahko predstaviteľná a intuitívne prijateľná je pojednané v Doplnkoch.

ani zjednotenie H neobsahuje 1. Preto podľa Zornovej lemy I je podideálom nejakého maximálneho ideálu J.

Veta 26. Ku každému poľu F existuje algebricky uzavreté pole E také, že $F \subset E$.

Dôkaz. Uvažujme okruh polynómov $F[x]$. Priraďme každému polynómu $f(x) \in F[x]$ neurčitú, ktorú označíme x_f. Nech $R = F[x_f; f(x) \in F[x]]$ je okruh polynómov nad F s neurčitými $x_f; f(x) \in F[x]$. Označme

$$I = (\{f(x_f), f(x) \in F[x]\})$$

ideál okruhu R generovaný všetkými $f(x_f)$, kde stupeň $f(x)$ je aspoň 1. Ukážeme, že tento ideál je netrivialny. Ak by $I = R$ tak $1 \in I$ a teda pre nejaké polynómy $p_1, \ldots, p_k \in R$ by platilo

$$1 = p_1 f_1(x_{f_1}) + \cdots + p_k f_k(x_{f_k}).$$

Podľa vety 24 má každý polynóm stupňa aspoň 1 koreň v nejakom nadpoli, existovali by prvky $\alpha_1, \ldots, \alpha_k$ z nejakého nadpoľa F také, že $f_i(\alpha_i) = 0, i = 1, \ldots, k$. Potom by sme dostali

$$1 = p_1 f_1(\alpha_1) + \cdots + p_k f_k(\alpha_k) = 0$$

a to je spor. Z vety 25 vyplýva, že existuje maximálny ideál $J \subset R$ taký, že $I \subset J$. Faktorový okruh $F_1 = R/J$ je pole.

Trieda $x_f + J$ je koreňom polynómu $f(x) \in F[x]$ ak tento je stupňa aspoň jedna. Preto každý polynóm z $F[x]$ stupňa aspoň jedna má koreň v F_1.

Podobne k poľu F_1 môžeme zostrojiť nadpole F_2 také, že každý polynóm z $F_1[x]$ stupňa aspoň 1 má koreň v F_2. Teda matematickou indukciou dos- távame postupnosť polí

$$F = F_0 \subset F_1 \subset \ldots F_j \subset F_{j+1} \subset \ldots$$

takú, že každý polynóm stupňa aspoň jedna z $F_j[x]$ má koreň v F_{j+1}, $j = 0, 1, 2, \ldots$. Je zrejmé, že $E = \bigcup_{j=0}^{\infty} F_j$ je pole[8] . Ak $f(x) \in E[x]$ tak koeficienty tohoto polynómu patria do jednotlivých polí F_j. Teda pre vhodné k platí $f(x) \in F_k[x]$. Preto ak je tento polynóm stupňa aspoň 1 má koreň v F_{k+1} a teda v E. □

Veta 27. Nech F je pole a $E \supset F$ je algebricky uzavreté pole. Nech $\tilde{F} \subset E$ je pole všetkých prvkov E ktoré sú algebrické nad F. Potom $\tilde{F}$ je algebricky uzavreté pole.

Dôkaz. Predpokladajme, že $f(x) \in \tilde{F}[x]$. Tento polynóm má nejaký koreň $\alpha \in E$. V takom prípade prvok α je

[8]To, že E je pole vyplýva z toho, že ak $x, y \in E$ tak existujú prirodzené čísla $n_1 \leq n_2$ také, že $x \in F_{n_1}, y \in F_{n_2}$. Určite $F_{n_1} \subset F_{n_2}$ a teda $x, y \in F_{n_2}$ potom $x + y, x - y \in F_{n_2} \subset E$ a podobne ak $y \neq 0$ tak $\frac{x}{y} \in E$.

algebricý nad $\tilde{F}$ a podľa vety je teda algebrický aj nad F. Preto $\alpha \in \tilde{F}$. □

2.6 Jednoduché rozšírenie

Veta 28. Nech $F \subset \mathbb{C}$ je pole a α, β sú algebrické prvky nad F. Označme $f_1(x)$ minimálny polynóm prvku α nad F a $f_2(x)$ minimálny polynóm prvku β nad F. Ďalej nech $\alpha = \alpha_1, \ldots, \alpha_m$ sú všetky korene polynómu $f_1(x)$ v nadpoliach F a tak isto $\beta = \beta_1, \ldots, \beta_n$ sú všetky korene polynómu $f_2(x)$ v nadpoliach F. Položme

$$\gamma = \alpha + t\beta$$

kde $t \in F$ je taký prvok aby

$$\gamma - t\beta_i \neq \alpha_j \tag{7}$$

pre $i = 2, \ldots, m, j = 2, \ldots, n$. Potom $F(\alpha, \beta) = F(\gamma)$.

Dôkaz. Je zrejmé, že $\gamma \in F(\alpha, \beta)$ a teda $F(\gamma) \subset F(\alpha, \beta)$. Preto stačí dokázať opačnú inklúziu. Na to zase stačí dokázať, že $\beta \in F(\gamma)$ lebo v tom prípade $\alpha = \gamma - t\beta \in F(\gamma)$.

Definujme polynóm

$$h(x) = f_1(\gamma - tx) \in F(\gamma)[x].$$

Vidíme hneď, že

$$h(\beta) = f_1(\alpha) = 0.$$

Podľa (7) polynómy $h(x)$ a $f_2(x)$ nemajú ine spoločné korene. Nech $g(x)$ je minimálny polynóm prvku β nad poľom $F(\gamma)$. V takom prípade $g(x)$ je deliteľom polynómov $h(x)$, $f_2(x)$ pretože oba majú koreň β. Z toho vidíme, že $g(x)$ musí byt lineárny. V opačnom prípade by mal v nejakom nadpoli viac koreňov a teda $h(x)$, $f_2(x)$ by mali aspoň dva spoločné korene, co je spor s predošlým. Z linearity $g(x)$ vyplýva $\beta \in F(\gamma)$. □

Príklad 21. Platí napríklad $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.

Ak $E = F(\gamma)$ tak prvok γ sa nazýva **primitívny prvok** a E sa nazýva **jednoduché** rozšírenie poľa F.

Ak F je nekonečné pole tak existuje nekonečne veľa prvkov t ktoré spĺňajú (7) a teda platí

Veta 29. Každé konečné rozšírenie nekonečného poľa F jednoduchým rozšírením.

2.7 Cyklotomické polynómy

Z vety 2.17 vidíme, že pri rozširovaní polí hrajú istú úlohu minimálne polynómy. Odvodíme formulu pre mini- málne polynómy tzv. odmocnín z 1 v poli komplexných čísel.

Nech n je prirodzené číslo. Položme

$$w_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

[9] Z Moivreovej vety vyplýva, že $w_n^n = 1$ a teda hodnoty $w_n^j, j = 0, \dots n-1$ sú koreňom polynómu $x^n - 1$. Preto tento polynóm sa rozkladá na lineárne činitele

$$x^n - 1 = \prod_{j=0}^{n-1}(x - w_n^j). \tag{8}$$

Komplexné čísla $w_n^j, j = 0, \dots n-1$ tvoria vrcholy pravidelného n uholníka na jednotkovej kružnici.

Príklad 22. Komplexné číslo w_5 je koreňom rovnice

$$x^5 - 1 = 0$$

[9] V literatúre je viac rozšírené iné označenie w_n. Ak si exponencialnu funkciu rozvinieme do Taylorovho radu a dosadíme komplexnú premennú dostaneme po istých úpravách rovnosť

$$e^{ix} = \cos x + i\sin x.$$

V našom prípade to znamená

$$w_n = e^{\frac{2\pi}{n}}.$$

a po vydelení činiteľom $x-1$ dostávame, že je koreňom

$$x^4 + x^3 + x^2 + x + 1 = 0$$

a z toho si môžeme vyjadriť w_5 pomocou druhých odmocnín. To nám okrem iného umožní zostrojiť pravidelný päťuholník pomocou pravítka a kružidla. V prípade iných n uholníkov je situácia omnoho komplikovanejšia. Tejto problematike bude venovaná špecialna kapitola.

Ak $(j,n) = 1$ tak hodnota w_n^j sa nazýva **primitívna n - tá odmocnina z** 1.

Príklad 23. Dá sa dokázať , že korene rovnice $x^n = 1$ tvoria grupu vzhľadom na násobenie, ktorá je izomorfná s $(\mathbb{Z}_n, +)$ a každá primitívna n - té odmocnina s 1 je jej generátorom.

Bude nas zaujímať minimálny polynóm čísla w_n. Dokážeme že je to polynóm

$$\Phi_n(x) = \prod_{j<n,(n,j)=1} (x - w^j).$$

Jednoducho sa dá preveriť

$$w_n^{\frac{n}{d}} = w_d$$

pre každý deliteľ čísla n. Z rovnosti (8) preto vyplýva

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{9}$$

Veta 30. Pre každé $n \in \mathbb{N}$ je polynóm $\Phi_n(x)$ je normovaný celočíselnými koeficientami.

Dôkaz. Budeme postupovať indukciou podľa n. Je zrejmé, že $\Phi_1(x) = x - 1$. Nech veta platí pre $d < n$. Z rovnosti (9) dostávame

$$\Phi_n(x) = x^n - 1 : \prod_{d|n, d<n} \Phi_d(x).$$

Všetky činitele v deliteli v tejto rovnosti sú normované polynómy s celočíselnými koeficientami , preto aj delteľ je normovaný polynóm s celočíselnými koeficientami. Teda aj výsledok hore uvedeného delenia je normovaný polynóm s celočíselnými koeficientami. □

Stačí teda dokázať už len to, že tento polynóm je ireducibilný. Okrem iného tam použijeme vlastnosti redukcie celočíselného polynómu modulo daného prvočísla. Ak p je pevne dané prvočíslo a

$$f(x) = a_n x^n + \cdots + a_0$$

je polynóm patriaci $\mathbb{Z}[x]$ symbolom $\overline{f}(x)$ budeme označovať jeho redukciu modulo p danú rovnosťou

$$\overline{f}(x) = (a_n \mod p)x^n + \cdots + (a_0 \mod p),$$

teda koeficienty zameníme ich zvyškami po delení p. A $\overline{f}(x)$ uvažujeme ako polynóm patriaci do $\mathbb{Z}_p[x]$. Je zrejmé , že platí

$$\overline{f(x)f_1(x)} = \overline{f}(x)\overline{f_1}(x) \tag{10}$$

a

$$\overline{f(x) + f_1(x)} = \overline{f}(x) + \overline{f_1}(x) \tag{11}$$

pre $f(x), f_1(x) \in \mathbb{Z}[x]$.

Príklad 24. Ak $f(x) = 21x^8 + 27x^4 + 7x + 6$ a $p = 5$ tak $\overline{f}(x) = x^8 + 2x^4 + 2x + 1$.

Veta 31. Polynóm $\Phi_n(x)$ je ireducibilný pre $n = 1, 2, 3, \ldots$.

Dôkaz. Nech $\Phi_n(x) = f(x)g(x)$ kde $f(x)$ je ireducibilný polynóm taký, že $f(w_n) = 0$. Ak dokážeme, že $f(x)$ má tie isté korene ako $\Phi_n(x)$ veta bude dokázaná. Je zrejmé, že

$$\Phi_n(v) = 0 \Longrightarrow \Phi_n(v^r) = 0 \tag{12}$$

pre každé komplexné číslo v a $r \in \mathbb{N}$ také že $(r, n) = 1$. Dokážeme rovnakú implikáciu aj pre $f(x)$. Nech $f(v) =$

0 a p je prvočíslo nesúdeliteľné s n. Ak $f(v^p) \neq 0$ tak podľa (12) máme $g(v^p) = 0$. Teda v je koreňom polynómu $g(x^p)$. Z toho vyplýva $f(x)|g(x^p)$. Označme pre ľubovoľný polynóm $h(x)$ symbolom $\overline{h}(x)$ jeho redukciu na polynóm patriaci do $\mathbb{Z}_p[x]$. Z Malej fermatovej vety [10] vyplýva $\overline{g}(x^p) = \overline{g}(x)^p$. Preto $\overline{f}(x)|\overline{g}(x)^p$. Nech $\overline{f_1}(x)$ je ireducibilný faktor polynómu $\overline{f}(x)$ v $\mathbb{Z}_p[x]$. Preto $\overline{f}_1(x)|\overline{g}(x)$. Je zrejmé že $f(x)g(x)|x^n - 1$. Položme $m(x) = x^n - 1$. Preto

$$\overline{f}_1(x)^2\overline{m}_1(x) = \overline{m}(x),$$

kde $\overline{m}_1(x)$ je nejaký polynóm patriaci do $\mathbb{Z}_p[x]$. Z tejto rovnosti vyplýva $\overline{f}_1(x)|\overline{m}(x)'$. To je spor lebo z podmienky $(p, n) = 1$ vyplýva $(\overline{m}(x), \overline{m}(x)') = 1$. □

Veta 32. Nech F je podpole $\mathbb{C}$ a $a \in F$. Pre každé prvočíslo $p \in \mathbb{N}$ platí , že polynóm $x^p - a$ je ireducibilný nad F vtedy a len vtedy ak nemá v poli F koreň.

Dôkaz. Nech $\alpha \in \mathbb{C}$ je také komplexné číslo , ze $\alpha^n =$

[10] Pierre de Fermat bol sudca a matematik, žil v 17. storočí . Malá fermatova veta patrí do elementárnej teórie čísel hovorí : $a^p \equiv a \pmod{p}$, kde $a \in \mathbb{Z}$ a p je prvočíslo. Dejiny matematiky ovplyvnila tzv. Veľká fermatova veta o neexistencii netrivialnych riešení diofantickej rovnice $x^n + y^n = z^n$ pre $n > 2$. Dokázal ju až John Wiles v roku 1994.

a. Potom

$$x^p - a = \prod_{j=0}^{p-1}(x - w_p^j \alpha).$$

Ak by polynóm $x^p - a$ bol reducibilný nad poľom F tak pre nejaké $k < p$ by sa súčin k faktorov z hore uvedeného rozkladu, ktorý má tvar

$$\prod_{i=1}^{k}(x - w_p^{j_i} \alpha) \tag{13}$$

by tvoril polynóm ktoý ma koeficienty z F. Označme konštantný koeficient tohoto polynómu c. Z výrazu (13) dostávame, že $c = w_p^s \alpha^k$ pre vhodné $s \in \mathbb{N}$. Preto

$$c^p = (w_p^s \alpha^k)^p = a^k.$$

Keď uvážime, že p je prvočíslo dostávame $1 = (p, k)$. Preto pre nejaké celé čísla x, y platí $1 = px + ky$. To znamená

$$a = a^{px} a^{ky} = a^{px} c^{py} = (a^x c^y)^p.$$

Preto hodnota $a^x c^y$ je koreňom polynómu $x^p - a$. □

Príklad 25. Podľa predošlej vety je polynóm $x^7 - 2$ ireducibilný, teda
$[\mathbb{Q}(\sqrt[7]{2}) : \mathbb{Q}] = 7$ a teda podobným argumentom ako v

Príklade 11 sa dá dokázať, že $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[7]{2})$. Rovnako môže- me odvodiť, že žiaden koreň x^3-2 nepatrí do $\mathbb{Q}(\sqrt[7]{2})$ a teda x^3-2 je ireducibilný aj nad $\mathbb{Q}(\sqrt[7]{2})$. To znamená $[\mathbb{Q}(\sqrt[7]{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[7]{2})] = 3$. Z toho vyplýva $[\mathbb{Q}(\sqrt[7]{2}, \sqrt[3]{2}) : \mathbb{Q}] = 21$.

.

Príklad 26. Podobne ako Veta 32 sa dá dokázať :
Nech $n \in \mathbb{N}$ a $F \subset C$ je pole ktoré obsahuje w_n. Ak $a \in F \setminus \{1\}$ tak polynóm $x^n - a$ je reducibilný nad F práve vtedy ak existuje $d \in \mathbb{N}, d > 1$ také, že $d|n$ a $\sqrt[d]{a} \in F$, (podľa [8]).

Príklad 27. Rovnako sa tiež dá dokázať, že ak a, n sú také prirodzené čísla, že

$$a = p_1^{\alpha_1} \dots p_j^{\alpha_j}$$

je kanonický rozklad a a $(\alpha_1, \dots, \alpha_j, n) = 1$ tak polynóm $x^n - a$ je ireducibilný nad $\mathbb{Q}$.

Trochu komplikovanejšia je otázka, či napríklad $\sqrt[7]{3}$ patrí do $\mathbb{Q}(\sqrt[7]{2})$. Neskôr ukážeme, že nepatrí .

2.8 Rozširovane izomorfizmov

Túto časť začneme príkladmi pre ilustráciu.

Príklad 28. Dá sa dokazať že zobrazenie

$$\varphi : \mathbb{Q}[x]/(x^2 - 2) \to \mathbb{Q}(\sqrt{2})$$

kde

$$\varphi(a + bx + (x^2 - 2)) = a + b\sqrt{2}$$

je izmorfizmus.

Príklad 29. Zobrazenie

$$\varphi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(w_3\sqrt[3]{2})$$

pričom

$$\varphi(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + bw_3\sqrt[3]{2} + c(w_3\sqrt[3]{2})^2$$

je izomorfizmus.

Nech F_1, F_2 sú polia a zobrazenie $\varphi : F_1 \to F_2$ izomorfizmus. Môžeme ho prirodzeným spôsobom rozšíriť zobrazenie medzi okruhmi polynómov $\tilde{\varphi} : F_1[x] \to F_2[x]$ ak pre $f(x) = \sum_{j=0}^{n} a_j x^j$ definujeme

$$\tilde{\varphi}(f)(x) = \sum_{j=0}^{n} \varphi(a_j)x^j. \tag{14}$$

Jednoduchými výpočtami sa dá preveriť, že toto zobrazenie je izomorfizmus.

Veta 33. Nech $g(x) \in F_1[x]$ je ireducibilný polynóm stupňa m , α je jeho koren v nejakom nadpoli F_1 a β je koreňom polynómu $\tilde{\varphi}(g)(x)$ nejakom nadpoli F_2. Potom existuje jediný izomorfizmus $\varphi_\alpha : F_1(\alpha) \to F_2(\beta)$ taky, že $\varphi_\alpha(\alpha) = \beta$ a $\varphi_\alpha|_{F_1} = \varphi$.

Dôkaz. Definujme zobrazenie

$$\varphi_\alpha : F_1(\alpha) \to F_2(\beta)$$

$$\varphi_\alpha(c_{m-1}\alpha^{m-1} + \cdots + c_0) = \varphi(c_{m-1})\beta^{m-1} + \cdots + \varphi(c_0).$$

Je evidentné ze dané zobrazenie je bijekcia a zachováva súčet. Nech $a, b \in F_1(\alpha)$ a $a = h(\alpha), b = h_1(\alpha)$ kde $h(x)$, $h_1(x) \in F_1[x]$ sú polynómy stupňa menšieho ako m. Potom

$$h(x)h_1(x) = g(x)q(x) + h_2(x) \tag{15}$$

kde $q(x), h_2(x) \in F_1[x]$ a stupeň $h_2[x]$ je menší ako m. Preto

$$ab = h(\alpha)h_1(\alpha) = h_2(\alpha).$$

Teda $\varphi_\alpha(ab) = \tilde{\varphi}(h_2)(\beta)$. Z rovnosti (15) dostávame

$$\tilde{\varphi}(h)(x)\tilde{\varphi}(h_1)(x) = \tilde{\varphi}(g)(x)\tilde{\varphi}(q)(x) + \tilde{\varphi}(h_2)(x).$$

Z toho vyplýva

$$\tilde{\varphi}(h)(\beta)\tilde{\varphi}(h_1)(\beta) = \tilde{\varphi}(h_2)(\beta),$$

čo znamená $\varphi_\alpha(ab) = \varphi_\alpha(a)\varphi_\alpha(b)$. □

Príklad 30. Nech p je prvočíslo. Je zrejmé, že $\Phi_p(x) = x^{p-1} + \cdots + 1$. Pre $j = 1, \ldots, p-1$ platí $\mathbb{Q}(w_p) = \mathbb{Q}(w_p^j)$. Podľa Vety 33 pre tieto j existuje izomorfizmus φ_j daný rovnosťou $\varphi_j(w_p) = w_p^j$. Je zrejmé, že $\varphi_j \circ \varphi_k = \varphi_{jk \mod p}$. Preto $G(\mathbb{Q}(w_p) : \mathbb{Q}) = \{\varphi_j; j = 1, \ldots, p-1\}$ a platí , že grupa $G(\mathbb{Q}(w_p) : \mathbb{Q})$ je izomorfná multiplikatívnou grupou zvyškov modulo p.

Ak $f(x)$ je polynóm na poľom F a $f(x) = a(x - \alpha_1) \ldots (x - \alpha_n)$ kde $\alpha_1, \ldots, \alpha_n$ sú prvky nejakého nadpoľa F, tak pole $F(\alpha_1, \ldots, \alpha_n)$ sa nazýva **rozkladové pole** polynómu $f(x)$ nad poľom F. Dá sa povedať že, z hľadiska inklúzie je to minimálne pole nad ktorým sa daný polynóm rozkladá na lineárne činitele.

Príklad 31. Pole $\mathbb{Q}(\sqrt{2}, -\sqrt{2})$ je rozkladove pole polynómu $x^2 - 2$ nad poľom $\mathbb{Q}$. Je jasné na prvý pohľad, že toto vzniká adjunkciou jediného prvku a to $\sqrt{2}$ pretože $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$.

Príklad 32. Ak E je rozkladové pole kvadratickeho polynómu nad $\mathbb{Q}$ a diskriminant tohoto polynómu nie je druhou mocninou racinálneho čísla tak $G(E : F)$ je izomorfná s aditívnou grupou $\mathbb{Z}_2$.

Príklad 33. Pole $\mathbb{Q}(\sqrt[3]{2}, w_3\sqrt[3]{2}, w_3^2\sqrt[3]{2})$ je rozkladové pole polynómu $x^3 - 2$ nad poľom $\mathbb{Q}$. Aj v tomto prípade platí , že

stačí adjungovať menej prvkov ako všetky korene daného polynómu, pretože $\mathbb{Q}(\sqrt[3]{2}, w_3\sqrt[3]{2}, w_3^2\sqrt[3]{2}) =$
$= \mathbb{Q}(\sqrt[3]{2}, w_3\sqrt[3]{2})$. Dokonca platí $\mathbb{Q}(\sqrt[3]{2}, w_3\sqrt[3]{2}, w_3^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, w_3)$.

Príklad 34. Uvažujme galoisovu grupu $G(\mathbb{Q}(\sqrt[3]{2}, w_3) : \mathbb{Q})$. Ak φ je prvok tejto grupy tak $\varphi(\sqrt[3]{2}) = w_3^j\sqrt[3]{2}$ a $\varphi(w_3) = w_3^k$ pre nejaké $j = 0, 1, 2$ a $k = 1, 2$.

Podľa vety 33 pre každé $k = 1, 2$ exisuje izomorfizmus $\varphi_k : \mathbb{Q}(w_3) \to \mathbb{Q}(w_3^k), \varphi_k(w_3) = w_3^k$ ktorý ja na $\mathbb{Q}$ identický. K tomuto izomorfizmu existuje izomorfizmus $\varphi_{k,j} : \mathbb{Q}(w_3, \sqrt[3]{2}) \to \mathbb{Q}(w_3^k, w_3^j\sqrt[3]{2})$ taky, že $\varphi_{k,j}(\sqrt[3]{2}) = w_3^j\sqrt[3]{2}$ ktorý ja na $\mathbb{Q}(w_3^j)$ totožný s φ_k. (To, že uvedené polia sú rovnaké nie je na závadu.) Preto $G(\mathbb{Q}(\sqrt[3]{2}, w_3) : \mathbb{Q}) = \{\varphi_{1,0}, \varphi_{1,1}, \varphi_{1,2}, \varphi_{2,0}, \varphi_{2,1}, \varphi_{2,2}\}$.

Treba poznamenať, že rozkladové pole nie je určené pre daný polynóm úplne jednoznačne. Napríklad konečné pole, ktoré má p^k prvkov, p je prvo- číslo, je rozkladové pole polynómu $x^{p^k} - x \in \mathbb{Z}_p[x]$. Vieme, že týchto polí môže byť viac, závisia od polynómu podľa ktorého faktorizujeme. Z nasledujúcej vety vyplynie, že všetky takéto polia sú izomorfné.

Veta 34. Nech $g(x) \in F_1[x]$. Ak E_1 je rozkladove pole $g(x)$ nad F_1 a E_2 je rozkladové pole $\tilde{\varphi}(f)(x)$ nad F_2 tak existuje izomorfizmus $\psi : E_1 \to E_2$ taký, že pre $a \in F_1$ plati $\psi(a) = \varphi(a)$.

Dôkaz. Pole E_1 je konečným rozšírením poľa F_1. To nám umožňuje postupovať indukciou podľa $[E_1 : F_1]$. Ak $[E_1 : F_1] = 1$ platnosť vety je zrejmá. Nech $m \in \mathbb{N}$. Predopokladajme, že veta platí pre všetky prípady ked $[E_1 : F_1] < m$. Predpokladajme, že $[E_1 : F_1] = m$. Nech $g_1(x)$ je ireducibylný faktor $g(x)$ a α nejaký koreň $g_1(x)$. Potom $F_1 \subset F_1(\alpha) \subset E_1$ a

$$[E_1 : F_1] = [E_1 : F_1(\alpha)] \cdot [F_1(\alpha) : F_1]$$

teda $[E_1 : F_1(\alpha)] < m$. Koreňu α zodpovedá nejaký koreň polynómu
$\tilde{\varphi}(g_1(x))$ ktorý môžeme označiť $\beta \in E_2$. Podľa vety 33 existuje izmorfizmus $\varphi_\alpha : F_1(\alpha) \to F_2(\beta)$ taký, že $\varphi_\alpha(\alpha) = \beta$. Podľa indukčného predpokladu preto existuje izomorfizmus $\psi : E_1 \to E_2$ taký, že $\psi(c) = \varphi_\alpha(c)$ pre $c \in F_1(\alpha)$ a teda sa zhoduje s φ na F_1. □

Príklad 35. Patrí číslo $\sqrt[3]{3}$ do $\mathbb{Q}(\sqrt[3]{2})$? Ukážeme, že nie. Uvažujme izomorfizmus polí $\varphi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(w_3\sqrt[3]{2})$, $\varphi(\sqrt[3]{2}) = w_3\sqrt[3]{2}$. Pretože $\mathbb{Q}(w_3, \sqrt[3]{2})$ rozkladove pole polynómu $x^3 - 2$ môžeme predpokladať, že existuje izomorfizmus $\psi : \mathbb{Q}(w_3, \sqrt[3]{2}) \to \mathbb{Q}(w_3, \sqrt[3]{2})$ taký, že $\psi(a) = \varphi(a), a \in \mathbb{Q}(\sqrt[3]{2})$. Ak by $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$ tak $\sqrt[3]{3} \in \mathbb{Q}(w_3, \sqrt[3]{2})$. Potom $(\psi(\sqrt[3]{3}))^3 = 3$ a teda $\psi(\sqrt[3]{3}) = w_3^j\sqrt[3]{3}$ pre nejaké $j = 0, 1, 2$. Z druhej strany predpoklad $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$ dáva

$$\sqrt[3]{3} = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, a, b, c \in \mathbb{Q}.$$

a teda

$$\psi(\sqrt[3]{3}) = a + bw_3\sqrt[3]{2} + cw_3^2(\sqrt[3]{2})^2.$$

Teda

$$w_3^j\sqrt[3]{3} = a + bw_3\sqrt[3]{2} + cw_3^2(\sqrt[3]{2})^2$$

čo znamená

$$aw_3^j + bw_3^j\sqrt[3]{2} + cw_3^j(\sqrt[3]{2})^2 = a + bw_3\sqrt[3]{2} + cw_3^2(\sqrt[3]{2})^2$$

teda

$$a(1 - w_3^j) + b(w_3 - w_3^j)\sqrt[3]{2} + c(w_3^2 - w_3^j)(\sqrt[3]{2})^2 = 0.$$

Polynóm $x^3 - 2$ nemá koreň v $\mathbb{Q}(w_3)$, teda je podľa vety 32 ireduciblný nad týmto poľom. To znamená, že prvky $1, (\sqrt[3]{2}), (\sqrt[3]{2})^2$ sú lineárne nezávisé nad $\mathbb{Q}(w_3)$. Preto $a(1 - w_3^j), b(w_3 - w_3^j), c(w_3^2 - w_3^j)$ sú nulové. Iba jediné z čísel $(1 - w_3^j), (w_3 - w_3^j), (w_3^2 - w_3^j)$ je 0 a teda najviac jedno z racionalnćh čísel a, b, c je rôzne od 0. Preto $\sqrt[3]{3} = r(\sqrt[3]{2})^s$, pre nejaké $r \in \mathbb{Q}, s = 0, 1, 2$ - spor.

Veta 35. Pre každé prvočíslo p a prirodzené číslo n existuje konečné pole ktoré má p^n prvkov. Dve polia s rovnakým počtom prvkov sú izomorfné.

Dôkaz. Uvažujme pole $\mathbb{Z}_p$ a jeho algebrický uzáver A. Uvažujme polynóm $x^{p^n} - x \in \mathbb{Z}_p[x]$. Jeho formálna

derivácia je rovná $(x^{p^n} - x)' = -1$. Z tohoto dôvodu nemá tento polynóm násobné korene a teda má v A presne p^n koreňov. Túto množinu označíma

$$F = \{\alpha \in A; \alpha^{p^n} = \alpha\}.$$

Pole A má charakteristiku p a preto pre každé $\alpha, \alpha_1 \in A$ platí $(\alpha + \alpha_1)^{p^n} = \alpha^{p^n} + \alpha_1^{p^n}$. Z toho vyplýva, že F je pole.

Ak F_1 a F_2 sú polia ktoré majú rovnaký počet prvkov tak majú p^n prvkov pre nejaké prvočíslo p. Z toho vyplýva, že majú charakteristiku p. Teda obe polia obsahujú podpolia E_1 a E_2 ktoré sú izomorfné zo $\mathbb{Z}_p$. Obe polia F_1 aj F_2 sú rozkladovými poľami polynómu $x^{p^n} - x$ nad E_1 resp. E_2 a preto sú podľa vety 34 izomorfné. □

Príklad 36. Izomorfizmus z predošlej vety nemusí byť na prvý pohľad zrejmý. Napríklad polia $\mathbb{Z}_5[x]/(x^2 + x + 1)$ a $\mathbb{Z}_5[x]/(x^2 + 2)$ sú rozkladové polia polynómu $x^{25} - x$ nad $\mathbb{Z}_5$ ale násobenie je v každom iné. Je to tým, že prvom poli sa násobí modulo polynóm $x^2 + x + 1$ teda $(x + (x^2 + x + 1))(x + (x^2 + x + 1)) = 4x + 4 + (x^2 + x + 1)$. V druhom poli sa násobí modulo polynóm $x^2 + 2$ a preto platí $(x + (x^2 + 2))(x + (x^2 + 2)) = 3 + (x^2 + 2)$. Teda zobrazenie $ax + b + (x^2 + x + 1) \to ax + b + (x^2 + 2)$ nie je izomorfizmus.

Príklad 37. Ak F je konečné nadpole $\mathbb{Z}_p$ kde p je prvočíslo, tak je ho multiplikatívna grupa je cyklická. Nech α je

jej generátor tak $F = \mathbb{Z}_p(\alpha)$. Ak $|F| = p^n$ tak minimálny polynóm α nad $\mathbb{Z}_p$ ja n - tého stupňa. Okrem iného teda platí ,že pre každé n existuje ireducibilný polynóm stupňa n nad $\mathbb{Z}_p$.

Veta 36. Nech F je pole a $f(x) \in F[x]$ je separabilný polynóm. Ak E je rozkladove pole polynómu $f(x)$ nad F tak

$$|G(E : F)| = [E : F].$$

Dôkaz. Budeme postupovať indukciou podľa $[E : F]$. Veta určite platí ak $[E : F] = 1$. Nech $n \in \mathbb{N}, n > 1$ a predpokladajme, že veta platí vždy ked $[E : F] < n$. Budeme študovať prípad $[E : F] = n$. Z podmienky $n > 1$ vyplýva že $f(x) = p(x)q(x)$ kde $p(x)$ je ireducibliný polynóm stupňa $d > 1$. Tento polynóm má presne d koreňov $\alpha_1, \dots \alpha_d$ ktoré patria do E pretože E obsahuje všetky korene $f(x)$. Teda E obsahuje podpolia $F(\alpha_i), i = 1, \dots, d$. Uvažujme podgrupu $G(E : F(\alpha_1)) \subset G(E : F)$ Podľa indukčného predpokladu platí

$$|G(E : F(\alpha_1))| = [E : F(\alpha_1)] = \frac{n}{d}. \tag{16}$$

Budeme teraz zisťovať ako sa grupa $G(E : F)$ dá rozložiť na triedy podľa podgrupy $G(E : F(\alpha_1))$. Pole $F(\alpha_1)$ je izomorfné z každým z polí $F(\alpha_i)$, $i = 1, \dots d$. Každý z

týchto izomorfizmov sa dá rozšíriť na izomorfizmus $\varphi_i \in G(E:F)$ taký že $\varphi_i(\alpha_1) = \alpha_i, i = 1, \ldots, d$.

Grupa $G(E : F(\alpha_1))$ obsahuje práve tie automorfizmy, ktoré zobrazujú prvky $F(\alpha_1)$ na seba. Každý prvok $F(\alpha_1)$ je polynomický výraz obsahujúci len α_1 a koeficienty z F. Pretože každý automorfizmus z $G(E : F)$ zachováva prvky F tak bude zachovávať prvky $F(\alpha_1)$ práve vtedy keď bude zachovávať α_1. To znamená

$$\varphi \in G(E : F(\alpha_1)) \iff \varphi(\alpha_1) = \alpha_1. \tag{17}$$

Ak $\psi \in G(E : F)$ tak $\psi(\alpha_1)$ je tiež koreňom polynómu $p(x)$ (prečo?) a teda $\psi(\alpha_1) = \alpha_i$ pre nejaké $i = 1, \ldots, d$. V takom prípade máme $(\varphi_i\psi^{-1})(\alpha_1) = \psi^{-1}(\varphi_i(\alpha_1)) = \psi^{-1}(\alpha_i) = \alpha_1$. Podľa (17) dostávame že $\varphi_i\psi^{-1}$ je prvkom $G(E : F(\alpha_1))$ a teda $\psi \in \varphi_i G(E : F(\alpha_1))$. Teda každý automorfizmus ktorý patrí do $G(E : F)$ patrí do nejakej triedy $\varphi_i G(E : F(\alpha_1))$. Dostávame takto rozklad

$$G(E : F) = \varphi_1 G(E : F(\alpha_1)) \cup \cdots \cup \varphi_d G(E : F(\alpha_1)).$$

Je zrejmé že tento rozklad je disjunktný a teda podľa indukčného predpoklado a (16) platí

$$|G(E : F)| = d|G(E : F(\alpha_1))| = d\frac{n}{d} = n.$$

□

Príklad 38. Pole $\mathbb{Q}(\sqrt[3]{2})$ nie je rozkladové pole polynómu a grupa $G(\mathbb{Q}(\sqrt[3]{2})$ je trivialna.

2.9 Galoisova grupa polynómu

Nech $f(x)$ je separabilný polynóm na poľom F a $F(\alpha_1, \ldots, \alpha_n)$ je jeho rozkladové pole. Grupu $G(F(\alpha_1, \ldots, \alpha_n) : F)$ budeme nazývať **Galoisovou grupou polynómu** $f(x)$ nad poľom F alebo aj **Galoisova grupa rovnice** $f(x) = 0$.

Príklad 39. Polynóm $X^4 + 1$ sa rozkladá

$$X^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1).$$

Teda jeho rozkladové pole je $\mathbb{Q}(\sqrt{2}, i)$. Galoisova grupa tohoto polynómu je izomorfná s $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Príklad 40. Dá sa dokázať, že Galoisova grupa polynómu $x^4 + 2$ má osem prvkov a je izomorfná s grupou symetrií štvorca.

Príklad 41. Uvažujme galoisovu grupu binomickej rovnice $x^p - 2 = 0$, kde $p > 2$ je prvočíslo. Rozkladové pole tejto rovnice je $\mathbb{Q}(w_p, \sqrt[p]{2})$. Vieme, že $[\mathbb{Q}(w_p, \sqrt[p]{2}) : \mathbb{Q}] = p(p-1)$. Ak G je galoisova grupa tejto rovnice tak vety 36 vyplýva, že $|G| = p(p-1)$. Ak $\varphi \in G$ tak $\varphi(w_p) = w_p^j, j = 1, \ldots, p-1$ a $\varphi(\sqrt[p]{2}) = w_p^k \sqrt[p]{2}, j = 0, \ldots, p-1$. Takýchto automorfizmov je najviac $p(p-1)$. Teda grupu G tvoria práve všetky automorfizmy $\varphi_{j,k}$ kde $\varphi_{j,k}(w_p) =$

$w_p^j, j = 1, \ldots, p-1$ a $\varphi_{j,k}(\sqrt[p]{2}) = w_p^k \sqrt[p]{2}, j = 0, \ldots, p-1$. Výpočtom, sa dá zistiť

$$\varphi_{j,k} \circ \varphi_{\ell,m} = \varphi_{j\ell \mod p, k\ell+m \mod p}.$$

Táto grupa teda nie je komutatívna.

Napriek tomu, že grupa v predošlom príklade je nekomutatívna, je to grupa rozšírenia pomocou odmocnín. Nasledujúci výsledok nám pomôže študovať štruktúru galoisovych grúp pomocou tzv. medzipolí a faktorovych grúp.

Veta 37. Nech F je pole, $f(x)$ je separabilný polynóm nad F a E je jeho rozkladové pole. Uvažujme separabilný polynóm$g(x)$ nad E. Označme E_1 jeho rozkladové pole. Potom
i) $G(E_1 : E)$ je normálna podgrupa $G(E_1 : F)$ a
ii) faktorová grupa $G(E_1 : F)/G(E_1 : E)$ je izomorfná s grupou $G(E : F)$

Dôkaz. Využijeme vetu 92 dokázanú v dodatku. Nech $f(x)$ má korene $\alpha_1, \ldots, \alpha_n$. Potom $E = F(\alpha_1, \ldots, \alpha_n)$ teda ak $a \in E$ tak podľa vety 16 existuje nejaký polynóm $r(x_1, \ldots, x_n)$, že $a = r(\alpha_1, \ldots, \alpha_n)$. Ak $\varphi \in G(E_1 : F)$ tak $\varphi(a) = \varphi(r(\alpha_1, \ldots, \alpha_n)) = r(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$. Ale $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ sú tiež korene polynómu $f(x)$. Preto $\varphi(a) \in E$. Tomuto izomorfizmu teda môžeme priradiť jeho zúženie

$$\Psi(\varphi) = \varphi|_E.$$

Je zrejmé, že takto definované zobrazenie $\Psi : G(E_1 : F) \to G(E : F)$ je homorfizmus. Je zrejmé, že $\mathbf{K}er(\Psi) = G(E_1 : E)$. Tým sme dokázali i). Každý F automorfizmus z $G(E : F)$ sa dá rozšíť na F automorfizmus z $G(E_1 : F)$. Preto Ψ ja surjektívny homorfizmus. Tvrdenie teda vyplýva z už spomenutej vety 92. □

Príklad 42. Keď sa vrátime k prikladu 41, vidíme, že

$$G(\mathbb{Q}(w_p, \sqrt[p]{2}) : \mathbb{Q}(w_p)) = \{\varphi_{1,k}; k = 0, \ldots, p-1\}.$$

Teda táto grupa je cyklická grupa izomorfná s aditívnou grupou $(\mathbb{Z}_p, +)$. Grupa $G(\mathbb{Q}(w_p) : \mathbb{G})$ je cyklická grupa izomorfná s multiplikatívnou grupou $(\mathbb{Z}_p^*, \cdot)$. Podľa vety 37 dostáveme

$$G(\mathbb{Q}(w_p, \sqrt[p]{2}) : \mathbb{Q})/\mathbb{Q}(w_p, \sqrt[p]{2}) : \mathbb{Q}(w_p)) \sim \mathbb{Z}_p^*.$$

Postup z predošlého príkladu sa dá jednoducho zovšeobecniť a dostávame:

Veta 38. Nech F je podpole poľa $\mathbb{C}$ a p je prvočíslo.
i) Ak w_p nepatrí do F galoisova grupa polynómu $x^p - 1$ nad F je izomorfná s multiplikatívnou grupou $\mathbb{Z}_p^*$.
ii) Ak $w_p \in F$ a $a \in F$ je taký prvok, že polynóm $x^p - a$ nemá koreň v F tak galoisova grupa tohoto polynómu je izomorfná s aditívnou grupou $\mathbb{Z}_p$.

Príklad 43. Nech $n \in \mathbb{N}$ a $m \in \mathbb{N}$ je nepárny deliteľ n. Dokážeme, že ak $r \in \mathbb{N}$ je také prirodzené číslo, že existuje prvočíslo $p|m$ také, že $\sqrt[p]{r}$ je iracionálne číslo tak $\sqrt[m]{r} \notin \mathbb{Q}(w_n)$. Nech to neplatí. Tak potom aj $\sqrt[p]{r} \in \mathbb{Q}(w_n)$. Je zrejmé, že $w_p \in \mathbb{Q}(w_n)$ a teda $\mathbb{Q}(w_p, \sqrt[p]{r}) \subset \mathbb{Q}(w_n)$. Galoisova grupa $G(\mathbb{Q}(w_p, \sqrt[p]{r}) : \mathbb{Q})$ je nekomutatívna. Pole $\mathbb{Q}(w_p, \sqrt[p]{r})$ je rozkladové pole polynómu $x^p - r$ a teda podľa vety 37 $G(\mathbb{Q}(w_p, \sqrt[p]{r}) : \mathbb{Q})$ je homorfným obrazom $G(\mathbb{Q}(w_n) : \mathbb{Q})$. Táto grupa je komutatívna a to je spor.

2.10 Riešiteľnosť v radikáloch

Ako sme spomínali v úvode existuje formula ktorá obsahuje druhé odmocniny a zlomky a vyjadruje všetky riešenia kvadratickej rovnice. Niečo podobné sa podarilo objaviť aj pre rovnice kubické a rovnice štvrtého stupňa. To vedie k nasledujúcemu pojmu:

Riešiteľnosť polynómu v radikáloch znamená to isté ako riešiteľnosť pomocou odmocnín. [11]Hovoríme, že polynomická rovnica $f(x) = 0$ je **riešiteľná v radikáloch** nad poľom F práve vtedy ak rozkladové pole polynómu $f(x)$ na poľom F sa dá vyjadriť v tvare $F(\alpha_1, \ldots, \alpha_n)$

[11]Výraz radikál pochádza pravdepodobne z latinského slova "radix", ktoré znamená "koreň". n tá odmocnina z nejaké prvku a je koreň rovnice $x^n - a = 0$. Vo viacerých jazykoch sa slová koreň a odmocnina nerozlišujú.

kde $F(\alpha_1, \ldots, \alpha_{i+1})$ je rozkladové pole nejakej binomickej rovnice prvočíselného stupňa nad poľom $F(\alpha_1, \ldots, \alpha_i)$ kde $i = 1, \ldots n-1$.

Podľa vety 16 to vlastne znamená

Veta 39. Separabilný polynóm $f(x) \in F[x]$ je riešiteľný v radikáloch práve vtedy ak každý jeho koreň sa dá vyjadriť v tvare $r(\sqrt[k_1]{\beta_1}, \ldots, \sqrt[k_n]{\beta_n})$ kde $\beta_1 \in F$ a $\beta_j = r_j(\sqrt[k_1]{\beta_1}, \ldots, \sqrt[k_{j-1}]{\beta_{j-1}}), j = 2, \ldots, n$ kde $r_j(\ldots)$ sú polynómy $j-1$ premenných a $r(\ldots)$ je vhodný polynóm n premenných nad F.

2.11 Riešteľné grupy

Hovoríme, že nejaká grupa G je **riešiteľná** práve vtedy ak existuje koneňá postupnosť podgrúp

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\} \tag{18}$$

taká, že G_{i+1} je normálna pogrupa G_i a faktorová grupa G_i/G_{i+1} je komutatívna pre $i = 0, \ldots, n-1$.

Príklad 44. Každá konečná komutatívna grupa je riešiteľná.

Príklad 45. Podgrupa riešiteľnej grupy je riešiteľná.

Príklad 46. Grupa $G(\mathbb{Q}(w_p, \sqrt[p]{2}) : \mathbb{Q})$ je podľa prikladu 42 riešiteľná.

Príklad 47. Grupa $\mathbf{S}_3$ je riešiteľná.

Príklad 48. Ak G_1, G_2 sú riešiteľné grupy, tak aj grupa $G_1 \times G_2$ je riešiteľná.

Veta 40. Ak grupa G_1 je riešiteľná a grupa G_2 je jej homomorfný obraz tak G_2 je riešiteľná

Dôkaz. Ak $\Psi : G_1 \to G_2$ surjektívny homorfizmus a $H \subset G_1$ je normálna podgrupa a G_1/H je komutatívna grupa tak aj $\Psi(H)$ je normálna podgrupa G_2 a $G_2/\Psi(H)$ je komutatívna grupa. □

Príklad 49. Z predošlej vety vyplýva, že ak grupa G je riešiteľná a H je jej normálna podgrupa tak aj faktorová grupa G/H je riešiteľná.

Veta 41. Ak $f(x)$ je separabilný polynóm nad F a polynomická $f(x) = 0$ je riešiteľná v radikáloch tak aj jej galoisova grupa nad poľom F je riešiteľná.

Dôkaz. Nech $E = F(\alpha_1, \ldots, \alpha_n)$ rozkladové pole polynómu $f(x)$. Položme $F_0 = F$ a $F_i = F(\alpha_1, \ldots, \alpha_i), i = 1, \ldots, n$. K postupnosti polí

$$F = F_0 \subset F_1 \subset \cdots \subset F_n = E$$

môžeme uvažovať postupnosť grúp

$$G(E : F) \supset G(E : F_1) \supset \cdots \supset G(E : F_n) =$$

$$= G(E : E) = \{id\}.$$

Podľa vety 37 dostávame že $G(E : F_{i+1})$ je normálna podgrupa grupy $G(E : F_i)$ a faktorová grupa $G(E : F_i)/G(E : F_{i+1})$ je izomorfná s grupou $G(F_{i+1}/F_i)$ pre $i = 0, \ldots, n-1$. Z vety 38 vyplýva že grupa $G(F_{i+1}/F_i)$ je cyklická a teda komutatívna. □

2.12 Grupy permutácií

Každému automorfizmu φ z galoisovej grupy nejakého separabilného polynómu s koreňmi $\alpha_1, \ldots, \alpha_n$ môžeme jednoznačne priradiť permutáciu kore- ňov $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$. Túto permutáciu môžeme stotožniť s permutáciou $\pi_\varphi \in \mathbf{S}_n$ kde

$$\pi_\varphi(i) = j \Longleftrightarrow \varphi(\alpha_i) = \alpha_j.$$

Ľahko sa preverí , že zobrazenie $\varphi \to \pi_\varphi$ je injektívny homomorfizmus. Teda platí

Veta 42. Grupa $G(F(\alpha_1, \ldots, \alpha_n) : F)$ je izomorfná s nejakou podgrupou grupy $\mathbf{S}_n$.

Príklad 50. Galoisova grupa polynóm $x^2 - 3$ na poľom $\mathbb{Q}$ je izomorfná s grupou $\mathbf{S}_2$.

Príklad 51. Galoisova grupa z príkladu 33 má šesť prvkov. Je izomorfná s nejakou podgrupou grupy $\mathbf{S}_3$, a preto sa táto musí rovnať celej grupe $\mathbf{S}_3$.

Príklad 52. Polynóm $(x^2-2)(x^2-3)$ ma rozkladové pole $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Preto galoisova grupa tohoto polynómu je izomorfná s grupou

$$\left\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2134\end{pmatrix},\begin{pmatrix}1234\\1243\end{pmatrix},\begin{pmatrix}1234\\2143\end{pmatrix}\right\}.$$

Príklad 53. Rozkladove pole polynómu x^5-1 nad poľom $\mathbb{Q}$ je $\mathbb{Q}(w_5)$ jeho galoisova grupa je izomofná s

$$\left\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2413\end{pmatrix},\begin{pmatrix}1234\\3142\end{pmatrix},\begin{pmatrix}1234\\4321\end{pmatrix}\right\}.$$

Výpočtom sa dá preveriť, že táto grupa je generovaná napríklad permutáciou $\binom{1234}{2413}$.

Príklad 54. Ak $f(x)\in\mathbb{Q}[x]$ je ireducibilný separabilný polynóm ktorý má práve dva komplexné korene, tak jeho galoisova prupa je izomorfná s grupou, ktorá okrem iných prvkov obsahuje aspoň jednu transpozíciu. Je to permutácia, ktorá zodpovedá zobrazeniu $z\to\overline{z}$, teda komplexné číslo zobrazíme do komplexne združeného.

2.13 Cauchyho veta

Štúdium grúp permutácií nám uľahčí nasledovné tvrdenie, ktoré je známe ako Cauchyho veta. Ide o jednoduchší prípad tzv. Sylowovych viet.

Veta 43. Ak G je konečná grupa a prvočíslo p delí $|G|$ tak G obsahuje prvok rádu p.

Dôkaz. Nech M je množina všetkých usporiadaných $p-$ tíc $[x_1, \ldots, x_p]$ ktoré spľňajú rovnosť

$$x_1 \cdot \cdots \cdot x_p = e$$

kde $x_i \in G, i = 1, \ldots, p$ a e je neutrálny prvok grupy G. Ak $[x_1, \ldots, x_p] \in M$ tak

$$x_1 \cdot \cdots \cdot x_{p-1} = x_p^{-1}$$

a teda aj$[x_p, x_1, \ldots, x_{p-1}] \in M$. Teda prvky M sa dajú otáčať "do kruhu". Môžeme preto definovať bijektívne zobrazenie $T : M \to M$ kde

$$T([x_1, \ldots, x_p]) = [x_p, x_1, \ldots, x_{p-1}].$$

Je zrejmé, že pre každé $\mathbf{x} \in M$ platí $T^p(\mathbf{x}) = \mathbf{x}$. Označme pre $\mathbf{x} \in M$ symbolom $j(\mathbf{x})$ najmenšie také $j = 1, \ldots, p$ pre ktoré $T^j(\mathbf{x}) = \mathbf{x}$ [12]. Pomocou delenia so zvyškom sa dá dokázať že $j(\mathbf{x})|p$ pre $\mathbf{x} \in M$. Preto sú len dve možnosti :$j(\mathbf{x}) = 1$ alebo $j(\mathbf{x}) = p$. Ak označíme $((\mathbf{x})) = \{T^j(\mathbf{x}); j =$

[12] Táto množina sa zvykne nazývať aj orbita prvku x pri iteráciach zobrazenia T

$1, \ldots, p\}$ tak $|((\mathbf{x}))| = p$ alebo $|((\mathbf{x}))| = 1$. Tieto množiny sú disjunktné a ich zjedontením je celá množina M. Preto

$$|M| = kp + \ell \tag{19}$$

kde k označuje počet tých $((\mathbf{x}))$ pre ktoré $|((\mathbf{x}))| = p$ a ℓ tých pre ktoré $|((\mathbf{x}))| = 1$. Usporiadaná $p-$ tica $[e, \ldots, e]$ patrí do M a teda $\ell \geq 1$. Prvky množiny M dostaneme tak, že prvých $p-1$ zložiek danej $p-$ tice vyberieme z G a posledný potom vypočítame tak spľňal danú rovnosť. Teda $|M| = |G|^{p-1}$. Preto hodnota $|M|$ je deliteľná p. Z toho vyplýva podľa (19), že $p|\ell$. Potom ale musí byť $\ell > 1$. Teda existuje $\mathbf{x} \neq [e, \ldots, e]$ pre ktoré $j(\mathbf{x}) = 1$. Potom $\mathbf{x} = [x, \ldots, x]$ pre nejaké $x \in G, x \neq e$ a teda $x^p = e$. Teda prvok x má rád p. □

Príklad 55. Z predošlej vety vyplýva, že každá konečná komutatívna grupa rádu $p_1 \cdot \cdots \cdot p_k$ kde $p_i, i = 1, \ldots, k$ sú rôzne prvočísla je cyklická.

Príklad 56. Ak G je grupa rádu pq kde $q < p$. Ak $a \in G$ je prvok rádu p tak každý prvok rádu p je mocninou a. Uvažujme a_1 - nejaký prvok rádu p. Môzeme utvoriť triedy $[a], a_1[a], \ldots a_1^{p-1}[a]$. Niektoré z týchto tried musia byť rovnaké pretože grupa G sa rozkladá na q tried podľa $[a]$. Teda pre nejaké $i < j < p$ platí $a_1^i[a] = a_1^j[a]$. Z toho vyplýva $a_1^{j-i} \in [a]$. Pretozže $(j - i, p) = 1$ po umicnení na vhodný exponent dostávame $a_1 \in [a]$.

Príklad 57. Ak $p > q$ a $p \not\equiv 1 \pmod{q}$ tak grupa rádu pq je cyklická. Dokáže sa to pomocou vety 43 a predchádzajúceho prikladu. Nech a je prvok rádu p a b je prvok rádu q. Ak dokážeme, že tieto prvky komutujú tak ab je generátor G. To, že komutujú je ekvivalentné rovnosti

$$bab^{-1} = a. \tag{20}$$

Prvok bab^{-1} je rádu p a teda podľa predchádzajúceho príkladu $bab^{-1} = a^r$ kde $r \in \{1, \ldots, p-1\}$. Potom $(bab^{-1})^r = a^{r^2}$, teda $ba^r b^{-1} = a^{r^2}$ a to znamená $b^2ab^{-2} = a^{r^2}$. Takto postupne dostaneme $b^m ab^{-m} = a^{r^m}$, pre $m \in \mathbb{N}$. Ak dosadíme $m = q$ dostávame $a = a^{r^q}$ a teda $r^q \equiv 1 \pmod{p}$. V prípade $k \neq 1$ by sme podľa Malej fermatovej vety dostali $q|p-1$ a to je spor. Preto napriklad grupa ktorá má 15 prvkov je cyklická. Ale 6 prvková grupa cyklická byť nemusí lebo nie je splnený jeden z predpokladov.

2.14 Neriešiteľné grupy

Veta 44. Ak G je podgrupa $\mathbf{S}_p$, p je prvočíslo, a $p||G|$ tak G obsahuje cyklus dĺžky p.

Dôkaz. Podľa predošlej vety G obsahuje permutáciu rádu p. Ak by daná permutácia bola zložená z viac ako jedného cyklu, tak jej rád by nebol deliteľný p lebo by to bol najmenší spoločný násobok čísel menších ako p. □

Veta 45. Ak p je prvočíslo a G je podrupa $\mathbf{S}_p$ ktorej rád je deliteľný p a obsahuje aspoň jednu transpozíciu tak $G = S_p$.

Dôkaz. Podľa predošlej vety G obsahuje aspon jeden cyklus dĺžky p. Preto ak obsahuje transpozíciu tak podľa vety 102 v Doplnkoch dostávame $G = \mathbf{S}_p$. □

Veta 46. Ak $p \geq 5$ je prvočíslo a $f(x)$ je ireducibilný polynóm nad poľom $\mathbb{Q}$ stupňa p ktorý má práve dva komplexne korene, tak jeho galoisova grupa nad poľom $\mathbb{Q}$ je izomorfná s grupou permutácí $\mathbf{S}_p$.

Riešiteľnosť polynomickej rovnice v radikáloch sme charakterizovali pomocou riešteľnosti jej Galoisovej grupy. Ako vidíme z predošlej vety niektoré z týchto grúp sú izomorfné s celou grupou S_m. Preto pri hľadaní rovnice neriešiteľnej v radikáloch nám pomôže nasledujúci výsledok:

Veta 47. Ak $m \in \mathbb{N}$ je prirodzené číslo väčšie ako 4 tak grupa permutácií $\mathbf{S}_m$ nie je riešiteľná.

Tvrdenie je dôsledkom trochu všeobecnejšieho faktu:

Lema 1. Ak G je pogrupa $\mathbf{S}_m, m \geq 5$ ktorá obsahuje všetky cykly dĺžky 3 a $H \subset G$ je taká normálna podgrupa G, že faktorová grupa G/H je komutatívna tak aj H obsahuje všetky cykly dĺžky 3.

Dôkaz. Z predpokladu komutatívnosti G/H vyplýva

$$(\pi_1 H)(\pi_2 H) = (\pi_2 H)(\pi_1 H)$$

a teda $\pi_1\pi_2 H = \pi_2\pi_1 H$, pre $\pi_1, \pi_2 \in H$. To znamená

$$\pi_1\pi_2(\pi_2\pi_1)^{-1} = \pi_1\pi_2\pi_1^{-1}\pi_2^{-1} \in H. \tag{21}$$

Nech (a_1, a_2, a_3) je nejaký cyklus z $\mathbf{S}_m$. Podľa predpokladu $m \geq 5$ a teda dané permutácie pôsobia na množine ktorá obsahuje ešte aspoň dva rôzne prvky a_4, a_5. Grupa G teda obsahuje cykly $(a_1, a_5, a_2), (a_5, a_3, a_2)$. Ak v (21) dosadíme $\pi_1 = (a_1, a_5, a_2), \pi_2 = (a_5, a_3, a_2)$ dostávame po úprave $(a_1, a_2, a_3) \in H$. □

Dôkaz vety 47. Podľa lemy 1 ak G_n je podgrupa $\mathbf{S}_m$ ktorá obsahuje všetky cykly dĺžky 3 a G_{n+1} je normálna podgrupa G_n taká, že faktorová grupa G_n/G_{n+1} je komutatívna, tak G_{n+1} tiež obsahuje všetky cykly dĺžky 3. Preto nikdy nemôže nastať prípad $G_{n+1} = \{id\}$ ako je to požadované v (18). □

Príklad 58. Žiadna podgrupa $\mathbf{S}_m, m \geq 5$, ktorá obsahuje všetky cykly dĺžky 3 nie je riešiteľná.

Z vety 40 a viet 46, 47 dostávame

Veta 48. Ak $p \geq 5$ je prvočíslo a $f(x)$ je ireducibilný polynóm nad poľom $\mathbb{Q}$ stupňa p ktorý má práve dva komplexne korene, tak polynomická rovnica $f(x) = 0$ nie je riešiteľná v radikáloch nad poľom $\mathbb{Q}$.

2.15 Eisensteinovo kritérium ireducibility

Nasledujúci výsledok známy pod názvom Eisensteinovo kritérium ireducibility, nám umožní konštruovať ireducibilné polynómy s vlastnosťami, ktoré budeme potrebovať.

Veta 49. Nech $f(x) = a_n x^n + \cdots + a_0$ je polynóm s celočíselnými koeficientami. Ak existuje prvočíslo p také, že $p \nmid a_n$ a $p|a_j$ pre $j = 0, \ldots, a_{n-1}$ a $p^2 \nmid a_0$, tak polynóm $f(x)$ je ireducibilný nad $\mathbb{Q}$.

13

Polynóm $g(x) \in \mathbb{Z}[x]$ sa nazýva **primitívny** vtedy a len vtedy ak najväčší spoločný deliteľ jeho koeficientov je 1.

Lema 2. Ak $g_1(x), g_2(x)$ sú primitívne polynómy tak aj $g_1(x)g_2(x)$ je primitívny polynóm.

Dôkaz. Nech $g_1(x)g_2(x)$ nie je primitívny polynóm. Potom existuje prvo- číslo p, ktoré deí všetky jeho koeficienty. Preto pre redukciu modulo p plati

$$\overline{g_1(x)g_2(x)} = 0$$

[13] Tento výsledok nesie názov po nemeckom matematikovi menom Ferdinand Gotthold Max Eisenstein (1823 – 1852). Pred ním ho však dokázal iný nemecký matematik Theodor Schonemann (1812 - 1968).

a teda

$$\overline{g_1(x)} \cdot \overline{g_2(x)} = 0.$$

Preto $\overline{g_1(x)} = 0$ alebo$\overline{g_2(x)} = 0$. Z toho vyplýva, v ze p delí všetky koeficienty $g_1(x)$ alebo $g_2(x)$ a to je spor lebo sme predopokladali, že obidva sú primitívne. □

Lema 3. Ak polynóm $h(x) \in \mathbb{Z}[x]$ je reducibilný nad $\mathbb{Q}$ tak je reducibilný aj v $\mathbb{Z}[x]$.

Dôkaz. Nech $h(x) = h_1(x)h_2(x)$ kde $h_1(x), h_2(x) \in \mathbb{Q}[x]$. Oba polynómy môžeme vyjadrit v tvare

$$h_1(x) = \frac{p_1 h_3(x)}{r_1},\ h_2(x) = \frac{p_2 h_4(x)}{r_1}$$

kde polynómy $h_3(x), h_4(x)$ sú primitívne a $p_1, p_2, r_1, r_2 \in \mathbb{Z}$ a $(p_1, r_1) = 1, (p_2, r_2) = 1$. Potom po dosadení do rovnosti pre $h(x)$ a úprave dostávame

$$r_1 r_2 h(x) = p_1 p_2 h_3(x) h_4(x). \tag{22}$$

Podľa Lemy 2 dostávame, že $h_3(x)h_4(x)$ je primitívny polynóm. Preto z podmienok $(p_1, r_1) = 1, (p_2, r_2) = 1$ dostáveme pomocou (22) $r_1 | p_2, r_2 | p_1$. Teda $p_2 = p_2' r_1, p_1 = p_1' r_2$. Po dosadení do (22) a vykrátení číslami r_1, r_2 máme

$$h(x) = p_1' p_2' h_3(x) h_4(x).$$

□

Dôkaz vety 49. Nech $f(x) = f_1(x)f_2(x)$, kde stupne daných polynómov sú aspoň 1. Podľa Lemy 3 môžeme predpokladať že $f_1(x), f_2(x) \in \mathbb{Z}[x]$. Keď tieto polynómy zredukujeme modulo p dostávame

$$(a_n \mod p)x^n = \overline{f_1(x)} \cdot \overline{f_2(x)},$$

pričom hodnota $a_n \mod p$ je nenulová. Preto $\overline{f_1(x)} = ax^j, \overline{f_1(x)} = bx^{n-j}, j \geq 1, n - j \geq 1$. Z toho vyplýva, že konštatné koeficienty polynómov $f_1(x), f_2(x)$ sú deliteľné p a teda $p^2|a_0$ čo je spor. □

Príklad 59. Pomocou vety 49 sa tiež dá dokázať, že ak p je pre pročíslo, tak polynóm

$$f(x) = x^{p-1} + x^{p-2} + \cdots + 1,$$

je ireducibilný. Stačí si uvedomiť , že

$$f(x) = \frac{x^p - 1}{x - 1}$$

a teda ak označíme $x = y + 1$ tak

$$f(y+1) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{p-1} y^{p-2} + \cdots + p.$$

Preto $f(y + 1)$ ako polynóm neurčitej y je ireducibilný podľa Eisensteinovho kritéria ireducibility. Teda aj $f(x)$ je ireducibilný. Je zrejmé, že v tomto prípade $f(x) = \Phi_p(x)$.

Príklad 60. Polynóm $x^5 - 5x + 10$ je ireducibilný.

Príklad 61. Ak v predpokladoch vety 49 zameníme podmienku $p^2 \nmid a_0$ podmienkou $p^3 \nmid a_0$ môžeme rovnakým spôsobom odvodiť , ze $f(x)$ sa nedá vyjadriť ako súčin troch polynómov stupňa aspoň jedna, ktoré patria do $\mathbb{Q}[x]$.

Normálne rozšírenie. Pole $E \supset F$ sa nazýva **normálnym rozšírením** poľa F práve vtedy ak každý polynóm ireducibilný nad F má v poli E alebo všetky korene alebo ani jeden koreň.

Veta 50. Rozkladové pole separabilného polynómu nad poľom F je normálne rozšírenie poľa F.

Dôkaz. Nech $f(x)$ je separabilný polynóm nad poľom F a E je jeho rozkladové pole. Predpokladajme, že nejaky polynóm $g(x) \in F[x]$ ireducibilý nad F má korene β a β_1. Podľ vety 33 existuje izomorfizmus $\varphi_\beta : F(\beta) \to F(\beta_1)$ taký, že pre $a \in F$ plati $\varphi_\beta(a) = a$ a $\varphi_\beta(\beta) = \beta_1$. Ak $\beta \in E$ tak $\beta = p(\alpha_1, \ldots, \alpha_k)$ kde p je polynóm k neurčitých a $\alpha_1, \ldots, \alpha_k$ sú všetky korene polynómu $f(x)$. Preto $\beta_1 = p(\varphi_\beta(\alpha_1), \ldots, \varphi_\beta(\alpha_k))$. Hodnoty $\varphi_\beta(\alpha_1), \ldots,$
$\varphi_\beta(\alpha_k)$ sú znovu korene polynómu $f(x)$ a teda $\beta_1 \in E$. $\square$

Veta 51. Nech $E \subset \mathbb{C}$ je rozkladové pole nejakého separabilného polynómu nad poľom F. Potom pre každé $\alpha \in E$ platí

$$\alpha \in F \iff \forall \psi \in G(E : F); \psi(\alpha) = \alpha.$$

Dôkaz. Nech $\alpha \in E \setminus F$. Potom α_1 má nejaký minimálny polynóm $f(x) \in F(x)$, stupeň tohoto polynómu ja aspoň 2. Teda tento polynóm má ešte jeden koreň α_1 rôzny od α. Podľa predošlej vety máme $\alpha_1 \in E$. Podľa vety 33 existuje izomorfizmus $\varphi_\alpha : F(\alpha) \to F(\alpha_1)$ taký, že $\varphi_\alpha(\alpha) = \alpha_1$ a $\varphi_\alpha(a) = a$ pre $a \in F$. Podľa vety 34 teda existuje izomorfizmus $\psi \in G(E : F)$ taký, že $\psi(\alpha) = \alpha_1 \neq \alpha$. □

2.16 Tranzitívnosť grupy

Ak G je nejaká grupa bijekcí na istej množine M tak hovoríme, že je **tranzitívna** na nejakej podmnožine $S \subset M$ práve vtedy, keď pre každú dvojicu prvkov $s_1, s_2 \in S$ existuje bijekcia $\pi \in G$ taká, že $\pi(s_1) = s_2$.

Veta 52. Nech $f(x)$ je polynóm separabilný nad poľom F a E je jeho rozkladové pole. Tento polynóm je ireducibilný práve vtedy, keď grupa $G(E : F)$ je tranzitívna na množine koreňov $f(x)$.

Táto veta je dôsledok nasledujúceho tvrdenia:

Veta 53. Nech E je rozkladové pole nejakého separabilného polynómu nad poľom F. Predpokladajme, že $\alpha \in E$. Označme

$$\{\alpha_1, \ldots, \alpha_k\} = \{\varphi(\alpha); \varphi \in G(E : F)\}.$$

Potom polynóm

$$g(x) = (x - \alpha_1) \dots (x - \alpha_k)$$

patrí do $F[x]$ a je ireducibilný.

Dôkaz. Polynóm $g(x)$ si môžeme vyjadriť v tvare

$$g(x) = x^k + a_{k-1}x^{k-1} + \dots + a_0,$$

kde $a_j = (-1)^j \sigma_{k-j}, j = 1, \dots, k-1$ a $\sigma_i, i = 1, \dots k$ sú elementarne symetrické polynómy od $\alpha_1, \dots, \alpha_k$. Z tohoto dôvodu platí

$$\varphi(a_j) = (-1)^j \varphi(\sigma_{k-j}) = (-1)^j \sigma_{k-j} = a_j, j = 0, \dots, k-1.$$

Preto podľa vety 51 dostávame $a_j \in F$.

Označme $h(x) \in F[x]$ minimálny polynóm prvku α nad poľom F. Potom $h(x)$ je ireducibilný a $\alpha_1, \dots, \alpha_k$ sú korene $h(x)$, teda $h(x) = cg(x)$ pre vhodné $c \in F$. □

Príklad 62. Rozkladové pole polynómu $(x^2 - 2))(x^3 - 3)$ obsahuje čísla $\sqrt{2}, -\sqrt{2}, \sqrt[2]{3}, w_3\sqrt[3]{3}, w_3^2\sqrt[3]{3}$. Pre každý izomorfizmus $\varphi \in G(E : \mathbb{Q})$ platí $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Teda táto grupa nie je tranzitívna na množine koreňov tohoto polynómu.

2.17 Norma prvku

Ak E je normálne rozšírenie poľa F a $\alpha \in E$ tak hodnotu

$$\mathcal{N}_F(\alpha) = \prod_{\varphi \in G(E:F)} \varphi(\alpha)$$

budeme nazývať **normou** prvku α nad poľom F.

Príklad 63. Norma prvku $a + b\sqrt{2} \in Q(\sqrt{2})$ je rovná $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$.

Je zrejmé, že pre $\alpha_1, \alpha_2 \in E$ platí

$$\mathcal{N}_F(\alpha_1\alpha_2) = \mathcal{N}_F(\alpha_1)\mathcal{N}_F(\alpha_2), \tag{23}$$

pre každé $\varphi \in G(E : F)$ platí

$$\mathcal{N}_F(\alpha_1) = \mathcal{N}_F(\varphi(\alpha_1)) \tag{24}$$

a

$$\mathcal{N}_F(a) = a^{[E:F]} \tag{25}$$

pre ľubovoľné $a \in F$.

Veta 54. Pre každé $\alpha \in E$ platí $\mathcal{N}_F(\alpha) \in F$.

Dôkaz. Použijeme vetu 51. Ak $\psi \in G(E : F)$ tak $\{\psi \circ \varphi; \varphi \in G(E : F)\} = G(E : F)$. Preto

$$\psi(\mathcal{N}_F(\alpha)) = \prod_{\varphi \in G(E:F)} (\psi \circ \varphi)(\alpha) = \prod_{\varphi \in G(E:F)} \varphi(\alpha) = \mathcal{N}_F(\alpha),$$

a teda podľa vety 51 dostávame $\mathcal{N}_F(\alpha) \in F$. □

Veta 55. Nech G je grupa a $n \in \mathbb{N}$. Predpokladajme, že $\mathcal{X}_1, \ldots, \mathcal{X}_n$ su rôzne homomorfizmy G do multiplikatívnej grupy nejakého poľa F. Potom pre $a_1, \ldots, a_n \in F$ platí

$$a_1\mathcal{X}_1 + \cdots + a_n\mathcal{X}_n = 0 \Rightarrow a_1 = 0, \ldots, a_n = 0.$$

Dôkaz. Budeme postupovať indukciou podľa n. Ak $a_1\mathcal{X}_1 = 0$ tak $a_1 = a_1\mathcal{X}_1(e) = 0$. Predpokladajme, že veta platí pre $n-1$. Nech

$$a_1\mathcal{X}_1 + \cdots + a_n\mathcal{X}_n = 0.$$

Predpokladajme, že $x \in G$ a $y \in G$ je taký prvok, že $\mathcal{X}_n(y) \neq \mathcal{X}_{n-1}(y)$. Potom

$$a_1\mathcal{X}_1(x) + \cdots + a_n\mathcal{X}_n(x) = 0 \tag{26}$$

ale aj

$$a_1\mathcal{X}_1(xy) + \cdots + a_{n-1}\mathcal{X}_{n-1}(xy) + a_n\mathcal{X}_n(xy) = 0$$

teda

$$\sum_{i=1}^{n-1} a_i\mathcal{X}_1(x)\mathcal{X}_i(y) + a_n\mathcal{X}_n(x)\mathcal{X}_n(y) = 0.$$

Ak rovnosť (26) vynásobíme $\mathcal{X}_n(y)$ a odčítame od poslednej rovnosti dostávame

$$\sum_{i=1}^{n-1} a_i\mathcal{X}_i(x)(\mathcal{X}_1(y) - \mathcal{X}_n(y)) = 0$$

pre každé $x \in G$. To znamená

$$\sum_{i=1}^{n-1} a_i(\mathcal{X}_i(y) - \mathcal{X}_n(y))\mathcal{X}_i = 0.$$

Hodnota $\mathcal{X}_{n-1}(y) - \mathcal{X}_n(y)$ je nenulová a preto z indukčného predpokladu dostávame $a_{n-1} = 0$. Rovnakým spôsobom sa dá dokázať , že $a_i = 0, i = 1, \ldots n-2$. Teda aj $a_n = 0$. □

Veta 56. Nech E je normálne rozšírenie poľa F také, že grupa $G(E : F)$ je cyklická. Označme jej generátor φ. Potom pre každé $\alpha \in E$ platí

$$\mathcal{N}_F(\alpha) = 1 \Longleftrightarrow \exists \gamma \in E; \alpha = \frac{\gamma}{\varphi(\gamma)}.$$

[14]

Dôkaz. Jedna implikácia vyplýva bezprostredne z rovností (23) a (24).

Nech grupa $G(E : F)$ má rád n. Je zrejmé, že v tomto prípade platí

$$\mathcal{N}_F(\alpha) = \alpha\varphi(\alpha)\varphi^2(\alpha)\ldots\varphi^{n-1}(\alpha).$$

[14]Tento výsledok je známy aj pod názvom Hilberova lema číslo 90. David Hilbert - nemecký matematik, 23. 1, 1862 – 14. 2. 1943. Patril medzi vedúce osobnosti matematiky. Jedna z jeho myšlienok bola aj vytvorit axiomatický prístup k rôznym matematickým teóriam.

Definujme

$$\psi_j(\alpha) = \alpha\varphi(\alpha)\dots\varphi^j(\alpha), j = 0, \dots, n-1.$$

Uvažujme zobrazenie $\lambda : E \to E$ definované nasledovne

$$\lambda = id + \psi_0(\alpha)\varphi + \psi_1\varphi^2 + \dots + \psi_{n-2}(\alpha)\varphi^{n-1}.$$

Podľa vety 55 existuje $\beta \in E$ také, že $\lambda(\beta) \neq 0$. Je zrejmé, že

$$\lambda(\beta) =$$

$$= \beta + \psi_0(\alpha)\varphi(\beta) + \psi_1(\alpha)\varphi^2(\beta) + \dots + \psi_{n-2}(\alpha)\varphi^{n-1}(\beta).$$

Ak uvážime, že $\psi_{n-1}(\alpha) = 1$ dostáveme

$$\alpha\varphi(\lambda(\beta)) = \psi_0(\alpha)\varphi(\beta) + \psi_1(\alpha)\varphi^2(\beta) + \dots + \psi^{n-1}(\alpha)\beta =$$

$$= \psi_0(\alpha)\varphi(\beta) + \psi_1(\alpha)\varphi^2(\beta) + \dots + \beta =$$

$$= \lambda(\beta).$$

Teda pre $\gamma = \lambda(\beta)$ dostávame

$$\alpha = \frac{\gamma}{\varphi(\gamma)}.$$

□

Veta 57. Nech pole F obsahuje w_n pre dané $n \in N$ a E je také rozšírenie poľa F že grupa $G(E : F)$ je cyklická rádu n. Potom existuje také $a \in F$, že $E = F(\sqrt[n]{a})$.

Dôkaz. Podľa rovnosti (25) dostávame, že $\mathcal{N}_F(w_n^{-1}) = 1$. Nech φ je generátor grupy $G(E : F)$. Podľa vety 56 dostávame, že existuje $\gamma \in E$ také, že

$$w_n^{-1} = \frac{\gamma}{\varphi(\gamma)}$$

a teda $\varphi(\gamma) = w_n\gamma$. Z toho vidíme že $\varphi^j(\gamma) = w_n^j\gamma$ pre $j = 0, \ldots, n-1$. Ak položíme $a = \mathcal{N}_F(\gamma)$ tak $a \in F$ a $\gamma^n = a$. Teda $\gamma = \sqrt[n]{a}$. Podľa vety 53 dostávame, že polynóm

$$x^n - a = (x - \gamma)(x - w_n\gamma)\ldots(x - w_n^{n-1}\gamma)$$

je ireducibilný nad F a teda $[F(\sqrt[n]{a}) : F] = n$. Ak si uvedomíme $[E : F] = n$ tak vidíme, že $E = F(\sqrt[n]{a})$. □

Grupa G sa nazýva **prostá** práve vtedy ak $\{e\}$ a G sú všetky jej normálne podgrupy. Veľmi jednoducho nahliadneme tento fakt:

Veta 58. Komutatívna grupa je prostá práve vtedy ak je cyklickou grupou prvočíselného rádu.

Túto skutoňosť použijeme na dôkaz :

Veta 59. Nech G je grupa a H je taká jej normálna podgrupa, že faktorová grupa G/H je komutatívna. Ak $H_1 \supset H$ je maximálna normálna podgrupa G v zmysle inklúzie, rôzna od G, ktorá obsahuje H tak G/H_1 je cyklická grupa prvočíselného rádu.

Dôkaz. Podľa vety 58 stačí dokázať že daná faktorová grupa je komutatívna a prostá. Komutativita vyplýva okamžite z toho, že $H \subset H_1$. Nech $A \subset G/H$ je podgrupa. Položme

$$\tilde{A} = \{g \in G; gH_1 \in A\}.$$

Je jasné, že $H_1 \subset \tilde{A}$. Jednoduchými úpravamim, sa dá preveriť že $\tilde{A}$ je normálna podgrupa G. Z maximality H_0 dostávame $H_1 = \tilde{A}$ alebo $G = \tilde{A}$. Preto $A = e$ alebo $A = G/H$. □

Veta 60. Ak G je konečná grupa a H je taká jej normálna podgrupa že faktorová grupa G/H je komutatívna tak existuje konečná postupnosť podgrúp $H = H_n \subset H_{n-1} \subset \dots H_1 \subset H_0 = G$ že
i) H_i je normálna podgrupa H_{i-1}, $i = 1, \dots n$ a
ii) faktorová grupa H_{i-1}/H_i je cyklická.

Z tohoto vyplýva bezprostredne:

Veta 61. Konečná grupa G je riešteľná vtedy a len vtedy ak existuje konečná postupnosť podgrúp $H_0 = G \supset H_1 \cdots \supset H_k = \{e\}$ taká, že
i) H_j je normálna podgrupa H_{j-1} pre $j = 1, \dots, k$
ii) Faktorová grupa H_{j-1}/H_j je cyklická pre $j = 1, \dots, k$.

Normálne podgrupy. Nech E je normálne konečné rozšírenie poľa F. Predpokladajme, že H je normálna podgrupa grupy $G(E:F)$. Položme

$$E_H = \{\alpha \in E; \forall \varphi \in H : \varphi(\alpha) = \alpha\}. \tag{27}$$

Veta 62. Predpokladajme, že F obsahuje pole $\mathbb{Q}$. Potom
i) E_H je normálne rozšírenie poľa F,
ii) E je normálne rozšírenie poľa E_H a
iii) $G(E:E_H) = H$.

Dôkaz. Nech $\psi \in G(E:F)$. Potom pre každý izomorfozmus $\varphi \in H$ platí $\psi\varphi\psi^{-1} \in H$. Teda ak $\alpha \in E_H$ tak $\psi\varphi\psi^{-1}(\alpha)(\alpha) = \alpha$. To znamená $\psi^{-1}(\varphi(\psi(\alpha))) = \alpha$ a teda $\varphi(\psi(\alpha) = \psi(\alpha)$. Z toho vyplýva, že $\psi(\alpha)$ spĺňa podmienku (27) a teda $\psi(\alpha) \in E_H$. Tým sme dokázali i).

Bod ii) vyplýva z toho že E je normálne rozšírenie F.

Určite platí $H \subset G(E:E_H)$. Preto na dôkaz iii) stačí dokázať $|H| \geq |G(E:E_H)|$. Podľa vety exiatuje taký prvok $\beta \in E$, že $E = E_H(\beta)$. Potom $|G(E:E_H)| = [E_H(\beta) : E_H]$. Nech $|H| = k$ a $H = \{\varphi_1, \ldots, \varphi_k\}$. Uvažujme polynóm

$$\begin{aligned} h(x) &= (x - \varphi_1(\beta)) \ldots (x - \varphi_k(\beta)) = \\ &= x^k + s_{k-1}x^{k-1} + \cdots + s_0. \end{aligned} \tag{28}$$

Koeficieny $s_j, j = 0, \ldots, k-1$ su hodnoty symetrických polynomov v $\varphi_1(\beta)$,

$\ldots \varphi_k(\beta)$ a teda pre každé $\varphi_i(s_j) = s_j, 0 \leq j < k, 1 \leq i \leq k$. Z toho vyplýva, že $s_j \in E_H$. Preto $h(x) \in E_H[x]$. Grupa H obsahuje aj neutrálny prvok, teda identické zobrazenie. Preto $h(\beta) = 0$. Z toho vyplýva, že minimálny polynóm prvku β nad E_H je deliteľom $h(x)$. Teda $[E_H(\beta) : E] \leq k$. □

Veta 63. Nech $F \subset C$ je pole, $f(x) \in F[x]$ je separabilný polynóm a E je jeho rozkladové pole nad F. Označme $n = [E : F]$. Ak F obsahuje w_n a grupa $G(E : F)$ je riešteľná tak rovnica $f(x) = 0$ je riešiteľná v radikáloch.

Dôkaz. Nech

$$G(E : F) = H_0 \supset H_1 \supset \cdots \supset H_k = \{id\},$$

je postupnosť podgrúp takých, že H_{i+1} je normálna podrgrupa H_i a grupa H_i/H_{i+1} cyklická. Položme $F_i = E_{H_i}$, $i = 0, \ldots k$. Potom podľa vety 62 E je normálne rozšírenie F_i a F_i je normálne rozšírenie $F, i = 0, \ldots k$. Naviac $G(E : F_i) = H_i$. Podlľa vety 37 dostávame

$$G(F_{i-1} : F_i) \simeq G(E : F_i)/G(E : F_{i+1})$$

a teda galoisova grupa $G(F_{i-1} : F_i)$ je cyklická. Z vety 57 preto vyplýva, že $F_{i-1} = F_i(\sqrt[m]{\alpha_{i-1}})$ kde $m = [F_{i-1} : F_i]$ a $\alpha_{i-1} \in F_i$. □

2.18 Wedderburnova veta

Usporiadanú trojicu $(T, +, \cdot)$ sa nazýva **teleso** práve vtedy ak $+$ a $\cdot$ sú binárne operácie na T pričom $(T, +)$ je komutatívna grupa, $(T \setminus \{0\}, \cdot)$ je grupa a pre $a, b, c \in T$ platí

$$a(b + c) = ab + ac, \ (b + c)a = ba + ca.$$

Teda na rozdiel od poľa sa nevyžaduje v tomto prípade komutatívnosť násobenia. Príkladom telesa, ktoré nie je pole je teleso kvaternionov.

V tejto časti dokážeme:

Veta 64. Každé konečné teleso je pole.

Tento výsledok súvisí s komutativitou grúp, preto začneme s niektorými faktami na túto tému.

Nech G je konečná grupa. Označme pre $a \in G$ symbolom C_a množinu všetkých prvkov $g \in G$ takých, že $ag = ga$. Množina C_a sa nazýva **centralizátor** prvku a. Prienik $C = \cap_{a \in G} C_a$ sa nazýva **centrum** grupy G. Pomocou úprav sa dá dkázať, že

Veta 65. i) C_a **je podgrupa** G **a**
ii) C **je podgrupa** G**.**

Príklad 64. Centrum grupy je určite normálna podgrupa. Dá sa dokázať, že grupa G je komutatívna práve vtedy keď faktorová grupa G/C je cyklická.

Príklad 65. Podľa príkladu 86 sa dá dokázať, že z riešiteľnosti grupy G/C vyplýva riešiteľnosť grupy G.

Na grupe G si môžeme definivať reláciu

$$a \sim b \Longleftrightarrow \exists g \in G; a = gbg^{-1}.$$

Aj v tomto prípade jednoducho overíme, že $\sim$ je relácia ekvivalencie na G. Ak $a \sim b$ tak prvky a, b sa nazývajú **konjugované**. Označme symbolom K_a triedu ekvivalencie ktorá obsahuje prvok a. Teda

$$K_a = \{gag^{-1}; g \in G\}. \tag{29}$$

Veta 66. Množina K_a obsahuje $\frac{|G|}{|C_a|}$ prvkov.

Dôkaz. Stačí dokázať, že existuje bijekcia medzi K_a a množinou tried rozkladu G/C_a. Triedy rozkladu majú tvar $gC(a)$, $g \in G$. Zostrojíme bijekciu $K_a \to G/C_a$.

Rovnosť $gag^{-1} = g_1 a g_1^{-1}$ práve vtedy keď $g_1^{-1} g a = a g_1^{-1} g$ a teda $g_1^{-1} g \in C_a$ to znamená $gC_a = g_1 C_a$. To znamená, že priradenie
$gag^{-1} \mapsto gC_a$ je bijekcia. □

Lema 2. Ak $q \in N, q > 1$ tak pre $m, n \in \mathbb{N}, m < n$ platí

$$q^m - 1 | q^n - 1 \Longrightarrow m | n.$$

Dôkaz. Ak $q^m - 1 | q^n - 1$ tak $q^m - 1 | q^n - 1 - (q^m - 1) = q^m(q^{n-m} - 1)$ a teda $q^m - 1 | q^{n-m} - 1$. Ak r je zvyšok n po delení m tak postupne dokážeme $q^m - 1 | q^r - 1$ a to je možné jedine v prípade $r = 0$. □

Dôkaz vety 64. Nech T je konečné teleso. Označme $G = T \setminus \{0\}$ je multiplikatívnu grupu. Ak budeme používať označenia ako v predošlom texte tak veľmi lahko nahliadneme, že množina $F = C \cup \{0\}$ obsahuje s každými dvomi prvkami aj ich súčet a teda tvorí pole. T preto môžeme považovať za vektorový priestor nad F. Z toho vyplýva

$$|T| = |F|^n$$

pre nejaké $n \in \mathbb{N}$. Veta bude dokázaná ak dokážeme, že $n = 1$. Rovnako ako to, že $C \cup \{0\}$ je pole sa dá preveriť, že $C_a \cup \{0\}$ je teleso. Preto táto množina je tiež vektorový priestor nad F. Z toho vyplýva

$$|C_a \cup \{0\}| = |F|^{n_a}.$$

Grupa G je disjunktnym zjednotením tied $K_a, a \in G$. Je zrejmé, že $a \in C \Leftrightarrow |K_a| = 1$. Preto podľa vety 66 dostávame

$$|G| = |C| + \sum_{K_a \in B} \frac{|G|}{|C_a|} \tag{30}$$

kde B je množina tých tried ekvivalencie $\sim$, ktoré majú

viac ako 1 prvok. To znamená

$$|F|^n - 1 = |F| - 1 + \sum_{[a]\in B} \frac{|F|^n - 1}{|F|^{n_a} - 1}. \tag{31}$$

Podľa Lagrangeovej vety dostávame že prirodzené číslo $|F|^{n_a}-1$ je deliteľom $|F|^n-1$, a tedy z lemy 2 vyplýva $n_a|n$, pretože $|F| > 1$. Z definície $\Phi_n(x)$ dostávame že polynóm $\frac{x^n-1}{x^{n_a}-1}$ je polynóm tvaru $h(x)\Phi_n(x)$, kde
$h(x) \in \mathbb{Z}[x]$. Z rovnosti (31) vyplýva teda, že

$$\Phi_n(|F|)||F| - 1. \tag{32}$$

Ak by platilo $n > 1$ tak $\Phi_n(x)$ je súčinom činiteľov tvar $x - w_n^k$ kde $(k, n) = 1$. V tom prípade

$$||F| - w_n^k| = \sqrt{\left(|F| - \cos\frac{2k\pi}{n}\right)^2 + \sin^2\frac{2k\pi}{n}} > |F| - 1$$

preto aj $\Phi_n(|F|) > |F| - 1$ a to je spor s (32). □

Príklad 66. Rovnosť (30) platí pre ľubovolnú konečnú grupu G. Ak $|G| = p^n$ kde p je prvočí slo a $n = 2, 3, \ldots$ tak $|C| = p^k$ pre vhodné $k \in \mathbb{N}$.

Príklad 67. Grupa rádu p^2 , kde p je prvočíslo, je komutatívna.

Príklad 68. Grupa rádu p^n je riešiteľná.

2.19 Euklidovské geometrické konštrukcie

Geometrická konštrukcia, ktorá sa dá vykonať konečným počtom krokov pri pomoci pravítka a kružidla sa nazýva **Euklidovská geometrická konštrukcia**. Ako sa môžeme domievať už podľa názvu, snaha o takéto konštrukcie siaha do doby Euklida teda do antických čias. Postupom času sa vyčlenili tri úlohy, ktoré sa nedarilo riešiť. Sú to **trisekcia uhlu, reduplikácia kocky a kvadratúra kruhu.** Nemožnosť prvých dvoch dá dokázať pomocou algebry. Vyplýva to z výsledku francúzskeho matematika menom Pierre Wantzel [15]. Pod trisekciou uhlu sa myslí Euklidovská konťrukcia, ktorá k ľubovoľnému uhlu dokáže zostrojiť uhol ktorého odchylka sa rovná jednej tretine pôvodného uhlu. Bisekcia uhlu teda rozdelenie na polovicu je dobre známa jednoduchá konštrukcia. Reduplikácia kocky znamená úlohu euklidovsky zostrojiť stranu kocky, ktorá by mala dvojnásobný objem ako daná kocka. Budeme sa týmto výsledkom zaoberať. Nerieštelnosť poslednej úlohy súvisí sa trancendentnosťou čísla π a metódami patrí skôr do matematickej analýzy.

Každý krok Euklidovskej geometrickej konštrukcie znamená zostrojenie priesečníku
a) dvoch priamok

[15] Pierre Laurent Wantzel (1814 – 1848) sa narodil v Paríži. V roku 1837 dokázal nemožnosť trisekcie uhlu a a reduplikácie kocky.

b) priamky a kružnice
c) dvoch kružníc.

V algebre kroku a) zodpovedá riešenie sú stavy dvoch lineárnych rovníc o dvoch neznámych.
Ak nejaká priamka prechádza bodmi $A = [a_1, a_2], B = [b_1, b_2]$ kde a_1, a_2 ,
b_1, b_2 sú prvkami nejaého poľa F, tak bod $[x, y]$ patrí do tejto priamky práve vtedy keď existuje t také , že

$$x = a_1 + t(a_1 - b_1), y = a_2 + t(a_2 - b_2)$$

ak z týchto rovností eliminujeme úpravami t dostávame že rovnica tejto priamky má tvar

$$Ax + By + C = 0, A, B, C \in F.$$

Teda priesečník s inou priamkou , ktorá tiež prechádza bodmi ktorých súradnice patria do poľa F spĺňa rovnice

$$Ax + By + C = 0, A_1x + B_1y + C_1 = 0,$$

kde $A, B, C, A_1, B_1, C_1 \in F$. Riešenie takejto sústavy rovníc sa hľadá pomocou sčítania, násobenia, delenia a ak x, y je ich riešením tak $x, y \in F$.

Kroku b) zodpovedá riešenie sú stavy lineárnej rovnice o dvoch nez- námych a kvadratickej rovnice o dvoch neznámych.

Nech nejaká kružnice má stred $[m, n], m, n \in F$ a polomer $r \in F$. Tak jej rovnica bude

$$(x - m)^2 + (y - n)^2 = r^2.$$

Ak hľadáme jej priesečníky s priamkou $Ax + By + C = 0, A, B, C \in F$, dajme tomu, že $A \neq 0$ tak môžeme dosadiť

$$x = \frac{-By - C}{A}$$

a dostávame kvadratickú rovnicu

$$\left(\frac{-By - C}{A} - m\right)^2 + (y - n)^2 = r^2.$$

Ak túto rovnicu upravíme a jej diskriminant označíme α tak $\alpha \in F$ a vidíme, že jej koreň y patrí do $F(\sqrt{\alpha})$.

Kroku c) zodpovedá riešenie sú stavy dvoch kvadratických rovníc o dvoch neznámych

$$(x - m)^2 + (x - n)^2 = r^2$$

a

$$(x - m_1)^2 + (x - n_1)^2 = r_1^2.$$

Teda

$$x^2 + 2xm + m^2 + y^2 + 2yn + n^2 = r^2$$
$$x^2 + 2xm_1 + m_1^2 + y^2 + 2yn_1 + n_1^2 = r_1^2.$$

Keď odčítame prvú od druhej vidíme, že táto sústava je ekvivalentná sústave

$$x^2 + 2xm + m^2 + y^2 + 2yn + n^2 = r^2$$

$$2x(m_2 - m_1) + m_2^2 - m_1^2 + 2y(n_2 - n_1) + n_2^2 - n_1^2 = r_2^2 - r_1^2.$$

Teda kvadratické členy v druhej vypadli a vlastne riešime rovnakú sústavu ako v bode 2.

Ak vychádzame z nejakého poľa F tak priesečník v prípade a) má súradnice znovu v poli F. V prípadoch b) a c) súradnice priesečníku patrí do poľa $F(\sqrt{\alpha})$ pre vhodné $\alpha \in F$. Wantzelov výsledok je

Veta 67. Bod $[x, y]$ sa dá zostrojiť vtedy a len vtedy ak existuje konečná postupnosť $\alpha_1, ..., \alpha_n$ že platí
a) $\alpha_1 \in Q, \alpha_k \in Q(\sqrt{\alpha_1})...(\sqrt{\alpha_{k-1}}), k = 2, ..., n-1$
b) $x, y \in Q(\sqrt{\alpha_1})...(\sqrt{\alpha_n})$.

Dôkaz. Jedna implikácia vyplýva z predošlých úvah. Opačná implikácia vyplýva z:

Lema 4. Predpokladajme, že vieme zostrojiť všetky body $[x, y]$ také že x, y patria do nejakého poľa F. Preto vieme zostrojiť všetky body $[a+b\sqrt{x}, c+d\sqrt{x}]$ kde $a, b, c, d \in F$.

Dôkaz. Môžeme predpokladať ,že $x > 0$. Ak zostrojíme úsečku AB dľžky $x + 1$, môžeme nad ňou zostrojiť polkružnicu. Uvažujme bod C na tejto úsečke taký, že

$|AC| = x$. Ak spustíme kolmicu na úsečku AB v bode C a označíme D jej priesečník s danou polkružnicou tak $|CD| = \sqrt{x}$. □

Veta 68. Nech F je pole. Ak kubický polynóm $f(x)$ s koeficientami z poľa F nemá koreň v F tak nemá ani koreň v $F(\sqrt{\alpha})$ pre $\alpha \in F$.

Dôkaz. Nech $c = a + b\sqrt{\alpha} \in F(\sqrt{\alpha})$. Potom c je koreňom polynómu

$$h(x) = x^2 - 2ax + a^2 - b^2\alpha.$$

(Prečo?). Polynóm $f(x)$ sa dá vydeliť so zvyškom polynómom $h(x)$ a dost- ávame rovnosť

$$f(x) = (x + a_1)h(x) + a_2x + a_3, a_1, a_2, a_3 \in F. \qquad (33)$$

Ak by c bolo koreňom $f(x)$ tak z poslednej rovnosti vyplýva

$$a_2c + a_3 = 0.$$

, Preto ak $a_2 \neq 0$ tak $c \in F$ a to je spor. Teda $a_2 = 0$ a preto aj $a_3 = 0$. Potom ale z (33) dostávame $f(-a_1) = 0$ a to je spor. □[16]

[16]Georg Mohr v roku 1672 a Lorenzo Mascheroni v roku 1797 dokázali, že každá konštrukcia ktorá sa dá vykonať pomocou pravítka a kružidla sa dá vykonať len pomocou kružidla. Myslí sa tým konštrukcia bodov. Teda nie narysovanie priamky. Tento výsledok je dnes známy ako Mohrova - Mascheroniho veta.

Postupnými krokmi sa dá odvodiť

Veta 69. Ak $f(x)$ je kubický polynóm s racionálnymi koeficientami ktorý nemá koreň v Q tak nemá koreň ani v poli $Q(\sqrt{\alpha_1})...(\sqrt{\alpha_n})$ kde $\alpha_1 \in Q$ a $\alpha_k \in Q(\sqrt{\alpha_1})...(\sqrt{\alpha_{k-1}}), k = 2, \dots n$, kde $n \in \mathbb{N}$.

Teda

Veta 70. Ak $f(x)$ je kubický polynóm s racionálnymi koeficientami ktorý nemá koreň v Q tak jeho korene sa nedajú euklidovsky zostrojiť.

Príklad 69. Hodnota $\sqrt[3]{2}$ je koreňom polynómu $x^3 - 2$ ktorý je ireducibilný nad $\mathbb{Q}$. Preto sa táto hodnota nedá zostrojiť euklidovsky. Tento fakt vysvetľuje tiež nemožnosť tzv. reduplikácie kocky - jednu z historických úloh.

Príklad 70. Teraz sa vrátime k skôr spomínanej trisekcii uhlu. Ak by bola možná trisekcia uhlu, tak by sa dal zostrojiť uhol 20^o. Pretože 60^o má uhol v rovnostrannom trojuholníku a ten by sa dal rozdeliť euklidovsky na tri rovnaké časti, teda jedna by mala 20^o. Ak by sa dal zostrojiť tento uhol tak by sa euklidovsky dala zostrojiť aj hodnota $\cos 20^o$. Vieme, že $\cos 60^o = \frac{1}{2}$. Ak si odvodíme formulu pre $\cos 3\alpha$ obasahujúcu iba $\cos \alpha$ dostaneme, že $\cos 20^o$ je koreňom ireducibilnej rovnice tretieho stupňa, teda podľa vety 70 sa zostrojiť nedá.

Príklad 71. Ak sa nedá zostrojiť uhol 20^o tak sa určite nedá zostrojiť ani uhol 1^o, 2^o, 5^o, 10^o. Vlastne sa dá povedať ak sa nedá zostrojiť m^o uhol tak sa nedá zostrojiť ani d^o uhol, kde $d|m$.

Príklad 72. Ak sa dá zostrojiť uhol $m_1^o, m_1 \in \mathbb{N}$ a m_2 je prirodzené číslo nesúdeliteľné s m_1 tak sa nedá zostrojiť uhol m_2^o.

Na záver tejto časti môžeme poznamenať že euklidovské konštrukcie používajú iba dva nástroje pravítko a kružidlo a ukázalo sa, že to je málo. Ukážeme to na nasledujúcom príklade:

Príklad 73. Predpokladajme, že dokážeme zostrojiť každý bod paraboly $y = x^2$. Pre každé dve racionálne čísla a, b vieme zostrojiť kružnicu so stredom $[x, y]$ a polomerom $\sqrt{a^2 + b^2}$. Teda množinu bodov $[x, y]$ kde

$$(x - a)^2 + (y - b)^2 = a^2 + b^2.$$

Ak dosadíme do tejto rovnice $y = x^2$, zostrojíme priesečník paraboly a tejto kružnice tak pri vhodnej voľbe a, b prídeme na to, že dokážeme zostrojiť aj $\sqrt[3]{2}$. Teda v tomto prípade stačí pridať parabolítko.

2.20 Pravidelné mnohouholníky

Antickí Gréci ovládali konštrukcie pravidelného trojuholníka inými slovami rovnostranného, štvoruholníka, teda štvorca a päťuholníka. Konštrukcia päťuholníka je uvedená v príklade 22. To vedie prirodzene na otázku konštrukcie pravidelného n - uholníka. Tento problém je 2000 rokov starý. Karl Friedrich Gauss v roku 1792 ako študent dokázal, že podmienka (34) uvedená nižšie, je postačujúca.

Príklad 74. Dá sa zostrojiť pravidelný sedemuholník? Ukážeme, že nie. Ak by sa dal zostrojiť tak by sa dal zostrojiť aj uhol $\frac{2\pi}{7}$. Teda by sa dali zostrojiť aj hodnoty $\cos\frac{2\pi}{7}$ a $\sin\frac{2\pi}{7}$. Teda podľa vety 67 by existovalo pole $F \supset \mathbb{Q}$ take, že $[F:\mathbb{Q}] = 2^k$ a $\cos\frac{2\pi}{7}, \sin\frac{2\pi}{7} \in F$. Potom ale $w_7 \in F(i)$. To znamená, že $\mathbb{Q}(w_7) \subset F(i)$. Preto by platilo $[\mathbb{Q}(w_7):Q]|[F(i):Q]$. To je spor pretože $[\mathbb{Q}(w_7):Q] = 6$ a $[F(i):Q]$ je mocnina 2. Teda pravidelný sedem uholník sa zostrojiť nedá.

Veta 71. Pravidelný n - uholník sa dá zostrojiť práve vtedy keď

$$n = 2^k p_1 \dots p_s \tag{34}$$

kde $k, s = 0, 1, 2, 3 \dots$ **a v prípade** $s \geq 1$ **sú** $p_j = 2^{m_j} + 1, j = 1, \dots, s$ **navzájom rôzne prvočísla väčšie ako 2.**

Dôkaz nutnosti podmienky (34). To že (34) je nutná podmienka na to aby sa pravidelný n uholník dal zostrojiť dokážeme rovnako ako a predošlom príklade. Je to práve vtedy keď sa dá zostrojiť uhol $\frac{2\pi}{n}$ a teda práve vtedy keď sa dajú zostrojiť hodnoty $\cos\frac{2\pi}{n}$ a $\sin\frac{2\pi}{n}$. Teda existuje pole $F \supset \mathbb{Q}$ také, že $[F:\mathbb{Q}] = 2^r$, pre vhodné $r \in \mathbb{N}$ a $\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n} \in F$. V takom prípade $w_n \in F(i)$ a teda $\mathbb{Q}(w_n) \subset F(i)$ a preto $[\mathbb{Q}(w_n):\mathbb{Q}] = 2^\ell$. To znamená, že $\phi(n) = 2^\ell$. Ak $n = 2^k p_1^{e_1} \dots p_s^{e_s}$ je kanonický rozklad, tak $\phi(p_j^{e_j}) = 2^{m_j}$. To je možné jedine vtedy keď $e_j = 1$ a $p_j = 2^{m_j} + 1$. □

Príklad 75. Ak máme zostrojený nejaký uhol α tak známou konštrukciou vieme zostrojiť uhol $\frac{\alpha}{2}$. Z algebrického pohľadu to vyplýva z rovnosti

$$\cos\frac{\alpha}{2} = \sqrt{\frac{1-\cos\alpha}{2}}.$$

Preto ak dá zostrojiť pravidelný n uholník tak sa dá zostrojiť uhol $\frac{2\pi}{n}$ a jeho rozpolením sa dá zostrojiť aj uhol $\frac{2\pi}{2n} = \frac{\pi}{n}$ a teda aj pravidelný $2n$ uholník.

Lema 5. Ak m_1, m_2 sú nesúdeliteľné prirodzené čísla a uhly $\frac{2\pi}{m_1}, \frac{2\pi}{m_2}$ sa dajú zostrojiť tak sa dá zostrojiť aj uhol $\frac{2\pi}{m_1 m_2}$

Dôkaz. Tvrdenie vyplýva z toho, že pre vhodné celé čísla n_1, n_2 platí $1 = n_1 m_1 + n_2 m_2$ a teda

$$\frac{2\pi}{m_1 m_2} = \frac{2\pi}{m_1 m_2} \cdot (n_1 m_1 + n_2 m_2) = \frac{2n_1\pi}{m_2} + \frac{2n_2\pi}{m_1}.$$

□

Príklad 76. Ak chceme zostrojiť pravidelný 15 - uholník stačí zostrojiť uhol $\frac{2\pi}{15}$. Zostrojíme rovnostranný trojuholník, teda uhol $\frac{2\pi}{3}$. Potom zostrojíme uhol $\frac{2\pi}{5}$. Odčítaním dostaneme

$$\frac{2\pi}{3} - \frac{2\pi}{5} = \frac{4\pi}{15}.$$

Rozpolením výsledného uhla dostaneme uhol $\frac{2\pi}{15}$.

Aby sme dokázali vetu 34 stačí dokázať už iba to že pravidelný p uholník sa dá zostrojiť v prípade keď $p = 2^\ell + 1$ je prvočíslo. Je to ekvivalentné s tým, že alebo uhol $\frac{2\pi}{p}$ sa dá zostrojit a to je ekvivalentné tomu že sa dá zostrojiť w_p. V tomto prípade je galoisova grupa $[\mathbb{Q}(w_p) : \mathbb{Q}]$ izomorfná s multiplikatívnou grupou poľa $\mathbb{Z}_p$ a teda je to cyklická grupa rádu 2^ℓ.

Veta 72. Nech F je normálne konečné rozšírenie poľa $\mathbb{Q}$. Ak $H \subset G(F : \mathbb{Q})$ taká normálna podgrupa, že $|G(F : \mathbb{Q})/H| = 2$ tak F_H je také normálne rozšírenie $\mathbb{Q}$, že existuje $a \in F_H$, že $F = F_H(\sqrt{a})$.

Dôkaz. Pole F je konečné rozšírenie poľa racionálnych čísel tak je konečné a normálne rozšírenie aj poľa F_H. Podľa vety 2.17 existuje prvok $b \in F$ taký, že $F = F_H(b)$. Podľ vety platí $[F : F_H] = 2$. Preto mnimálny polynóm prvku b nad F_H je kvadratický. Z toho vyplýva

$$b = a_1 + \sqrt{a}$$

kde $a_1, a \in F_H$ a $\sqrt{a} \notin F_H$. Preto $F = F_H(\sqrt{a})$. □

Komplexné číslo $x + iy$ sa dá euklidovsky zostrojiť práve vtedy keď sa dá zostrojiť bod $[x, y]$. Rovnako platí , že komplexné číslo $z = |z|(\cos\alpha + i\sin\alpha)$ sa dá euklidovsky zostrojiť práve vtedy keď sa dá euklidovsky zostrojiť $|z|$ a uhol α. Ďalej budeme používať

Lema 6. Ak sa dajú zostrojiť komplexné čísla z_1, z_2 tak sa dajú zostrojiť ak $z_1 + z_2$, $z_1 z_2$ a $\sqrt{z_1}$.

Dôkaz. Je zrejmé, že sa dá zostrojiť $z_1 + z_2$. Ďalej môžeme predpokladať, že $z_1 \neq 0 \neq z_2$. V takom prípade ich môžeme vyjadriť trigonometricky

$$z_1 = |z_1|(\cos\alpha_1 + \sin\alpha_1), z_2 = |z_2|(\cos\alpha_2 + \sin\alpha_2).$$

Potom

$$z_1 z_2 = |z_1||z_2|(\cos(\alpha_1 + \alpha_2) + \sin(\alpha_1 + \alpha_2)$$

a

$$\sqrt{z_1} = \sqrt{|z_1|}(\cos\Big(\frac{\alpha_1}{2} + \sin\frac{\alpha_1}{2}\Big).$$

Teda obidve hodnoty sa dajú zostrojiť. □

Podľa vety 72 a predošlej lemy dostávame

Veta 73. Ak F je také konečné normálne rozsšírenie poľ $\mathbb{Q}$ že pre jeho galoisovu grupu $G(F:\mathbb{Q})$ existuje $j \in \mathbb{N}$ a postupnosť podgrúp $G_0 = G(F:\mathbb{Q}) \supset G_1 \supset \ldots G_j = \{id\}$, že
i) G_{i+1} je normálna podgrupa G_i pre $i = 0, \ldots, j-1$ a
ii) $|G_i/G_{i+1}| = 2$, pre G_i pre $i = 0, \ldots, j-1$
tak každý prvok F sa dá zostrojiť pomocou pravítka a kružidla.

Keď uvedomíme, že $G(\mathbb{Q}(w_p):\mathbb{Q})$ je cyklická grupa rádu 2^ℓ s nejakým generátorom φ, tak $G_1 = [\varphi^2], G_2 = [\varphi^4], \ldots, G_\ell = [\varphi^{2^\ell}] = \{id\}$ je postupnosť podgrúp ktorá spľňa podmienky vety 73 dostávame, že w_p sa dá zostrojiť.

Prvočísla tvaru $2^\ell + 1$ sa nazývajú **Frematove prvočísla.**

Príklad 77. Z vety 71 vyplýva, že sa dá zostrojiť pravidelný 120 uholník, a teda, že sa dá zostrojiť uhol 3^o. A teda sa nedá zostrojiť žiaden uhol k^o kde $3 \nmid k$.

3 Kummerovské polia

Táto časť bude do istej miery opakovať niektoré fakty uvedená skôr. Uvázdzame ju pretože prináša o niečo kopmplexnejší a teoreticky hlbší pohľad na problematiku.

Ak F je pole a n je prirodzené číslo nedeliteľné charakteristkou F a $a_1, \ldots, a_q$ sú prvky F tak rozkladové pole polynómu $(x^n - a_1) \ldots (x^n - a_q)$ sa nazýva **Kummerovské rozširenie** poľa F, alebo **Kummerovské pole**. [17]

Veta 74. Nech F je pole charakteristiky p a n je prirodzené číslo. Polynóm $x^n - 1$ má n koreňov v nejakom nadpoli F práve vtedy ak p nedelí n. V takom prípade množina koreňov tohoto polynómu tvorí cyklickú grupu.

Na dôkaz využijeme aj nasledovné tvrdenie:

Lema 7. Ak G je konečná komutatívna grupa a $n \in N$ je najväčší z rádov prvkov z G tak rády všetkých prvkov G sú deliteľmi n.

Dôkaz. Uvažujme nejaký prvok $b \in H$ a označme jeho rád r. Ak r nie je deliteľom n tak existuje prvočíslo p také

[17] Ernst Eduard Kummer (29. Januŕa 1810 – 14. Maja 1893) bol nemecký matematik. Získal doktorát na univerzite v Hale v roku 1931. Zaoberal sa aj velkou Fernatovou vetou, ktorú dokázal pre tzv. regulárne prvočísla.

, že v kanonickom rozklade n vystupuje s exponentom α (prípadne $\alpha = 0$) a v kanonickom rozklade r vystupuje s exponentom β kde $\beta > \alpha$. Prvok a^{p^α} má rád $\frac{n}{p^\alpha}$ má rád $\frac{n}{p^\alpha}$ a prvok $b^{\frac{r}{p^\beta}}$ má rád p^β. Pretože čísla $\frac{n}{p^\alpha}, p^\beta$ sú nesúdeliteľné dostáveme podľa vety 9, že prvok $a^{p^\alpha} b^{\frac{r}{p^\beta}}$ má rád $np^{\beta-\alpha} > n$ a to je spor s maximalitou n. □

Príklad 78. Pomocou vety 7 sa tiez dá dokázať veta **??**.

Dôkaz vety 74. Ak $p \not| n$ tak $(x^n - 1)' = nx^{n-1} \neq 0$. Teda

$$x(x^n - 1)' - n(x^n - 1) = n \neq 0.$$

Z toho vyplýva, že $x^n - 1$ nemá násobné korene v žiadnom nadpoli F. Preto vo svojom rozkladovom poli má práve n rôznych koreňov. To že daná množina koreňov je grupa je zrejmé. Dokážeme, že táto grupa je cyklická. Nech ζ je jej prvok z najvyšším rádom. Nech m označuje rád ζ. Určite platí $m \leq n$. Podľa Lemy 7 všetky prvky tejto grupy sú koreňom polynómu $x^m - 1$. Pretože ich je n nemôže platiť $m < n$. Z toho vyplýva, že ζ generuje všetky korene uvažovaného polynómu. □

Prvky vyššie spomínanej grupy sa nazývajú n **té odmocniny s** 1 nad poľom a jej generátor sa nezýva **primitívna** n tá odmocnina s 1 nad poli F.

Príklad 79. Ak $F = \mathbb{C}$ je pole komplexných čísel tak primitívne n tá odmocniny z 1 sú $w_n^j, n \in \mathbb{N}$, kde $(j, n) = 1$.

Príklad 80. Primitívna 4 tá odmocnina z 1 na poľom $\mathbb{Z}_5$ je 2 alebo aj 3. Všetky prvky tohoto poľa okrem 0 sú 4 té odmocniny z 1. Vo všeobecnosti platí ,že všetky nenulové prvky konečného poľa F sú $|F|-1$ té odmocniny z 1 a generátor jeho multiplikatívnej grupy je primitívna $|F|-1$ tá odmocnina z 1.

Príklad 81. Primitívna 3 odmocnina z 1 nad poľom $\mathbb{Z}_5$ sa nenachádza v tomto poli ale v jeho nadpoli $\mathbb{Z}_5[x]/(x^2+x+1)$.

Príklad 82. Ak n spĺňa podmienky vety 74 a ζ primitívna n tá odmocnina z jednej tak
1) všetky primitívne n té odmocniny z 1 sú $\zeta^k, (k,n)=1$.
2) ak $a \in F$ a $\sqrt[n]{a}$ je jeden koreň polynúmu $x^n - a$ tak všetky korene tohoto polynómu sú $\zeta^j \sqrt[n]{a}, j = 0, \ldots, n-1$.

3.1 Noetherovej systémy a charaktery

Ak E je nejaké pole a G je nejaká podrupa grupy automorfizmov poľa F tak systém prvkov tohoto poľa $x_\varphi, \varphi \in G$ sa nazýva **Noetherovej systémom** pre grupu G práve vtedy keď

$$x_\varphi \varphi(x_\psi) = x_{\psi\varphi} \tag{35}$$

pre každé $\varphi, \psi \in G$. [18] Je zrejmé, že $x_\varphi = 0, \varphi \in G$ je Noetherovej systém pre grupu G. Tento sa nazýva **trivialny**. Noetherovej systém pre grupu G sa nazýva **netrivialny** ak existuje aspoň jeden $\varphi \in G$ taký, že $x_\varphi \neq 0$.

Príklad 83. L'ahko sa dá dokázať, že Noetherovej systém pre grupu G je netrivialny práve vtedy keď hodnota x_φ je nenulová pre všetky $\varphi \in G$.

Veta 75. Ak G je konečná grupa tak Noetherovej systém $x_\varphi, \varphi \in G$ je netrivialny vtedy a len vtedy ked existuje $\alpha \in E \setminus \{0\}$ také, že $x_\varphi = \frac{\alpha}{\varphi(\alpha)}$ pre každý automorfizmus $\varphi \in G$.

Dôkaz. Jedna implikácia vyplýva z dosadenia $x_\varphi = \frac{\alpha}{\varphi(\alpha)}$ do (35).

Podľa vety 55 sú automorfizmy z grupy G lineárne nezávislé nad poľom E. Preto ak $x_\varphi, \varphi \in G$ je netrivialny Noetherovej systém pre grupu G tak zobrazenie $\sum_{\varphi \in G} x_\varphi \varphi$ je nenulové a preto existuje prvok $a \in E$ taký, že

$$\sum_{\psi \in G} x_\psi \psi(a) = \alpha \neq 0. \tag{36}$$

[18] Emmy Noether (23. 3. 1882 - 14. 4. 1935) bola nemecká matematička, ktorá okrem iného významne prispela ku štúdiu rozkladu prvkov v okruhoch na ireducibilné činitele.

Pre konkretne $\varphi \in G$ z tejto rovnosti dostávame

$$\sum_{\psi \in G} \varphi(x_\psi)\varphi(\psi(a)) = \psi(\alpha).$$

Pretože $x_\varphi \neq 0$ rovnosť (35) môžeme upraviť a dostávame $\varphi(x_\psi) = \frac{x_{\psi\varphi}}{x_\varphi}$. Po dosadení do poslednej rovnosti dostávame

$$\frac{1}{x_\varphi} \sum_{\psi \in G} x_{\psi\varphi}\varphi(\psi(a)) = \psi(\alpha).$$

Ak ψ prebieha celú grupu G tak aj $\psi\varphi$ prebieha celú grupu G a teda podľa (36) sa suma z poslednej rovnosti rovná α. Preto $\frac{\alpha}{x_\varphi} = \varphi(\alpha)$. Po úprave dostávame tvrdenie. □

Ak G je grupa a F pole tak každý homorfizmus χ grupy G do multiplikatívnej grupy poľa F sa nazýva **charakter** grupy G v poli F. Množinu všetkých charakterov grupy G v poli F budeme označovať symbolom $\mathbf{X}(G, F)$. Na tejto množine sa dá prirodzene definovať operácia

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$$

pre $g \in G$. Zobrazenie χ_0 kde

$$\chi_0(g) = 1, g \in G.$$

je charakter. Tento charakter tvorí neutrálny prvok vzhľa dom na násobenie. Hodnoty charakterov sú nenulové teda

pre každý charakter χ je aj $\frac{1}{\chi}$ charakter, je to inverzný prvok k χ. Z asociatívnosti násobenia v poli F výplýva aj asociatívnosť násobenia charakterov. Z toho vyplýva, že množina $\mathbf{X}(G, F)$ s touto operáciou je grupa. Nazýva sa **grupa charakterov** grupy G v poli F.

Príklad 84. Charakter multiplikatívnej grupy $\mathbb{Z}_m^*$ v poli komplexných čísel sa nazýva aj **Dirichletov charakter** modulo m, pre $m \geq 2$. Ak symbolom G_m označíme grupu Dirichletovych charakterov modulo m tak sa dá dokázať

$$\sum_{n \in \mathbb{Z}_m^*} \chi_0(n) = \phi(m)$$

a

$$\sum_{n \in \mathbb{Z}_m^*} \chi(n) = 0$$

ak $\chi \neq \chi_0$. Podobne

$$\sum_{\chi \in G_m} \chi(1) = \phi(m)$$

a

$$\sum_{\chi \in G_m} \chi(n) = 0$$

ak $n \neq 1$.

Veta 76. Nech E je konečné normálne rozšírenie poľa F. Ak $\mathbf{X}$ je grupa charakterov grupy $G(E:F)$ v poli F tak exisuje taký prvok $\alpha \in E \setminus \{0\}$, že pre každý charakter $\chi \in \mathbf{X}$ platí

$$\chi(\varphi) = \frac{\alpha}{\varphi(\alpha)}$$

pre každé $\varphi \in G(E:F)$. Ak n je prirodzené číslo deliteľné rádmi všetkých prvkov z $G(E:F)$ tak pre dané α platí $\alpha^n \in F$.

Dôkaz. Uvažujme systém $x_\varphi = \chi(\varphi)$ pre $\chi \in \mathbf{X}$ a $\varphi \in G(E:F)$. Potom pre každé $\psi \in G(E:F)$ platí

$$x_\varphi \varphi(x_\psi) = x_\varphi x_\psi = \chi(\varphi)\chi(\psi) = \chi(\varphi\psi) = x_{\varphi\psi}.$$

Teda $\chi(\varphi); \varphi \in G(E:F)$ je netrivialny noetherovej systém grupy $G(E:F)$. Pretože $G(E:F)$ je grupa automorfizmov poľ E dostávame podľ vety 75 to, že existuje $\alpha \in E$ také, že $\chi(\varphi) = \frac{\alpha}{\varphi(\alpha)}$ pre každé $\varphi \in G(E:F)$.

Ak n je spomínané prirodzené číslo tak pre každé $\varphi \in G(E:F)$ platí $\varphi^n = id$. Preto pre každý charakter $\chi \in \mathbf{X}$ máme $1 = \chi(\varphi^n)$. To znamená $(\frac{\alpha}{\varphi(\alpha)})^n = 1$ a teda $\alpha^n = \varphi(\alpha^n)$. Z toho vyplýva $\alpha^n \in F$.

□

Príklad 85. Nech G je cyklická grupa rádu n, pre nejaké $n \in \mathbb{N}$, a pole F obsahuje primitívnu n - tú odmocninu z 1 a

charakteristika poľa nedelí n. Dokážeme, že grupa $\mathbf{X}(G, F)$ je izomorfná s grupou G. Nech g je generátor grupy G a ζ_n je fundamentálna odmocnina z 1. Každý charakter je jednoznačne určený svojou hodnotou v g. Preto

$$\mathbf{X}(G, F) = \{\chi_k; k = 0, \ldots, n-1\},$$

kde $\chi_k(g) = \zeta_n^k$. Je zremé, že χ_1 je generátor $\mathbf{X}(G, F)$.

3.2 Rozklad konečnej komutatívnej grupy

V tejto časti budeme študovať zovšeobenenie príkladu 85 na konečné komutatívne grupy. Dôležitú úlohu bude hrať nasledujúci štrukturálny výsledok, ktorý volnými slovami hovorí , štruktúra konečných komutatívnych grúp je jednoduchá. Symbol $\odot$ označuje priamy súčin grúp. Tento pojem je definovaný a študovaný v príslušnej časti v Doplnkoch.

Veta 77. Ak G je konečná komutatívna grupa tak existujú prvky $b_1, \ldots, b_s \in G, s \in N$ také, že

$$G = [b_1] \odot \cdots \odot [b_s] \tag{37}$$

a rád prvku b_i je deliteľom rádu prvku b_{i-1} pre $i = 2, \ldots, s$.

Dôkaz začneme nasledujúcim tvrdením:

Lema 8. Nech $H_1 \subset H_2$ sú komutatívne grupy a $\Phi : H_2 \to H_1$ je taký homomorfizmus, že $\Phi|_{H_1} = id$. Potom $H_2 = H_1 \odot Ker\Phi$.

Dôkaz. Nech $a \in H_1 \cap Ker\Phi$. Potom $a = \Phi(a) = e$. Teda

$$H_1 \cap Ker\Phi = \{e\}. \tag{38}$$

Ak $b \in H_2$ tak $\Phi(b) = c \in H_1$. Potom

$$b = c(bc^{-1}).$$

Kde $\Phi(bc^{-1}) = \Phi(b)c^{-1} = cc^{-1} = e$. Preto $bc^{-1} \in Ker\Phi$. Dokázali sme $H_2 = H_1 Ker\Phi$. Podľa (38) dostávame tvrdenie. □

Lema 9. Nech H je konečná komutatívna grupa a $a \in H$ je prvok najväčšieho rádu. Potom rády všetkých prvkov G sú deliteľmi rádu a a pre každú podgrupu H_1 a homomorfizmus $\Psi : H_1 \to [a]$ existuje homomorfizmus $\Phi : H \to [a]$ taký, že $\Phi|_{H_1} = \Psi$.

Dôkaz. Prvá časť vyplýva z Lemy 7.

Nech $g_1 \in H$ je prvok ktorý nepatrí do H_1. Označme m rád prvku $g_1 H_1$ vo faktorovej grupe H/H_1. Potom m je najmenšie prirodzené také, že $g_1^m \in H_1$. Preto m je deliteľom n. Uvažujme grupu $H_2 = [H_1 \cup \{g_1\}]$. Každý prvok H_2 sa dá vyjadriť v tvare $hg_1^k, 0 \leq k < m$. Ukážeme

ako sa homomorfizmus Ψ dá rozširiť na homorfizmus Ψ_1 definovaný na H_2. Nech $\Psi(g_1^m) = a^\ell$. Potom

$$a^{\ell\frac{n}{m}} = (\Psi(g^m))^{\frac{n}{m}} = \Psi(g^n) = e.$$

V tomto prípade dostávame n je deliteľom $\ell\frac{n}{m}$, z toho dostáme $m|\ell$. Položme $\ell = jm$. Potom

$$\Psi(g_1^m) = a^{jm}. \tag{39}$$

Bolo by preto prirodzené definovať homomorfizmus $\Psi_1 : H_2 \to [a]$ tak aby platilo $\Psi_1(g_1) = a^j$, to znamená

$$\Psi_1(hg_1^i) = \Psi(h)a^{ji}. \tag{40}$$

Mali by sme dokázať, že táto definícia korektná. Inými slovami, že obraz prvku nezávisí na tvare v ktorom ho vyjadríme.

Predpokladajme

$$hg_1^k = h_1 g_1^{k_1} \tag{41}$$

potom

$$h_1^{-1}h = g_1^{k_1-k} \tag{42}$$

a teda $g_1^{k_1-k} \in H_1$ z toho vyplýva $m|(k_1 - k)$. Ak aplikujeme na obe strany (42) homomorfizmus Ψ dostávame

$$\Psi(h_1)^{-1}\Psi(h) = \Psi(g_1^{k_1-k}) = (\Psi(g_1^m))^{\frac{k_1-k}{m}}$$

Podľa (39) teda platí

$$\Psi(h_1)^{-1}\Psi(h) = a^{j(k_1-k)}.$$

A teda

$$\Psi(h)a^{jk} = \Psi(h_1)a^{jk_1}.$$

Tým sme dokázali, že zobrazenie definované pomocou (40) je definované korektne. To že toto zobrazenie je homorfizmus je dôsledkom jedoduchých úprav. Zostrojili sme homomorfizmus $\Psi_1 : H_2 \to [a]$. Grupa H je konečná a teda existujú prvky $g_1, \ldots, g_s \in H$ také, že $H = [H_1 \cup \{g_1, \ldots, g_s\}]$. Z tohoto dôvodu sa homorfizmus Ψ dá postupne rozšíriť na $\Phi : H \to [a]$. □

Dôkaz vety 77. Nech G je konečná komutatívna grupa a $b_1 \in G$ je prvok s najväčším rádom. Podľa Lemy 9 sa homomorfizmus $\Psi : [b_1] \to [b_1]$ kde $\Psi(x) = x$ dá rozšíriť homomorfizmus $\Phi : G \to [b_1]$. Podlä lemy 8 dostávame $G = [b_1] \odot Ker\Phi$. Podobne môžeme postupovať s gtupou $G_1 = Ker\Phi$. Z konečnosti G vyplýva. že po konečnom počte krokov dostaneme rozklad G s požadovanými vlastnosťami. □

Veta 78. Nech G je konečná komutatívna grupa a $n \in \mathbb{N}$ je najväčší z rádov prvkov z G. Ak charakteristika poľa F nedelí n a F obsahuje primitívnu n tú odmocninu s 1 tak $\mathbf{X}(G, F) \sim G$.

Dôkaz. Podľa vety 77 si grupu G môžeme vyjadriť v tvare (37) kde $n = n_1$ je rád prvku b_1 a n_i je rád prvku $b_i, i = 2, \ldots, s$. Ak $\chi \in \mathbf{X}(G, F)$ a $g = b_1^{t_1} \ldots b_s^{t_s}$ kde $0 \leq t_i < n_i, i = 1, \ldots, s$ tak

$$\chi(g) = \chi(b_1)^{t_1} \ldots \chi(b_s)^{t_s}. \tag{43}$$

Je zrejmé, že hodnota $\chi(b_i)$ je koreňom rovnice $x^{n_i} = 1$. Preto táto hodnota sa dá vyjadriť v tvare

$$\chi(b_i) = \zeta_i^{\epsilon_i}, 0 \leq \epsilon_1 < n_i$$

kde ζ_i je primitívna n_i- ta odmocnina z 1 v F. Definujme zobrazenia

$$\chi_i(g) = \chi_i(b_i^{t_i}) = \zeta_i^{t_i}, i = 1, \ldots, s.$$

Je zrejmé, že tieto zobrazenia sú charaktery G v poli F. Podľa (43) dostá- veme

$$\chi(g) = \chi_1^{\epsilon_1}(g) \ldots \chi_s^{\epsilon_s}(g), g \in G.$$

To znamená,

$$\chi = \chi_1^{\epsilon_1} \cdots \chi_s^{\epsilon_s}.$$

Preto grupa $\mathbf{X}(G, F)$ je generovaná charaktermi $\chi_1, \ldots, \chi_s$. Dokážeme

$$\mathbf{X}(G, F) = [\chi_1] \odot \cdots \odot [\chi_s]. \tag{44}$$

Stačí dokázať iba to, že podgrupy $[\chi_1], \ldots, [\chi_s]$ sú nezávislé. Nech napríklad

$$\chi' \in [\chi_1] \cap [\chi_2] \cdot \cdots \cdot [\chi_s].$$

Potom pre nejaké $\epsilon_1 < n_1, \ldots, \epsilon_s < n_s$ platí

$$\chi_1^{\epsilon_1} = \chi' = \chi_2^{\epsilon_2} \cdots \chi_s^{\epsilon_s}.$$

Charakter χ_1 je v skutočnosti závislý len od činiteľa b_1 a ostatné charaktery len od činiteľov $b_2, \ldots, b_s$. Preto ak do posledných rovností dosadíme b_1 dostávame $b_1^{\epsilon_1} = 1$ a teda $\epsilon_1 = 0$ preto $\chi' = 1$ je jednotkový charakter. Podobne sa ukážu ostatné nezávislosti. Dokázali sme (44). Môžeme preto definovať zobrazenie $\Phi : G \to \mathbf{X}(G, F)$ kde

$$\Phi(g_1^{t_1} \ldots g_s^{t_s}) = \chi_1^{t_1} \cdots \chi_s^{t_s}. \tag{45}$$

Provnávaním prvkov a úpravami sa dá preveriť, že Φ je izomorfizmua. □

Veta 79. Nech E je rozšírenie poľa F ktoré obsahuje primitívnu n tú odmocninu z 1 pre nejaké $n \in N$. Položme

$$A = \{\alpha \in E \setminus \{0\}; \alpha^n \in F\}.$$

Potom A je podgrupa multiplikatívnej grupy poľa E a $F \setminus \{0\}$ podgrupa A a platí
i)

$$A/(F \setminus \{0\}) \sim A^n/(F \setminus \{0\})^n.$$

a
ii) Ak X je grupa charakterov grupy $G(E:F)$ v poli F tak

$$\mathbf{X} \sim A/(F \setminus \{0\}).$$

Dôkaz. Uvažujme zobrazenie

$$\Phi : A \to A^n/(F \setminus \{0\})^n$$

$$\Phi(\alpha) = \alpha^n(F \setminus \{0\})^n.$$

Je zrejmé, že toto zobrazenie je homorfizmus a z definície množiny A^n vyplýva, že je surjekcia. Podľa hlavnej vety o homorfizme stačí dokázať,že $Ker\Phi = F \setminus \{0\}$. Ľahko je vidieť, že $F \setminus \{0\} \subset Ker\Phi$. Ak $\alpha \in Ker\Phi$ tak $\alpha^n \in (F \setminus \{0\})^n$ a teda $\alpha^n = a^n$ pre nejaké $a \in F \setminus \{0\}$. To znamená $(\frac{\alpha}{a})^n = 1$ a preto $\alpha = \zeta^j a$ kde ζ je primitívna n tá odmocnina z 1 a j je nejaké nezáporné celé číslo. Podľa predpokladu platí $\zeta \in F$ a teda $\alpha \in F$. Tým sme dokázali i). Ak $\alpha \in A$ tak pre každé $\varphi \in G(E:F)$ platí $\varphi(\alpha^n) = \alpha^n$ pretože podľa definície množiny A máme $\alpha^n \in F$. Z toho dostávame $(\frac{\alpha}{\varphi(\alpha)})^n = 1$ a teda $\frac{\alpha}{\varphi(\alpha)} \in F$. Prvku $\varphi \in G(E:F)$ môžeme priradiť hodnotu $\chi_\alpha(\varphi) = \frac{\alpha}{\varphi(\alpha)} \in F$. Ak $\psi \in G(E:F)$ tak

$$\chi_\alpha(\varphi\psi) = \frac{\alpha}{\psi(\varphi(\alpha))} = \frac{\alpha}{\psi(\alpha)} \cdot \frac{\psi(\alpha)}{\psi(\varphi(\alpha))} =$$

$$= \frac{\alpha}{\psi(\alpha)} \cdot \psi\Big(\frac{\alpha}{\varphi(\alpha)}\Big) = \frac{\alpha}{\psi(\alpha)} \cdot \frac{\alpha}{\varphi(\alpha)} = \chi_\alpha(\psi)\chi_\alpha(\varphi).$$

Vidíme teda, že χ_α je homorfizmus grupy $G(E:F)$ do F a preto je to charakter. Môžeme teda definovať zobrazenie

$$\Psi : A \to \mathbf{X}$$

kde

$$\Psi(\alpha) = \chi_\alpha.$$

Pre $\beta \in A$ a $\varphi \in G(E:F)$ platí $\frac{\alpha\beta}{\varphi(\alpha\beta)} = \frac{\alpha}{\varphi(\alpha)}\frac{\beta}{\varphi(\beta)}$. To znamená $\chi_{\alpha\beta}(\varphi) = \chi_\alpha(\varphi)\chi_\beta(\varphi)$. Teda

$$\Psi(\alpha\beta) = \Psi(\alpha)\Psi(\beta),$$

preto $\Psi : A \to \mathbf{X}$ je homorfizmus. Toto zobrazenie je surjekcia podľa vety 76. Pre každé $\alpha \in A$ platí $\alpha \in Ker\Psi$ práve vtedy keď $\frac{\alpha}{\varphi(\alpha)} = 1$ pre každý automorfizmus $\varphi \in G(E:F)$. To je ekvivalentné s tým, že $\alpha \in F \setminus \{0\}$. Preto $Ker\Psi = F \setminus \{0\}$. Z toho dostávame ii).

□

Veta 80. Nech F je pole a n je prirodzené číslo, ktoré nie je deliteľné charakteristikou poľa F. Predpokladajme, že F obsahuje primitívnu n tú odmocninu z 1. Ak E je konečné, normálne rozšírenie poľa F také, že grupa $G(E:F)$ je komutatívna tak existujú také prvky $a_1, \ldots, a_k \in F$, že pole E je rozkladové pole polynómu $(x^n - a_1)\ldots(x^n - a_k)$.

Dôkaz. Grupa $A/(F \setminus \{0\})$ je izomorfná s $G(E:F)$ a preto je konečná. Nech

$$A = F \setminus \{0\} \cup \alpha_1(F \setminus \{0\}) \cup \ldots \alpha_k(F \setminus \{0\}) \tag{46}$$

je disjunktný rozklad grupy A. Dokážme

$$E = F(\alpha_1, \ldots, \alpha_k). \tag{47}$$

Položme $a_i = \alpha_i^n, i = 1, \ldots, k$. Potom $a_i \in F$. Pretože F obsahuje prim- itívnu n tú odmocninu z 1 je $F(\alpha_1, \ldots, \alpha_k)$ rozkladovým poľom polynómu $(x^n - a_1) \ldots (x^n - a_k)$ a teda je to normálne rozšírenie poľa F. Nech neplatí (47). Potom existuje $\varphi \in G(E : F(\alpha_1, \ldots, \alpha_k))$ také, že $\varphi \neq id$. Ak uvážime zobrazenie (45) dostávame, že existuje charakter $\chi \in \mathbf{X}$ taký, že

$$\chi(\varphi) \neq 1. \tag{48}$$

Podľa vety 76 existuje $\alpha \in E$ také, že $\chi(\varphi) = \frac{\alpha}{\varphi(\alpha)}$. Podľa vety 76 dostávame $\alpha^n \in F$ a teda $\alpha \in A$. Z rovnosti (46) vyplýva $\alpha \in F(\alpha_1, \ldots, \alpha_k)$ a teda $\alpha = \varphi(\alpha)$ a to je spor s (48). □

4 Normálna báza

Ak E je rozkladové pole nejakého separabilného polynómu nad poľom F a pre nejaký prvok $\gamma \in E$ tvoria prvky

$\varphi(\gamma), \varphi \in G(E:F)$ bázu vektorového priestoru E nad F tak táto báza sa nazýva **normálna báza**. Pretože $|G(E:F)| = [E:F]$ je to ekvivalentné ss tým, že tieto prvky sú lineárne nezávislé nad F.

Ak $\gamma \in E$ kedy sú prvky $\varphi(\gamma), \varphi \in G(E:F)$ linearne nezávislé? Nech $G(E:F) = \{\varphi_1, \ldots, \varphi_n\}$. Uvažujme rovnicu

$$x_1\varphi_1(\gamma) + \cdots + x_n\varphi_n(\gamma) = 0.$$

Ak označíme $\varphi_1 = id$ a postupne aplikujeme všetky prvky $G(E:F)$ na ľavú aj pravú stranu tejto rovnice dostaneme sútavu rovníc

$$x_1\varphi_i(\varphi_1(\gamma)) + \cdots + x_n\varphi_i(\varphi_n(\gamma)) = 0, i = 1, \ldots, n.$$

Z toho vyplýva:

Lema 10. Prvky $\varphi_i(\gamma), i = 1, \ldots, n$ sú lineárne nezávislé práve vtedy, keď matica $A = (\varphi_i(\varphi_j(\gamma)))$ je regulárna.

Ukážeme ako sa taký prvok dá za istých predpokladov zostrojiť. Predpokladajme, že pole F má charakteristiku 0. V takom prípade je pole F nekonečné a preto existuje $\alpha \in E$ také, že $E = F(\alpha)$. Označme $f(x)$ minimálny polynóm tohoto prvku. Tento polynóm je ireducibinlný a teda nemá násobné korene. Označme $\alpha_1 = \alpha$ a $\alpha_j = \varphi_j(\alpha_1)$. Potom $\alpha_1, \ldots, \alpha_n$ s'u všetky korene polynómu $f(x)$.

Položme $f(x) = (x-\alpha_j)g_j(x)$. Je zrejmé, že $g_j(\alpha_j) \neq 0$ a pre pre $i \neq j$ platí $g_j(\alpha_i) = 0$. Uvažujme polynómy

$$h_j(x) = \frac{g_j(x)}{g_j(\alpha_j)},\ j = 1, \ldots, n.$$

Je zrejmé, že ak $a \in F$ tak $\varphi_j(h_1(a)) = h_j(a)$. Teda ak dosadíme $\gamma = h_1(a)$ do matice A z lemy 10 tak prvý riadok tajto matice bude vektor $(h_1(a), \ldots, h_n(a))$ a ostatné riadky budú mať tie isté prvky, iba v inom poradí .

Je zrejmé, že $h_j(\alpha_j) = 1$ a $h_j(\alpha_i) = 0$ ak $i \neq j$ pre $i.j = 1, \ldots, n$. Ak označíme $h(x) = \sum_{j=1}^{n} h_j(x)$ tak pre každé $\alpha_j, j = 1, \ldots, n$ platí $h(\alpha_j) = 1$. Ale $h(x)$ je polynóm stupňa $n-1$ a z predošlého vyplýva že polynóm $h(x)-1$ má n koreňov. Z toho vyplýva, že tento polynóm sa identicky rovná 0. Dokázali sme

$$h_1(x) + \cdots + h_n(x) = 1. \tag{49}$$

Uvažujme maticu polynomických funkcií

$$A(x) = (\varphi_i(\varphi_j(h_1(x)),$$

kde x je premenná z poľa F. Ak označíme $D(x)$ determinant dejto matice tak platí

$$D^2(x) = |A(x)A^T(x)|. \tag{50}$$

Matica napravo má na diagonále hodnotu $\sum_{j=1}^{n} h_j^2(x)$. Je zrejmé, že

$$h_i(x)h_j(x) \equiv 0 \pmod{f(x)}, i \neq j$$

a podľa (49) dostávame teda

$$h_i^2(x) \equiv h_i(x) \pmod{f(x)}.$$

Z toho vyplýva $D^2(x) \equiv 1 \pmod{f(x)}$. Z nekoneňosti poľa F dostávame, že existuje $a \in F$ také, že $D^2(a) \neq 0$. A pre túto hodnotu a budú hodnoty $h_i(a), i = 1, \ldots, n$ lineárne a preto platí

Veta 81. Hodnoty $\varphi_i(h_1(a)), i = 1, \ldots, n$ tvoria normálnu bázu E nad F.

5 Doplnky

5.1 Zornova lema a jej ekvivalenty

.

Nech M je neprázdna množina. Binárna relácia $\ll$ sa nazýva **čiastočné usporiadanie** na množine M práve vtedy ak :
1) $a \ll a$ pre každé $a \in M$,
2) ak $a \ll b$ a $b \ll a$ tak $a = b$,

3) ak $a \ll b$ a $b \ll c$ tak $a \ll c$
pre každé $a, b, c \in M$. V takom prípade hovoríme aj že množina M je **čiastočne usporiadaná**. Prvký $x, y \in M$ nazývame **porovnateľné** práve vtedy keď $x \ll y$ alebo $y \ll x$. Podmnožina množiny M sa nazýva **reťazec** práve vtedy ak každé jej dva prvky sú porovnateľné. Retazcom je naprílad prázdna množina , alebo jednoprvkové množiny.

Podmožina $S \subset M$ sa nazýva **zhora ohraničená** ak existuje $h \in M$, také, že pre každé $s \in S$ platí $s \ll h$. Prvok h sa nazýva **horné ohraničenie** množiny S. Prvok $s_1 \in S$ sa nazýva **maximálnym prvkom** S práve vtedy ak pre každé $s \in S$ platí $s_1 \ll s \Rightarrow s_1 = s$.

Podmožina $S \subset M$ sa nazýva **zdola ohraničená** ak existuje $d \in M$, také, že pre každé $s \in S$ platí $d \ll s$. Prvok d sa nazýva **dolné ohraničenie** množiny S.

Zornova lema. Ak každý reťazec v M je zhora ohraničený, tak M obsahuje maximálny prvok. [19]

Dokážeme, že Zornova lema je ekvivalentná s

Axioma výberu. Ak X je neprázdna množina tak existuje zobrazenie $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ také, že $f(A) \in A$ pre $A \in \mathcal{P}(X) \setminus \{\emptyset\}$.

[19] Tento výsledok sa volá aj Zornova - Kuratowského lema. Bol objavený prvý krát poliakom Kazimierzom Kuratowskym v roku 1922. V roku 1935 ho nezávisle na Kuratowskom dokázal Max Zorn. Povodom nemec, ktorý sa na protest proti nazizmu presťahoval v roku 1933 do USA.

Toto tvrdenie je intuitívne ľahko prijateľné. Hovorí , že z každej neprázdnej množiny A sa dá vybrať nejaký prvok označený ako $f(A)$.

Veta 82. Z Axiomy výberu vyplýva Zornova Lema.

Nasledujúci dôkaz je spracovaný podľla práce [9] .

Nech M je čiastočne usporiadaná množina, taká že každý reťazec v M je zhora ohraničený. Označme $\mathcal{R}$ množinu všetkých reťazcov v M čiatočne usporiadaná inklúziou. Maximálny prvok v $\mathcal{R}$ nazývame **maximálny reťazec** .

Lema 11. Ak $C \in \mathcal{R}$ je maximálny raťazec tak jeho horné ohraničenie je maximálny prvok v M.

Dôkaz. Ak m je horné ohraničenie C tak aj z maximality C vyplýva $m \in C$. Ak by pre niektoré $m_1 \in M$ platilo $m \leq m_1$ tak aj $C \cup \{m_1\}$ je retázec a teda znovu s maximality C dostávame $m_1 \in C$. Preto $m_1 \leq m$ a teda $m = m_1$. □

Zornova lema bude preto dokázaná ak sa nám podarí násť v $\mathcal{R}$ maximány reťazec. Pre $C \in \mathcal{R}$ definujme $\bar{C} = \{x \in M; C \cup \{x\} \in \mathcal{R}\}$, inými slovami je to množina všetkých prvkov, ktoré sú porovnateľné so všetkými prvkami C.

Podľa Axiomy výberu existuje zobrazenie $f : \mathcal{P}(M) \setminus \{\emptyset\} \to M$ také , že $f(A) \in A$. Je zrejmé, že pre reťazec $C \in$

$\mathcal{R}$, taký že $\bar{C} \setminus C \neq \emptyset$ je aj množina $C \cup \{f(\bar{C} \setminus C)\}$ reťzec. To nám umožňuje definovať zobrazenie $g : \mathcal{R} \to \mathcal{R}$ tak, že $g(C) = C$ ak $\bar{C} = C$ a $g(C) = C \cup \{f(\bar{C} \setminus C)\}$ inak. Takto dostávame veľmi jednoduché kritérium maximálnosti:

Lema 12. Reťazec C je maximálny práve vtedy, keď $g(C) = C$.

Budeme využívať vlastnosti nasledujúceho pojmu: systém množín $\mathcal{V} \subset \mathcal{R}$ sa nazýva **veža** práve vtedy keď
i) $\emptyset \in \mathcal{V}$,
ii) Ak $C \in \mathcal{V}$ tak aj $g(C) \in \mathcal{V}$ a
iii) ak $\mathcal{S} \subset \mathcal{V}$ je reťazec tak $\cup\mathcal{S} \in \mathcal{V}$.

Lema 13. Ak $\mathcal{V}$ je veža a reťazec tak $C = \cup\mathcal{V}$ je maximálny reťazec v $\mathcal{R}$.

Dôkaz. Ak $a, b \in C$ tak existujú reťazce $B_1 \in \mathcal{V}, B_2 \in \mathcal{V}$ také že $a \in B_1, b \in B_2$. Pretože $\mathcal{V}$ je reťazec tak $B_1 \subset B_2$ alebo $B_2 \subset B_1$. Teda a, b patria do rovnakého reťazca teda sú porovnateľné. Dokázali sme, že C je reťazec. Teraz použijeme lemu 12. Určite platí , že $C \subset g(C)$. $\mathcal{V}$ je reťazec a teda podľa vlastnosti iii) definície veže dostávame $C \in \mathcal{V}$ a teda aj $g(C) \in \mathcal{V}$. Teda $g(C) \subset C$ a teda C je maximálny reťazec. □

Stačí teda nájsť vežu ktorá je aj reťazec. Je zrejmé, že prienik sýtému všetkých veží je veží je veža. Označme

ju $\mathcal{V}_0$. Je to minimálna veža. Množina $C \in \mathcal{V}_0$ sa nazýva **porovnateľná** práve vtedy ak je porovnateľná so všetkými množinami v $\mathcal{V}_0$. Symbolom $\mathcal{C}$ budeme označovať systém všetkých porovnateľných množín.

Lema 14. *$\mathcal{C}$ je veža.*

Dôkaz. Je zrejmé, že $\emptyset \in \mathcal{C}$. Nech $\mathcal{S} \subset \mathcal{C}$ je reťazec. Ak $A \in \mathcal{V}_0$ tak alebo všetky množiny z $\mathcal{S}$ sú podmožiny A v takom prípade $\cup\mathcal{S} \subset A$, alebo aspoň jedna z nich je nadmožinou A a potom $A \subset \cup\mathcal{S}$. Teda $\cup\mathcal{S} \in \mathcal{C}$.

Stačí teda dokázať iba

$$C \in \mathcal{C} \Longrightarrow g(C) \in \mathcal{C}. \tag{51}$$

Nech $C \in \mathcal{C}$. Definujme si

$$\mathcal{U} = \{A \in \mathcal{V}_0; A \subset C \vee g(C) \subset A\}.$$

Ak dokážeme, že $\mathcal{U}$ je veža, tak z minimality $\mathcal{V}_0$ dostávame $\mathcal{U} = \mathcal{V}_0$ a teda pre každe $A \in \mathcal{V}_0$ platí $A \subset C \subset g(C)$ alebo $g(C) \subset A$ a teda platí (51).

Je jasné, že $\emptyset \in \mathcal{U}$. Uvažujme reťazec $\mathcal{Q} \subset \mathcal{U}$. Ak pre každú množinu $A \in \mathcal{Q}$ pltí $A \subset C$ tak aj $\cup\mathcal{Q} \subset C$. V opaňom prípade existuje $A \in \mathcal{Q}$ taká, že $g(C) \subset A$ a preto aj $g(C) \subset \cup\mathcal{Q}$. Zostáva dokázať vlastnosť ii) veže. Použijeme implikáciu

$$A \subsetneq C \Longrightarrow g(A) \subset C.$$

Vyplýva z toho, že v prípade $g(A) \not\subset C$ platí $C \subsetneq g(A)$ a preto $A \subsetneq C \subsetneq g(A)$ teda množina $g(A)$ by mala aspoň o dva prvky viac ako A a to je spor.

Nech $A \in \mathcal{U}$. Ak $A \subsetneq C$ tak $g(A) \subset C$. Ak $C = A$ tak $g(C) = g(A)$. Ak $C \subsetneq A$ tak $g(C) \subset A \subset g(A)$. Teda $g(A) \in \mathcal{U}$. Dokázali sme, že $\mathcal{U}$ je veža. □

Takže $\mathcal{C}$ je veže, je jasné, že to je reťazec. Preto $R \cup \mathcal{C}$ je podľa lemy 13 maximálny retázec a podľa lemy 11 platí , že jeho horné ohraničenie je maximálny prvok v M.

Nech $\mathbb{L}$ je ľuboovoľá množina. Hovoríme, že binárna relácia $\preceq$ je **dobrým usporiadaním** na B práve vtedy keď je čiastočným usporiadaním takým, že každé dva prvky $\mathbb{L}$ sú porovnateľné a každá neprázdna podmnožina $\mathbb{L}$ obsahuje minimálny prvok. Veľmi známym dobrým usporiadaním je usporiadanie množiny prirodzených čísel podľa veľkosti.

Zermelova veta. Na každej množine existuje dobré usporiadanie.

Veta 83. Axioma výberu, Zornova lema a Zermelova veta sú ekvivalentné.

Ak platí Zermelova veta a X je ľbovoľná množina, tak môžeme predpokladat že $\preceq$ je dobré usporiadanie na X. Potom každej neprázdnej množine $A \subset X$ môžeme priradiť prvkok $f(A) \in A$ ktorý bude jej najmenším prvkom

vzhľadom na usporiadanie $\preceq$. To je zobrazenie ktoré sa uvažuje v Axiome výberu.

Na dôkaz vety 83 stačí už dokázať iba to že z Zornovej lemy vyplýva Zermelova veta.

Z hladiska predstavivosti je zrejmé, že každú konečnú množinu môžeme usporiadať do postupnosti a tak dostaneme dobré usporiadanie. Nekonečnú spočítateľnú množinu môžeme zoradiť do prostej postupnosti a to nám definuje dobré usporiadanie na nej.

Nech $\mathbb{L}$ je ľubovoľná množina. Uvažujme množinu M ktorá obsahuje usporiadané dvojice $(A, \preceq_A)$ kde $A \subset \mathbb{L}$ jemnožina na ktorej existuje dobré usporiadanie $\preceq_A$. Ak $(A, \preceq_A), (B, \preceq_B) \in M$ tak hovoríme, že $(A, \preceq_A)$ je **segment** $(B, \preceq_B)$ práve vtedy $A \subset B$, pre $a, a' \in A$ platí

$$a \preceq_B a' \Rightarrow a \preceq_A a' \tag{52}$$

a pre $a \in A, b \in B$ platí

$$b \preceq_B a \Rightarrow b \in A. \tag{53}$$

Definijeme čiastočné usporiadanie na M takto $(A, \preceq_A) \ll (B, \preceq_B)$ práve vtedy keď $(A, \preceq_A)$ je segment $(B, \preceq_B)$.

Z prešlého vyplýva, že M je neprázdna množina. Uvažujme reťazec $C \subset M$. Definujme

$$A_0 = \cup\{A; (A; \preceq_A) \in C\}$$

a reláciu $\preceq_{A_0}$ tak, že pre $a, b \in A_0$ platí

$$a \preceq_{A_0} b \Longleftrightarrow a \preceq_A b$$

kde $(A, \preceq_A) \in C$ a $a, b \in A$. Je zrejmé $\preceq_{A_0}$ je čiastočné usporiadanie na A_0 a každé dva prvky sú porovnateľné. Dokážeme, že $\preceq_{A_0}$ je dobré usporiadanie na A_0. Teda stačí už dokázať iba to, že neprázdna podmnožina A_0 má najmenší prvok. Ak $B \subset A_0$ a $B \neq \emptyset$ tak existuje $(A, \preceq_A) \in C$ také, že $A \cap B \neq \emptyset$. Nech $b \in A \cap B$ je najmenší prvok $A \cap B$. Ukážeme , že b je najmenší prvok B. Nech $b' \preceq_{A_0} b, b' \neq b$. Potom existue A' také , že $(A', \preceq_{A'}) \in C$ a $b' \in B \cap A'$. Platí $A \cap B \subset A' \cap B$ alebo $A' \cap B \subset A \cap B$. Druhý prípad nemôže nastať, lebo by to bol s minimalitou b. Teda platí prvý prípad. Potom ale $(A, \preceq_A)$ je segment $(A', \preceq'_A)$ a teda $b' \in A$ a znovu dostávame spor s minimalitou b. Teda A_0 je dobre usporiadaná množina a $(A_0, \preceq_{A_0})$ je horným ohraničením C. Z Zornovej lemy dostávame že M obsahuje maximálny prvok. Nech je to $(\mathbb{L}', \preceq_{\mathbb{L}'})$. Ak by platilo, $\mathbb{L}' \neq \mathbb{L}$ tak existuje prvok $c \in \mathbb{L}$ taký, že $c \notin \mathbb{L}'$. Na množinu $\mathbb{L}'' = \mathbb{L} \cup \{c\}$ môžeme rozšíriť usporiadanie $\preceq_{\mathbb{L}'}$tak, že $a \preceq_{\mathbb{L}''} c$ pre každý prvok $a \in \mathbb{L}'$. Potom $(\mathbb{L}'', \preceq_{\mathbb{L}''}) \in M$ a dostávame spor s maximalitou $(\mathbb{L}', \preceq_{\mathbb{L}'})$. Preto $\mathbb{L}' = \mathbb{L}$ a $\preceq_{\mathbb{L}'}$ je dobré usporiadnie na množine $\mathbb{L}$. Tým sme dokázali, že Zermelova veta vyplýva z Zornovej lemy.

5.2 Rozklad grupy podla podgrupy

Nech G je grupa a H je jej podgrupa definujme pre $g \in G$ množinu

$$gH = \{gh; h \in H\}.$$

Keď si uvedomíme, že $e \in H$ dostávame

Lema 3. Pre každé $g \in G$ platí $g \in gH$.

Dôkaz: $g = ge \in gH$. □

Veta 84. Pre každé $g, g_1 \in G$ platí

$$gH = g_1H \iff g^{-1}g_1 \in H.$$

Dôkaz. Nech $g^{-1}g_1 \in H$, potom $g^{-1}g_1 = h \in H$. Preto $g_1 = gh$. Teda ak $a \in g_1H$ tak $a = g_1h_1$ pre nejaké $h_1 \in H$ a teda $a = ghh_1 \in gH$. Dokázali sme inklúziu $g_1H \subset gH$. Opačnú inklúziu dokážeme rovnako ak si uvedomíme $g^{-1}g_1 \in H \Rightarrow g_1^{-1}g = (g^{-1}g_1)^{-1} \in H$.

Opačná implikácia. Nech $gH = g_1H$. Podľa Lemy 3 dostávame $g_1 \in gH$ teda $g_1 = gh$ preto $g^{-1}g_1 = h \in H$. □

Veta 85. Pre g, g_1 platí

$$gH \cap g_1H \neq \emptyset \iff gH = g_1H.$$

Dôkaz. Jedna implikácia je zrejmá.

Nech $gH \cap g_1H \neq \emptyset$, potom existuje prvok $a \in gH \cap g_1H$. Teda existujú $h_1, h_2 \in H$ také , že

$$gh_1 = a = g_1h_2.$$

Teda po jednoduchej úprave dostávame

$$g^{-1}g_1 = h_1h_2^{-1} \in H$$

podľa vety 84 dostávame $gH = g_1H$. □

Dôsledok. Množiny $gH, g \in G$ tvoria disjunktný rozklad grupy G.

Množiny gH nazývame **triedy rozkladu** grupy G podľa podgrupy H.

Nasledujúce tvrdenie sa nazýva **Lagrangeova veta**:

Veta 86. Ak G je konečná grupa, ktorá má n prvkov a H je jej podgrupa ktorá má m prvkov tak $m|n$.

Dôkaz. Nech $g_1H, \ldots, g_kH$ sú všetky disjunktné triedy rozkladu grupy G podľa podgrupy H. Podľa lemmy 3 platí

$$G = g_1H \cup \cdots \cup g_kH$$

a teda

$$n = |g_1H| + \cdots + |g_kH|. \tag{54}$$

Teraz dokážeme, že trieda rozkladu má rovnaký počet prvkov ako H. Polo- žme

$$H = \{h_1, \ldots, h_m\}$$

potom pre každé $i = 1, \ldots, k$ platí

$$g_i H = \{g_i h_1, \ldots, g_i h_m\}.$$

Ak $g_i h_j = g_i h_\ell$ tak po vykrátení prvkom g_i dostávame $h_j = h_\ell$ a teda $j = \ell$. Všetky prvky $g_i h_1, \ldots, g_i h_m$ sú teda rôzne preto $|g_i H| = m$. Z rovnosti (54) vyplýva $n = km$. □

5.3 Rád prvku v grupe

Hovoríme, že prvok a grupy G má **konečný rád** práve vtedy ak existuje $n \in \mathbb{N}$ také, že $a^n = e$. Hodnotu

$$\min\{n \in \mathbb{N}; a^n = e\} \tag{55}$$

sa nazýva v takom prípade **rád** prvku a.

Veta 87. Ak $a \in G$ je prvok rádu m, tak pre každé $n \in \mathbb{Z}$ platí

$$a^n = e \iff m|n.$$

Dôkaz. Ak $n = km$ tak $a^n = a^{km} = (a^m)^k = e^k = e$. Teda jednu implikáciu sme dokázali. Nech $n = mq+r$, kde $0 \leq r < m$. Potom z rovnosti $a^n = e$ vylýva

$$e = a^{mq+r} = a^r a^{mq} = a^r (a^m)^q = a^r e = a^r.$$

Teda ak $r > 0$ dostávame spor s minimalitou m. □

5.4 Cyklická podgrupa

Ak G je grupa a $a \in G$ tak množina

$$[a] = \{a^n; n \in \mathbb{Z}\}$$

je podgrupa a nazýva sa **cyklická podgrupa**. Prvok a sa nazýva **generátor** tejto podgrupy. V prípade $G =< a >$ sa grupa G nazýva cyklická.

Veta 88. Ak G je konečná grupa, tak pre každé $a \in G$ platí $a^{|G|} = e$.

Dôkaz. Nech m je rád prvku a. Potom cyklická grupa $[a]$ generovaná týmto prvkom má m prvkov. Preto $m||G|$ a teda $a^{|G|} = e$. □

Toto tvrdenie má dôsledok v elementárnej teórii čísel známe ako **Eulerova veta:**

Nech $n \in N$ a $\phi(n)$ označuje počet prvkov množiny $\{0, \ldots, n-1\}$ ktoré sú nesúdeliteľné s n. Potom

pre každé celé číslo a ktoré je nesúdeliteľné s n platí

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

5.5 Faktorové grupy

Na množine tried rozkladu grupy podľa podgrupy sa dá za istých predpokladov definovať taká operácia, že táto množina bude grupou s touto operáciou.

Ak H je podgrupa grupy G, tak táto podgrupa sa nazýva **normána podgrupa** práve vtedy keď

$$\forall g \in G;\ gHg^{-1} \subset H. \tag{56}$$

Jednoducho sa dá dokázať

Veta 89. H je normálna podgrupa G práve vtedy keď pre každé $g \in G$ platí $gH = Hg$.

Veta 90. Ak H je normálna podgrupa grupy G tak pre každé $g_1, g_2, g_1', g_2' \in G$ platí

$$g_1H = g_2H \wedge g_1'H = g_2'H \Rightarrow g_1g_1'H = g_2g_2'H.$$

Dôkaz. Podľa vety 84 stačí dokázať , že $(g_1'g_2')^{-1}g_1g_2 \in H$. Je zrejmé, že

$$(g_2'g_2')^{-1}g_1g_1' = g_2'^{-1}g_2^{-1}g_1g_1'. \tag{57}$$

Z predpokladov dostávame $g_2^{-1}g_1 \in H$. Ak položíme $h = g_2^{-1}g_1$. Po dosadení do (57) z toho vyplýva

$$(g_2'g_2')^{-1}g_1g_1' = g_2'^{-1}hg_1'.$$

Z toho, že H je normálna podgrupa dostávame $hg_1' = g_1'h_1$ pre nejaké $h_1 \in H$. Teda

$$(g_2'g_2')^{-1}g_1g_1' = g_2'^{-1}g_1'h_1 \in H.$$

□

Z vety 90 vyplýva, že na triedach rozkladu G podľa H môžeme definovať operáciu

$$(gH) \cdot (g'H) = gg'H.$$

Ak označíme symbolom G/H množinu všetkých tried rozkladu G podľa H tak ľahko sa nahliadne, že $(G/H, \cdot)$ je grupa. Táto grupa sa nazýva **faktorová grupa** G podľa H.

5.6 Homorfizmus grúp

Ak G_1, G_2 sú grupy tak zobrazenie

$$\Psi : G_1 \to G_2$$

sa nazýva **homorfizmus** ak zachováva operácie, t.j. pre každé $a, b \in G_1$ platí

$$\Psi(ab) = \Psi(a)\Psi(b).$$

Veta 91. $\Psi(e) = e, \Psi(a^{-1}) = \Psi(a)^{-1}$ **pre každé** $a \in G_1$**.**

Dôkaz tohoto spočíva v jednoduchých úpravách.

Množina $Ker(\Psi) = \{a \in G_1; \Psi(a) = e\}$ sa nazýva **jadro** homorfizmu Ψ.

Zobrazenie $\Gamma : G \to G/H$ kde $\Gamma(g) = gH$ je homorfizmus a nazýva sa **kanonický homorfizmus**. Je zrejmé, že $Ker(\Gamma) = H$.

Bijektívny homomorfizmus medzi grupami sa nazýva **izomorfizmus.** Ak medzi grupami existuje izmorfizmus nazývajú sa **izmorfné**.

Veta 92. Pre každý homorfizmus Ψ **je** $Ker(\Psi)$ **normálnou podgrupou** G_1 **a ak** Ψ **je surjektívne zobrazenie tak faktorová grupa** $G_1/Ker(\Psi)$ **je izomorfná s** G_2**.**

Dôkaz. Je zrejmé, že $e \in Ker(\Psi)$ ak $a, b \in Ker(\Psi)$ tak $\Psi(ab) = \Psi(a)\Psi(b) = ee = e$. Teda $ab \in Ker(\Psi)$. Podobne $bb^{-1} = e$ a teda $e = \Psi(b)\Psi(b^{-1}) = \Psi(b^{-1})$. Preto $b^{-1} \in Ker(\Psi)$. Teda $Ker(\Psi)$ je podgrupa. Ak $c \in G_1, b \in Ker(\Psi)$ tak $\Psi(aba^{-1}) = \Psi(a)\Psi(b)\Psi(a^{-1}) = \Psi(a)\Psi(a^{-1})$ $= \Psi(aa^{-1}) = \Psi(e) = e$. Teda $aba^{-1} \in Ker(\Psi)$. Dokázali sme, že $Ker(\Psi)$ je normalna podgrupa.

Zostrojíme izomorfizmus $\tilde{\Psi} : G_1/Ker(\Psi) \to G_2$. Ak $a_1, a_2 \in G_1$ a $a_1 Ker(\Psi) = a_2 Ker(\Psi)$ tak $a_1 a_2^{-1} \in Ker(\Psi)$ a teda $\Psi(a_1 a_2^{-1}) = e$. To znamená $\Psi(a_1)\Psi(a_2^{-1}) = e$. Preto

$\Psi(a_1) = \Psi(a_2)$. Definujme teda

$$\tilde{\Psi}(a_1 Ker(\Psi)) = \Psi(a_1).$$

Priamo z definície jadra dostávame

$$\tilde{\Psi}(a_1 Ker(\Psi)) = \tilde{\Psi}(a_2 Ker(\Psi)) \Rightarrow$$

$$\Rightarrow a_1 Ker(\Psi) = a_2 Ker(\Psi))$$

Preto $\tilde{\Psi}$ je injektívny homomorfizmus. Ak Ψ je surjektívne zobrazenie tak pre $c \in G_2$ existuje $a \in G_1$, take, že $\Psi(a) = c$ a teda $\tilde{\Psi}(aKer(\Psi)) = c$. Dokázali sme, v ze $\tilde{\Psi}$ je surjekcia a teda aj bijekcia. □

Príklad 86. Ak H je normálna podgrupa grupy G a H_1 je normálna podgrupa G/H, tak $\tilde{H_1} = \{h \in G; hH \in H_1\}$ je normálna podgrupa G a grupy $G/\tilde{H_1}$ a $(G/H)/H_1$ sú izomorfné. Vyplýva to z toho, že zobrazenie $\Psi : G \to (G/H)/H_1$, kde $\Psi(a) = (aH)H_1$ je homorfizmus a $\tilde{H_1} = Ker(\Psi)$.

5.7 Súčin podgrúp

Veta 93. Ak H_1, H_2 su podgrupy nejakej grupy G tak H_1H_2 je podgrupa práve vtedy keď

$$H_1H_2 = H_2H_1. \tag{58}$$

Dôkaz. Ak H_1H_2 je podgrupa a $h_1 \in H_1, h_2 \in H_2$ tak $h_1^{-1}h_2^{-1} \in H_1H_2$. Z podmienky pre podgrupu vyplýva $(h_1^{-1}h_2^{-1})^{-1} \in H_1H_2$ to ale znamená $h_2h_1 \in H_1H_2$, preto $H_2H_1 \subset H_1H_2$. Podobne sa dokáže opačná inklúzia.

Nech platí (58). Je zrejmé, že $e \in H_1H_2$. Ak $a_1, a_2 \in H_1H_2$ tak $a_1 = b_1b_2, b_1 \in H_1, b_2 \in H_2$ a $a_2 = c_1c_2, c_1 \in H_1, c_2 \in H_2$. Potom

$$a_1a_2 = b_1b_2c_1c_2.$$

Ale $b_2c_1 \in H_2H_1$ a teda podľa (58) $b_2c_1 \in H_1H_2$. Teda $b_2c_1 = d_1d_2$ kde $d_1 \in H_1, d_2 \in H_2$. Preto

$$a_1a_2 = (b_1d_1)(d_2c_2) \in H_1H_2.$$

Ak $g_1g_2 \in H_1H_2$ tak $(g_1g_2)^{-1} = g_2^{-1}g_1{-}1 \in H_2H_1$. Z podmienky (58) vyplýva, že $(g_1g_2)^{-1}$. □

Hovoríme, že grupa G je **priamy súčin** podgrúp H_1 a H_2 práve vtedy ak $G = H_1H_2$ a každý prvok G sa dá jediným spôsobom vyjadriť v tvare g_1g_2 kde $g_1 \in H_1, g_2 \in H_2$. Označujeme to

$$G = H_1 \odot H_2.$$

Veta 94. Grupa G je priamym súčinom podgrúp H_1, H_2 práve vtedy keď $G = H_1H_2$ a $H_1 \cap H_2 = \{e\}$.

Dôkaz. Ak $a \in H_1 \cap H_2$ a $a \neq e$ tak $e = ee = aa^{-1}$ teda e sa dá vyjadriť dvomi rôznymi spôsobmi preto G nemôže byť priamym sýčinom H_1H_2.

Nech $H_1 \cap H_2 = \{e\}$ a $h_1h_2 = g_1g_2$, $h_1, g_1 \in H_1$ a $h_2, g_2 \in H_2$. V takom prípade dostávame $g_1^{-1}h_1 = g_2h_2^{-1} \in H_1 \cap H_2$. Preto $g_1^{-1}h_1 = g_2h_2^{-1} = e$, čo znamená $g_1 = h_2.g_2 = h_2$. □

Príklad 87. Ak G je komutatívna grupa a $G = H_1 \odot H_2$ tak G je izomorfná s grupou $H_1 \times H_2$ na ktorej sa operácia definuje po zložkách, teda

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1h_1, g_2h_2).$$

Príklad 88. Ak $G = H_1 \odot H_2$ kde H_1, H_2 sú normálne podgrupy G, tak podľa vety 89 zobrazenie je $\Phi : G \to H_2, \Phi(h_1h_2) = h_2$ je homorfzmus a $Ker\Phi = H_1$. Preto $G/H_1 \sim H_2$.

Ak G je komutatívna grupa $H_1, \ldots, H_k$ sú jej podgrupy, hovoríme, že G je **priamym súčinom** tychto podgrúp práve vtedy ak každý jej prvok g sa dá jednoznačne vyjadriť v tvare

$$g = h_1 \ldots h_k, h_i \in H_i, i = 1, \ldots, k. \tag{59}$$

Označujeme to

$$G = H_1 \odot \cdots \odot H_k.$$

Každá z podgrúp H_i sa potom nazýva **priamym činiteľom** grupy G.

Grupy $H_1, \ldots, H_k$ nazývame **nezávislé** vtedy a len vtedy ak

$$H_i \cap H_1 \ldots H_{i-1} H_{i+1} \ldots H_k = \{e\}.$$

Rovnakým spôsobom ako veta 94 sa dá dokázať

Veta 95. Ak G je komutatívna grupa a $H_1, \ldots, H_k$ sú jej podgrupy tak $G = H_1 \odot \cdots \odot H_k$ vtedy a len vtedy keď $G = H_1 \ldots H_k$ a podgrupy $H_i, i = 1, \ldots, k$ sú nezávislé.

5.8 Cardanov vzorec

Uvažujme kubickú rovnicu

$$y^3 + a_2 y^2 + a_1 y + a_0 = 0.$$

Substitúciou $y = x - \frac{a_2}{3}$ sa táto rovnica dá upraviť na tvar, ktorý neobsahuje kvadratický člen

$$x^3 + px + q = 0. \tag{60}$$

Neznámu si vyjadríme v tvare $x = u + v$. Po dosadení do (60) a úprave dostávame

$$u^3 + v^3 + (u + v)(3uv + p) + q = 0.$$

Môžeme predpokladať, že u, v sme vybrali tak aby platila podmienka

$$3uv + p = 0. \tag{61}$$

Rovnica potom dostane veľmi jednoduchý tvar

$$u^3 + v^3 + q = 0.$$

Ak $u \neq 0$ môžeme dosadiť z (61) $v = \frac{-p}{3u}$. To vedie na rovnicu

$$u^3 - \frac{p^3}{27u^3} + q = 0.$$

Položme $u^3 = U$. Po dosadení a úprave dostávame kvadratickú rovnicu pre U:

$$U^2 + qU - \frac{p}{27} = 0.$$

Ak za U zvolíme jeden koreň tejto rovnice, napríklad

$$U = \frac{1}{2}\Big(- q + \sqrt{q^2 + \frac{4p}{27}}\Big).$$

tak z (61) vyplýva, že V bude druhý koreň. Teda

$$x = \sqrt[3]{\frac{1}{2}\Big(- q + \sqrt{q^2 + \frac{4p}{27}}\Big)} + \sqrt[3]{\frac{1}{2}\Big(- q - \sqrt{q^2 + \frac{4p}{27}}\Big)}.$$

Na pohľad to pôsobí dojmom, že kubická rovnica má jediný koreň. Treba zobrať do úvahy že symbol $\sqrt[3]{\cdot}$ má tri hodnoty.

Ako riešiť rovnicu 4. stupňa? Podobnou substitúciou ako pri kubickej rovnici sa dá upraviť na tvar

$$x^4 = ax^2 + bx + c.$$

Položme $z = x^2 + t$. Potom

$$z^2 = x^4 + 2tx^2 + t^2 = ax^2 + bx + c + 2tx^2 + t^2 =$$

$$= (a + 2t)x^2 + bx + c + t^2.$$

Pri tejto rovnici je výhodné keď výraz na konci je v tvare $(Ax + B)^2$. To docielime tým, že diskriminant tohoto výrazu bude 0 ak ho chápeme ako polynóm neurčitej x. Dostávame tak rovnicu pre t:

$$b^2 - 4(a + 2t)(t^2 + c) = 0$$

čo je kubická rovnica pre t. Ak t je koreň tejto rovnice tak pôvodná rovnica prejde na tvar

$$(x^2 + t)^2 = (Ax + B)^2.$$

A táto sa už dá riešit rozkladom na dve kvadratické rovnice.

5.9 Rozklad permutácií na cykly

Nech n je prirodzené číslo. Permutácia $\pi \in \mathbf{S}_n$ sa nazýva **cyklus** ak existujú navzájom rôzne prvky $x_1, \ldots, x_k$ také, že $x_2 = \pi(x_1), x_3 = \pi(x_2), \ldots x_k = \pi(x_{k-1}), x_1 = \pi(x_k)$, ostatné prvky sú invariantné (to znamená $\pi(a) = a$ ak $a \notin \{x_1, \ldots, x_k\}$). Takúto permutáciu označujeme

$$\pi = (x_1 \ldots x_k).$$

Hodnota k sa nazýva **dĺžka cyklu** π. Cykly $(x_1 \ldots x_k)$, $(y_1 \ldots y_\ell)$ sa nazý- vajú disjunktné práve vtedy keď $\{x_1, \ldots, x_k\} \cap \{y_1, \ldots, y_\ell\} = \emptyset$. Ľahko sa preverí

Veta 96. Disjunktné cykly komutujú

Príklad 89. Ak $m \geq 5$ a $p \neq q$ sú také prvočísla, že $p + q \leq m$ tam grupa $\mathbf{S}_m$ obsahuje dva disjunktné cyklý, jeden dĺžky p a druhý dĺžky q a teda obsahuje cyklickú podgrupu rádu pq.

Veta 97. Každá permutácia sa dá vyjadriť ako súčin disjunktných cyklov

Dôkaz. Nech $\pi \in \mathbf{S}_n$. Uvažujme postupnosť $\pi(1), \pi(\pi(1)), \ldots$. Raz sa v tejto postupnosti vyskytne prvok 1 prvý krát. Tam končí prvý cyklus. Takto postupne vyčerpáme všetky prvky. □

Príklad 90. $\binom{123456}{546312} = (15)(2436)$

Veta 98. Rád súčinu disjunktných cyklov sa rovná najmenšiemu spoločnému násobku ich dĺžok .

Dôkaz. Ak $\pi = \pi_1 \dots \pi_s$ kde $\pi_1, \dots, \pi_s$ su disjunktne cykly tak z toho, že komutujú dostáveme

$$\pi^r = \pi_1^r \dots \pi_s^r.$$

S disjunknosti cyklov vyplýva, že $\pi^r = id$ práve vtedy ked $\pi_i^r = id$ pre všetky $i = 1, \dots, s$. A $\pi_i^r = id$ práve vtedy keď dĺžka π_i je deliteľom r. Z toho vyplýva tvrdenie. □

Cyklus dĺžky dva sa nazýva transpozícia. Pre každý cyklus dĺžky k plati

$$(x_1x_2)(x_1x_3)\dots(x_1x_k) = (x_1 \dots x_k).$$

To znamena, že každá permutácia je súčinom transpozícií . Preto:

Veta 99. Ak podgrupa $G \subset \mathbf{S}_n$ obsahuje všetky transpozície tak $G = \mathbf{S}_n$, pre $n \in \mathbb{N}$.

Transpozícia tvaru $(j-1, j)$ pre $j = 2, \dots, n$ sa nazýva **jednoduchá**.

Veta 100. Ak podgrupa $G \subset \mathbf{S}_n$ obsahuje všetky jednoduché transpozície tak $G = \mathbf{S}_n$.

Dôkaz. Podľa predošlej vety stačí dokázať že daná podgrupa G obsahuje každú transpozíciu $(i,j), i<j, i,j = 1,\ldots,n$.

G určite obsahuje cyklus

$$\lambda = (i, i+i, \ldots, j) =$$

$$= (j-1,j)(j-2,j-1)\ldots(i+1,i+2)(i,i+1).$$

Po jednoduchom výpočte dostávame

$$(i,j) = \lambda(j-1,j)\lambda^{-1}.$$

□

Veta 101. Ak podgrupa $G \subset \mathbf{S}_n$ obsahuje cyklus $(1,2,\ldots,n)$ a transpoziciu $(1,2)$ tak $G = \mathbf{S}_n$.

Dôkaz. Jednoduchým výpočtom môžeme preveriť rov--nosť

$$(1,n) = (1,2,\ldots,n)(1,2)(1,2,\ldots,n)^{-1}$$

a

$$(j-1,j) = (1,2,\ldots,n)^{j-1}(1,2)((1,2,\ldots,n)^{-1})^{j-1}$$

pre $j = 3,\ldots n$. □

Veta 102. Nech p je prvočíslo. Ak podgrupa $G \subset \mathbf{S}_p$ obsahuje cyklus dĺžky p a jednu transpozíciu tak $G = \mathbf{S}_p$.

Dôkaz. Nech (i, j) je spomínaná transpozícia a ρ ja daný cyklus. Existuje také $k \in \mathbb{Z}$, že $\rho^k(i) = j$. Označme $\pi = \rho^k$. Pretože p je prvočíslo je aj π cyklus dĺžky p. Nech

$$\pi = (i, j, x_3, \ldots, x_p).$$

Ak označíme $x_1 = i, x_2 = j$ tak

$$\pi = (x_1, x_2, x_3, \ldots, x_p).$$

Ak uvážime $(i, j) = (x_1, x_2)$ dostávame naše tvrdenie analogickým postupom v dôkaze vety 101. □

5.10 Vietove vzorce

Definujme polynómy n - premenných, pre dané $n \in \mathbb{N}$ nasledujúcim spôsobom

$$\sigma_k = \sum_{j_1 < j_2 < \cdots < j_k} x_{j_1} \ldots x_{j_k}$$

kde $j_1 < j_2 < \cdots < j_k$ prebiehajú všetky k - prvkové podmnožiny množiny $\{1, 2, \ldots, n\}$, $k = 1, \ldots, n$. Napríklad

$$\sigma_n = x_1 \ldots x_n,$$

alebo

$$\sigma_1 = \sum_{j=1}^{n} x_j.$$

Polynóm σ_k má $\binom{n}{k}$ sčítancov.

Ak predpokladáme, že $x_1, \ldots, x_n$ sú korene polynómu $f(x)$ daného rovnosťou (1) a predstavíme si ho v tvare

$$f(x) = a_n(x - x_1) \ldots (x - x_n)$$

tak porovnaním koeficientov dostávame

$$a_j = a_n(-1)^{n-j}\sigma_{n-j}$$

pre $j = 1, \ldots, n$. Tieto rovnosti sa nazývajú **Vietove vzorce**.

Polynóm n neurčitých $h(x_1, \ldots, x_n)$ sa masýva **symetrický** práve vtedy keď

$$h(x_1, \ldots, x_n) = h(x_{\pi(1)}, \ldots, x_{\pi(n)})$$

pre každú permutáciu $\pi \in \mathbf{S}_n$. Hneď vidíme, že polynómy $\sigma_1, \ldots, \sigma_n$ sú symetrické. Postupnými úpravami sa dá dokázať :

Hlavná veta o symetrických polynómoch. Ak $h(x_1, \ldots, x_n)$ **je symetrický polynóm nad poľom** F **tak existuje taký polynóm** $p(y_1, \ldots, y_n)$ **nad poľom** F**, že**

$$h(x_1, \ldots, x_n) = p(\sigma_1, \ldots, \sigma_n).$$

References

[1] Artin, E., *GALOIS THEORY*, DOVER PUBLICATION INC. Mineola, New York, 1998

[2] Battaglia, G., *Il teorema di Wedderbjurn per i corpi finiti*, Seminario di Algebra III, 2008/2009

[3] Besicovitch, A. S., *On the linear independence of fractional powers of integers*, J. London Math. Soc. 15, 1940, 3 - 6

[4] Birghof, B., Mac Lane, S., *Prehľad modernej algebry*, ALFA, Bratislava, 1979

[5] Butin, F., Algebre, polynomes, theorie de Galois et aplication informatiques, Hermann editeurs, Paris, 2012

[6] Escofier, J. P., *Theorie de Galois*, 2 sieme edition, DUNOD, Mayenne, 2004

[7] Herstein, I. N ., *Algebra*, Editori Riuniti, Roma, 1982

[8] Richards, I., *An Application of Galois Theory to Elementary Arithmetics*, Advances in Mathematics 13, 1974, 268 - 273

[9] Jain, A., *Zorn's Lemma An elementary pro of under Axiom of choise* Arxiv

[10] Lidl, L., Nidereiter, H., *Finite Fields*, Cambridge University Press, Cambridge, 1997

[11] Pinter, Ch. C. *A Book of Abstract Algebra*, second edition, Dover Publication. Inc., Mineola, New York, 2013

[12] Weintraub, S., H., *Several proofs of irreducibility of cyclotomic polynomials*

Contents