1. Ideály v oboroch integrity

Zopakujme si definíciu. *Obor integrity* je množina M, na ktorej sú definované binárne operácie $\oplus$ a $\odot$ (sčítanie a násobenie), pričom platí:

(1) $x \oplus y = y \oplus x$ pre každé $x, y \in M$;
(2) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ pre každé $x, y, z \in M$;
(3) existuje $o \in F$ také, že $x \oplus o = x$ pre každé $x \in M$;
(4) pre každé $x \in M$ existuje $y \in M$ také, že $x \oplus y = o$;
(5) $x \odot (y \odot z) = (x \odot y) \odot z$ pre každé $x, y, z \in M$;
(6) $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$, $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$ pre každé $x, y, z \in M$;
(7) $x \odot y = y \odot x$ pre každé $x, y \in M$;
(8) existuje $j \in M$ také, že $j \odot x = x$ pre každé $x \in M$;
(9) pre každé $x, y \in M$, $x, y \neq o$ platí $x \odot y \neq o$.

Najdôležitejšími príkladmi budú pre nás $\mathbb{Z}$ (celé čísla) a $F[x]$, obor integrity polynómov premennej x nad poľom F (s obvyklými operáciami sčítania a násobenia). V ďalšom budeme operácie ľubovoľného oboru integrity označovať obvyklými symbolmi $+$ (sčítanie) a $\cdot$ (násobenie). Prvky o a j budeme označovat 0 a 1. V obore integrity máme definované aj odčítanie: $a - b = a + (-b)$, kde $(-b)$ je opačný prvok ku b, ktorý existuje podľa axiómy (4).

Definícia 1.1. *Nech $(M, +, \cdot)$ je obor integrity. Množina $\emptyset \neq I \subseteq M$ sa nazýva* ideál*, ak platí:*

(I1) $a, b \in I$ *implikuje* $a - b \in I$*;*
(I2) $a \in I$, $x \in M$ *implikuje* $ax \in I$*.*

Pretože ideál je neprázdna množina, existuje $a \in I$ a potom aj $0 = a - a \in I$. Teda každý ideál obsahuje 0. Ďalej, každý ideál je uzavretý aj na súčet. Totiž, keď $a, b \in I$, tak $0 - b \in I$ a tiež $a + b = a - (0 - b) \in I$.

V obore integrity $F[x]$ vieme všetky ideály presne popísať. Pre každý polynóm $p(x) \in F[x]$ označme I_p množinu všetkých násobkov polynómu p, t.j.

$$I_p = \{pf \mid f \in F[x]\}.$$

Veta 1.2. *$I \subseteq F[x]$ je ideál práve vtedy, keď $I = I_p$ pre nejaké $p \in F[x]$.*

D ô k a z. Ľahko sa dokáže, že každé I_p spĺňa podmienky (I1), (I2) a teda je ideálom.

Predpokladajme teraz naopak, že I je ideál. Pokiaľ $I = \{0\}$ (I obsahuje iba nulový polynóm), tak $I = I_0$. Ak I obsahuje aj nenulové polynómy, vyberieme z nich ten, ktorý má najmenší stupeň a označíme ho p. Tvrdíme, že $I = I_p$.

Dokazujeme teda rovnosť dvoch množín. Nech najprv $h \in I_p$. Potom $h = pf$ pre nejaké $f \in F[x]$. Pretože $p \in I$, podmienka (I2) implikuje $h = pf \in I$. To dokazuje $I_p \subseteq I$. Kvôli opačnej nerovnosti predpokladajme $h \in I$. Podľa vety o delení so zvyškom existujú $q, z \in F[x]$ tak, že

$$h = pq + z,$$

pričom $z = 0$ alebo z má menší stupeň ako p. Pretože $p, h \in I$, z definície ideálu dostávame $pq \in I$ a tiež $z = h - pq \in I$. Preto z nemôže mať menší stupeň ako p, a zostáva možnosť $z = 0$, čo znamená $h = pq \in I_p$ a to sme chceli ukázať. ∎

Význam ideálov je v tom, že umožnujú faktorizáciu oborov integrity, podobne ako normálne podgrupy umožnujú faktorizáciu grúp. (Všimnime si, že keď "zabudneme" na násobenie, tak každý ideál je podgrupou aditívnej grupy $(M, +)$, normálnosť vyplýva z komutatívnosti.) Túto konštrukciu si teraz popíšeme. Nech I je ideál oboru integrity M.

Pre každé $x \in M$ definujeme (podobne ako pri grupách) vrstvu určenú prvkom x a ideálom I ako množinu

$$x + I = \{x + a \mid a \in I\}.$$

Kvôli prehľadnosti budeme namiesto $x + I$ používať označenie x_I. Pre každé $x, y \in M$ platí buď $x_I = y_I$ alebo $x_I \cap y_I = \emptyset$. Rovnosť $x_I = y_I$ platí práve vtedy, keď $(x - y) \in I$. (Dôkaz je rovnaký ako pre grupy.) Teda vrstvy podľa ideálu I tvoria rozklad oboru integrity M. Množinu všetkých vrstiev označíme M/I.

Lema 1.3. *Pre každé $x, y, u, v \in M$ platí:*

(1) *ak $x_I = y_I$, $u_I = v_I$, tak $(x + u)_I = (y + v)_I$;*
(2) *ak $x_I = y_I$, $u_I = v_I$, tak $(xu)_I = (yv)_I$.*

D ô k a z. Dôkaz (1) je rovnaký ako pri grupách. Overíme (2). Z rovností $x_I = y_I$, $u_I = v_I$ vyplýva $x - y \in I$, $u - v \in I$. Potom

$$xu - yv = xu - xv + xv - yv = x(u - v) + (x - y)v.$$

Podľa (I2) máme $x(u-v), (x-y)v \in I$, teda aj $xu-yv \in I$, čo znamená $(xu)_I = (yv)_I$. ∎

Predošlé tvrdenie nám umožňuje definovať operácie na M/I pomocou reprezentantov:

$$x_I + u_I = (x + u)_I$$

$$x_I \cdot u_I = (xu)_I.$$

Veta 1.4. *Množina M/I s vyššie definovanými operáciami spĺňa axiómy (0)-(8) z definície oboru integrity.*

D ô k a z. Platnosť všetkých axióm pre M/I vyplýva z ich platnosti pre M. Na ilustráciu uvažujme napríklad zákon opačných prvkov (4). Nech $x_I \in M/I$. Prvok $x \in M$ má v M opačný y, t.j. $x + y = 0$. Potom ale $x_I + y_I = (x+y)_I = 0_I$, takže v M/I je prvok y_I opačný ku x_I. ∎

Axióma (9) v M/I nemusí byť splnená. (Pozri príklad nižšie.) Splnenie axióm (1)-(8) znamená, že faktorizáciou oboru integrity vždy dostaneme komutatívny okruh s jednotkou.

So špeciálnym prípadom faktorizácie sme sa už stretli, v podobe okruhu zvyškových tried. Celé čísla tvoria obor integrity $\mathbb{Z}$. Zvoľme kladné celé n a uvažujme množinu I všetkých celočíselných násobkov n. Ľahko vidno, že I je ideál, vrstvy podľa I sú zvyškové triedy a naše operácie s vrstvami presme zodpovedajú operáciám so zvyškovými triedami. Takže $\mathbb{Z}/I$ nie je nič iné, ako náš známy okruh $\mathbb{Z}_n$.

Tu zároveň máme príklad, že faktorizáciou oboru integrity môžeme dostať okruh, ktorý nie je oborom integrity. Pokiaľ n nie je prvočíslo, tak $\mathbb{Z}_n$ nie je obor integrity (napr. $2_6 \cdot 3_6 = 0_6$).

2. Faktorizácia oboru integrity $F[x]$

Ak n je prvočíslo, tak okruh $\mathbb{Z}_n$ je obor integrity (dokonca pole). Teraz si dokážeme analógiu tohoto tvrdenia pre obor integrity $F[x]$. (F je ľubovoľné pole.) Už sme videli, že každý ideál v $F[x]$ je množina I_p všetkých násobkov polynómu p.

Veta 2.1. *Ak $p \in F[x]$ je ireducibilný, tak okruh $F[x]/I_p$ je pole. Ak p je reducibilný, tak $F[x]/I_p$ nie je ani obor integrity.*

D ô k a z. 1. Nech p je ireducibilný. Máme dokázať, že ku každému prvku $f_{I_p} \in F[x]/I_p$ rôznemu od 0_{I_p} $(= I_p)$ existuje inverzný. Nerovnosť $f_{I_p} \neq 0_{I_p}$ znamená, že $f \notin I_p$, teda f nie je násobkom p. Pretože p je ireducibilný, polynómy p a f musia byť nesúdeliteľné. Podľa vety o NSD potom existujú $u, v \in F[x]$ tak, že $fu + pv = 1$. Tvrdíme, že u_{I_p} je hľadaný inverzný prvok. Naozaj, pretože $p_{I_p} = 0_{I_p}$, tak máme

$$f_{I_p} u_{I_p} = (fu)_{I_p} = (1 - pv)_{I_p} = 1_{I_p} - 0_{I_p} v_{I_p} = 1_{I_p}.$$

2. Nech p nie je ireducibilný. Potom $p = uv$, kde žiaden z polynómov u, v nie je násobkom p. Teda $u, v \notin I_p$, čo znamená $u_{I_p}, v_{I_p} \neq 0_{I_p}$. Pritom ale $u_{I_p} v_{I_p} = p_{I_p} = 0_{I_p}$, takže axióma (9) nie je splnená. ∎

3. Izomorfizmy polí

Nech F_1 a F_2 sú polia. Funkcia $\varphi : F_1 \to F_2$ sa nazýva *izomorfizmus* ak je bijektívna a zachováva operácie, t.j. pre každé $x, y \in F_1$ platí

$$\varphi(x + y) = \varphi(x) + \varphi(y);$$

$$\varphi(x \cdot y) = \varphi(x \cdot \varphi(y).$$

Izomorfizmus $F \to F$ sa nazýva *automorfizmus* poľa F.

Ľahko sa overí, že pre každý izomorfizmus platí tiež $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(-x) = -\varphi(x)$ a $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Napríklad identické zobrazenie je vždy automorfizmus. Komplexné združovanie je automorfizmus poľa komplexných čísel.

Hovoríme, že $\varphi : F \to F$ zachováva prvok $a \in F$ ak $\varphi(a) = a$. Hovoríme, že φ zachováva množinu $A \subseteq F$ ak $\varphi(a) = a$ pre každé $a \in A$.

Často budeme využívať nasledujúce tvrdenie:

Veta 3.1. *Nech $\varphi : F \to F$ je automorfizmus, ktorý zachováva koeficienty polynómu f. Ak $u \in F$ je koreňom f, tak $\varphi(u)$ je tiež koreňom f.*

D ô k a z. Nech $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Potom

$$f(\varphi(u)) = a_0 + a_1\varphi(u) + \cdots + a_n\varphi(u)^n = \varphi(a_0) + \varphi(a_1 u) + \cdots + \varphi(a_n u^n) =$$

$$= \varphi(a_0 + a_1 u + \cdots + a_n u^n) = \varphi(0) = 0.$$

∎

So špeciálnym prípadom tejto vety sme sa už stretli: Ak polynóm s reálnymi koeficientmi má komplexný koreň $a + bi$, tak má aj koreň $a - bi$. Dôkaz využíva fakt, že komplexné združovanie je automorfizmus $\mathbb{C}$, ktorý zachováva $\mathbb{R}$.

4. Rozšírenia polí

Pole K sa nazýva *rozšírením* poľa F, ak $F \subseteq K$ a súčet aj súčin prvkov z F je definovaný v K tak isto ako vo F. V takom prípade tiež hovoríme, že F je *podpole* poľa K.

Napríklad $\mathbb{R}$ je rozšírením $\mathbb{Q}$. Podobne, $\mathbb{C}$ je rozšírením $\mathbb{R}$, ale aj $\mathbb{Q}$. Ako čoskoro uvidíme, každé pole sa dá rozšíriť.

Nech K je rozšírenie F. Prvok $u \in K$ sa nazýva *algebraický* nad F, ak je koreňom nejakého polynómu s koeficientmi vo F. V opačnom prípade sa u nazýva *transcendentný* nad F.

Napríklad $\sqrt{2} \in \mathbb{R}$ je algebraický nad $\mathbb{Q}$, lebo je koreňom polynómu $x^2 - 2$. Ludolfovo číslo $\pi \in \mathbb{R}$ je transcendentné nad $\mathbb{Q}$. (Dôkaz je zložitý.)

S jedným dôležitým príkladom rozšírenia poľa sme sa stretli v predošlom odseku. Nech p je polynóm ireducibilný nad F, nech I_p je ideál všetkých násobkov p. Potom faktorový okruh $F[x]/I_p$ je pole, ktoré možno považovať za rozšírenie poľa F, pokiaľ prvky $c \in F$ stotožníme s prvkami $c_p \in F[x]/I_p$. (Presnejšie povedané, prvky tvaru c_p, kde c je 0 alebo polynóm stupňa 0, tvoria podpole poľa $F[x]/I_p$ a toto podpole je izomorfné s F.)

Všimnime si, že prvok x_p v $F[x]/I_p$ je algebraický nad F, pretože je koreňom polynómu p: $p(x_p) = p(x)_p = 0_p$.

A ešte si všimnime, že ak p má stupeň 1, tak každý prvok v $F[x]/I_p$ je tvaru c_p ($c \in F$), takže $F[x]/I_p$ je izomorfné s F - žiadne nové prvky sa neobjavili. Preto napríklad pole $\mathbb{C}$ sa týmto spôsobom zväčšiť nedá.

Teraz sa pozrieme na podobnú konštrukciu rozšírenia, ktorá však produkuje transcendentné prvky. Nech F je pole. Označme $\mathrm{Rac}(F, t)$ množinu všetkých *racionálnych foriem* nad F s premennou t, t.j. výrazov tvaru $f(t)/g(t)$, kde $f(t)$ a $g(t)$ sú polynómy nad F a $g(t) \neq 0$. Pritom formy $f_1(t)/g_1(t)$ a $f_2(t)/g_2(t)$ považujeme za rovnaké, ak platí rovnosť polynómov $f_1(t)g_2(t) = f_2(t)g_1(t)$. Operácie s racionálnymi formami robíme rovnako ako s racionálnymi číslami:

$$\frac{f_1(t)}{g_1(t)} + \frac{f_2(t)}{g_2(t)} = \frac{f_1(t)g_2(t) + f_2(t)g_1(t)}{g_1(t)g_2(t)},$$

$$\frac{f_1(t)}{g_1(t)} \cdot \frac{f_2(t)}{g_2(t)} = \frac{f_1(t)f_2(t)}{g_1(t)g_2(t)}.$$

L'ahko sa overí, že $\mathrm{Rac}(F, t)$ s týmito operáciami je pole. (Je to tá istá konštrukcia, ktorou definujeme $\mathbb{Q}$ pomocou $\mathbb{Z}$.)

Pole $\mathrm{Rac}(F, f)$ môžeme opäť považovať za rozšírenie poľa F. (Prvok $c \in F$ možno stotožniť s formou $c/1$.) Prvok $t/1$ je tu teraz transcendentný: nie je koreňom polynómu nad F. Skutočne, ak $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, tak rovnosť $f(t) = 0$ by znamenala, že formy $f(t)/1$ a $0/1$ sa rovnajú, teda že polynómy $f(t) \cdot 1$ a $0 \cdot 1$ sa rovnajú, takže f by musel byť nulový.

Poznamenajme, že pomocou racionálnych foriem možno rozšíriť každé pole, napríklad aj $\mathbb{C}$.

Nech teraz $u \in K$ je algebraický prvok nad F. Medzi polynómami nad F, ktorých je u koreňom, existuje taký ktorý je normovaný a má najmenší možný stupeň. Budeme ho nazývať *minimálny polynóm* prvku u. Jeho jednoznačnosť vyplýva z nasledujúcej vety.

Veta 4.1. *Nech K je rozšírenie poľa F, nech m je minimálny polynóm prvku $u \in K$. Pre každý polynóm $f \in F[x]$ platí, že ak $f(u) = 0$, tak $m|f$.*

D ô k a z. Podľa vety o delení so zvyškom máme $f(x) = m(x)p(x) + z(x)$. Pretože $m(u) = f(u) = 0$, dostávame $z(u) = 0$. Keby stupeň z bol menší ako stupeň m, bolo by to v rozpore s tým, ako sme m vyberali. Preto jediná možnosť je $z = 0$. ∎

Stupeň mimimálneho polynómu prvku u budeme tiež stručnejšie nazývať stupňom u. Prvky $u \in F$ majú stupeň 1 (minimálny polynóm je $x - u$), prvky $u \notin F$ musia mať stupeň väčší ako 1.

Veta 4.2. *Normovaný polynóm p s koreňom u je minimálnym polynómom prvku $u \in K$ nad F prave vtedy, keď je nad F ireducibilný.*

D ô k a z. Keďže $p(u) = 0$, tak podľa predošlej vety je p deliteľné minimálnym polynómom. Keď je p ireducibilný, je to možné len tak, že tie polynómy sa rovnajú.

Obrátene, ak p je reducibilný, tak $p = fg$, kde f aj g majú menší stupeň ako p. Z rovnosti $p(u) = 0$ vyplýva, že $f(u) = 0$ alebo $g(u) = 0$, takže p nemá najmenší možný stupeň, nie je minimálny. ∎

5. Jednoduché rozšírenia

Nech K je rozšírenie poľa F, nech $u \in K$. Označme $F(u)$ množinu všetkých prvkov K, ktoré sa dajú vyjadriť v tvare $f(u)/g(u)$ pre nejaké polynómy $f, g \in F[x]$, $g(u) \neq 0$.

Veta 5.1. *$F(u)$ je pole. Ak u je transcendentný prvok, tak $F(u)$ je izomorfné s poľom $\mathrm{Rac}(F, t)$. Ak u je algebraický, s minimálnym polynómom p, tak $F(u)$ je izomorfné s poľom $F[x]/I_p$ a každý prvok $v \in F(u)$ sa dá vyjadriť v tvare*

$$v = a_0 + a_1 u + \cdots + a_{n-1} u^{n-1},$$

kde n je stupeň p.

D ô k a z. Je zrejmé, že $F(u)$ je pole. Predpokladajme, že u je transcendentný a definujme zobrazenie $\varphi : \mathrm{Rac}(F, t) \to F(u)$ predpisom

$$\varphi\left(\frac{f(t)}{g(t)}\right) = \frac{f(u)}{g(u)}.$$

Toto zobrazenie je korektne definované: ak $f_1(t)/g_1(t) = f_2(t)/g_2(t)$, tak platí rovnosť polynómov $f_1(t)g_2(t) = f_2(t)g_1(t)$ a potom aj $f_1(u)g_2(u) = f_2(u)g_1(u)$ (rovnosť prvkov v K) a potom aj $f_1(u)/g_1(u) = f_2(u)/g_2(u)$.

Tvrdíme, že φ je izomorfizmus. Ľahko sa ukáže, že φ zachováva operácie a je surjektívne. Ukážeme, že je prosté. Predpokladajme sporom, že $f_1(t)/g_1(t) \neq f_2(t)/g_2(t)$, ale $f_1(u)/g_1(u) = f_2(u)/g_2(u)$. Potom $f_1(u)g_2(u) - f_2(u)g_2(u) = 0$, čo znamená, že u je koreňom nenulového polynómu $f_1(t)g_2(t) - f_2(t)g_2(t)$, a to je spor s transcendentnosťou.

Predpokladajme teraz, že u je algebraický a má minimálny polynóm p. Dokážeme najprv poslednú časť nášho tvrdenia. Nech

$$v = \frac{f(u)}{g(u)} \in F(u).$$

Pretože $g(u) \neq 0$, polynóm g nie je deliteľný p. Pretože p ako minimálny polynóm musí byť ireducibilný, polynómy g a p sú nesúdeliteľné. Preto existujú polynómy $r, s \in F[x]$ tak, že

$$1 = gr + ps.$$

Dosadením u do tejto rovnosti dostávame

$$1 = g(u)r(u) + p(u)s(u) = g(u)r(u)$$

(lebo $p(u) = 0$). Takže

$$v = \frac{f(u)}{g(u)} = f(u)r(u).$$

Teraz polynóm fr vydelíme polynómom p. Dostaneme podiel q a zvyšok z, teda $fr = pq + z$, kde $z = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ (koeficienty a_i môžu byť aj 0). Potom

$$v = f(u)r(u) = p(u)q(u)+z(u) = z(u) = a_0+a_1u+a_2u^2+\cdots+a_{n-1}u^{n-1},$$

čo sme chceli dokázať.

Definujme teraz zobrazenie $\varphi: \ F[x]/I_p \to F(u)$ predpisom

$$\varphi(f_p) = f(u) \quad \text{pre každé } f \in F[x].$$

Toto zobrazenie je korektne definované: ak $f_p = g_p$, tak $f-g$ je násobok p, t.j. $f-g = pq$. Potom $f(u)-g(u) = p(u)q(u) = 0$, teda $f(u) = g(u)$.

Overme teraz zachovanie súčtu (pre súčin je to podobné). Nech $f, g \in F[x]$. Potom

$$\varphi(f_p + g_p) = \varphi((f+g)_p) = (f+g)(u) = f(u) + g(u) = \varphi(f_p) + \varphi(g_p).$$

Surjektívnosť φ sme už dokázali: každý prvok $v \in F(u)$ sa rovná $z(u) = \varphi(z_p)$ pre nejaké $z \in F[x]$. Ostáva ukázať injektívnosť. Nech $f_p \neq g_p$. Potom $f - g$ nie je deliteľné p, takže u nemôže byť koreňom $f - g$. To znamená $f(u) \neq g(u)$, čiže $\varphi(f_p) \neq \varphi(g_p)$. ∎

Ešte trochu terminológie. Hovoríme, že pole $F(u)$ je *jednoduché rozšírenie poľa F generované prvkom u*. Tiež sa zvykne hovoriť, že $F(u)$ vzniklo *adjunkciou* alebo *adjungovaním* prvku u k poľu F.

Jedným z dôsledkov práve dokázanej vety je, že o jednoduchom rozšírení $F(u)$ môžeme hovoriť aj bez vopred daného poľa K. Môžeme napríklad pracovať s poľom $\mathbb{Z}_5(u)$, kde u je koreňom polynómu $p(x) = x^3+x+1$. Prvky tohoto poľa sú všetky výrazy tvaru $a_0+a_1u+a_2u^2$, t.j. všetky polynómy z $F[u]$ stupňa najviac 2. Výpočty sa robia "modulo p", napríklad

$$(u^2+1)(2u^2+u) = 2u^4+u^3+2u^2+u = p(u)(2u+1)+(3u+4) = 3u+4,$$

keďže $p(u) = 0$.

Iným dôsledkom je, že ak prvky u, v majú nad F ten istý minimálny polynóm p, tak polia $F(u)$ a $F(v)$ sú izomorfné: obe polia sú totiž izomorfné s poľom $F[x]/I_p$. Naprí klad $\mathbb{Q}(\sqrt[3]{2})$ je izomorfné s $\mathbb{Q}(\sqrt[3]{2}j)$, kde $j = 1/2 + i\sqrt{3}/2$ je komplexná 3. odmocnina z jednotky.

Zovšeobecnením jednoduchých rozšírení sú *viacnásobné rozšírenia*. Nech $F \subseteq K$, $u_1, \ldots, u_n \in K$. Položíme $F_0 = F$, $F_1 = F_0(u_1)$, $F_2 = F_1(u_2)$, $\ldots$, $F_n = F_{n-1}(u_n)$. Pole F_n sa označuje $F(u_1, \ldots, u_n)$ a nazývame ho rozšírením F, ktoré je generované prvkami $u_1, \ldots, u_n$. Nazýva sa algebraické, ak všetky u_i sú algebraické. V takom prípade sa každý prvok poľa $F(u_1, \ldots, u_n)$ dá vyjadriť v tvare $h(u_1, \ldots, u_n)$, kde h je polynóm n premenných nad F.(To vyplýva z vety 5.1 použitej postupne na polia $F_1, F_2, \ldots, F_n$.

6. Konečné rozšírenia

Nech K je rozšírenie poľa F. Pole K je potom aj vektorový priestor nad F. To znamená, prvky K sú vektory a prvky F skaláre. Preto môžeme využiť poznatky z teórie vektorových priestorov.

Definícia 6.1. *K je* konečným rozšírením *F ak K je konečnorozmený vektorový priestor nad F.*

Napríklad $\mathbb{C}$ je konečným rozšírením $\mathbb{R}$. (Dimenzia je 2 - do bázy môžu ísť napr. vektory 1 a i.) Na druhej strane, $\mathbb{R}$ nie je konečným rozširením $\mathbb{Q}$.

Veta 6.2. *Ak K je konečné rozšírenie F, tak každý prvok K je nad F algebraický.*

D ô k a z. Nech n je dimenzia K nad F. Uvažujme ľubovoľné $u \in K$. Pretože K je pole, máme $1, u, u^2, u^3, \ldots, u^n \in K$. To je

ale $n+1$ vektorov v n-rozmernom priestore, takže musia byť lineárne závislé. To znamená, že existujú skaláre $a_0, a_1, \ldots, a_n \in F$ tak, že

$$a_0 \cdot 1 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$$

a nie všetky a_i sú 0. Takže u je koreňom nenulového polynómu $a_0 + a_1 x + \cdots + a_n x^n$. ∎

Takže $\mathrm{Rac}(F, t)$ nie je konečným rozšírením F, lebo obsahuje transcendentné prvky.

Ak K je konečné rozšírenie F, tak dimenzia K nad F sa nazýva aj *stupeň rozšírenia* a označuje $[K : F]$.

Veta 6.3. *Nech polynóm p je ireducibilný nad F, u jeho koreň. Potom $F(u)$ je konečné rozšírenie F a jeho stupeň je rovný stupňu p.*

D ô k a z. Nech n je stupeň p. Tvrdíme, že $\{1, u, u^2, \ldots, u^{n-1}\}$ je báza $F(u)$ nad F. Podľa vety 5.1 sa každý vektor (prvok poľa $F(u)$) dá vyjadriť v tvare $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}$. Teda každý vektor je lineárnou kombináciou vektorov 1, $u, \ldots, u^{n-1}$. Ďalej, tieto vektory sú lineárne nazávislé, lebo rovnosť $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} = 0$ (kde nie všetky a_i sú 0) by znamenala, že u je koreňom polynómu stupňa nižšieho ako n - spor s minimálnosťou p. Takže $F(u)$ má nad F bázu s n prvkami. ∎

Veta 6.4. *Nech K je konečné rozšírenie F a L je konečné rozšírenie K. Potom L je konečné rozšírenie F a platí $[L : F] = [L : K] \cdot [K : F]$.*

D ô k a z. Nech $\{b_1, \ldots, b_n\}$ je báza K nad F a $\{c_1, \ldots, c_m\}$ báza L nad K. Tvrdí me, že všetky prvky tvaru $b_i c_j$ tvoria bázu L nad F.

Overme najprv nezávislosť. Nech

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} b_i c_j = 0,$$

kde $a_{ij} \in F$. Táto rovnosť sa dá napísať v tvare

$$\alpha_1 c_1 + \alpha_2 c_2 + \cdots + \alpha_m c_m = 0,$$

kde

$$\alpha_j = a_{1j} b_1 + a_{2j} b_2 + \cdots + a_{nj} b_n \in K.$$

Z nezávislosti vektorov $c_1, \ldots, c_m$ vyplýva, že $\alpha_j = 0$ pre každé j, takže

$$a_{1j} b_1 + a_{2j} b_2 + \cdots + a_{nj} b_n = 0.$$

Nezávislosť vektorov $b_1, \ldots, b_n$ teraz znamená, že všetky a_{ij} sú 0.

Takže množina všetkých prvkov $b_i c_j$ je nezávislá. Ukážeme teraz, že generuje L. Nech $u \in L$. Pretože $\{c_1, \ldots, c_m\}$ je báza L nad K, platí

$$u = \alpha_1 c_1 + \alpha_2 c_2 + \cdots + \alpha_m c_m$$

pre nejaké $a_1, \ldots, \alpha_m \in K$. Pretože $b_1, \ldots, b_n$ je báza K nad F, existujú $a_{1j}, \ldots, a_{nj} \in F$ tak, že

$$\alpha_j = a_{1j} b_1 + a_{2j} b_2 + \cdots + a_{nj} b_n.$$

Spojením posledných dvoch rovností dostávame, že u je lineárna kombinácia a_{ij}.

Takže prvky $b_i c_j$ naozaj tvoria bázu. Ich počet je $mn = [L : K] \cdot [K : F]$. ∎

Ako dôsledok dostávame, že každé viacnásobné algebraické rozšírenie je konečné.

7. Euklidovské konštrukcie

Urobíme teraz odbočku a ukážeme, ako sa doteraz získané poznatky dajú využit na riešenie (resp. dokázanie neriešiteľnosti) niektorých klasických geometrických problémov. Týkajú sa toho, čo všetko je možné skonštruovať pomocou pravítka a kružidla. (Také konštrukcie voláme euklidovské.)

Prijmeme nasledujúci fakt: Dĺžka každej úsečky, ktorú môžeme zostrojiť pravítkom a kružidlom sa dá vyjadriť pomocou racionálnych čísel pomocou sčítania, odčítania, násobenia, delenia a druhej odmocniny. (Pričom tieto operácie môžeme požiť opakovane, takže napr. vieme urobiť štvrtú odmocninu.)

Zdvojenie kocky. Máme zostrojiť kocku, ktorá má dvojnásobný objem ako daná kocka.

Môžeme predpokladať, že hrana danej kocky má dĺžku 1. (To závisí len od voľby jednotky dĺžky.) Je jasné, že hrana kocky s dvojnásobným objemom má potom dĺžku $\sqrt[3]{2}$. Úloha teda žiada, aby sme pravítkom a kružidlom zostrojili úsečku dĺžky $\sqrt[3]{2}$. Dokážeme, že sa to nedá.

Predpokladajme sporom, že sa to dá. Potom existuje konečná postupnosť čísel $a_1, a_2, \ldots, a_n$ tak, že každé a_i je buď racionálne, alebo je získané z predchádzajúcich pomocou niektorej z operácií $+, -, \cdot, /$ a $\sqrt{}$, a že a_n sa rovná $\sqrt[3]{2}$. Uvažujme postupnosť polí $F_0, F_1, F_2, \ldots, F_n$, kde $F_0 = \mathbb{Q}$, $F_1 = F_0(a_1)$, $F_2 = F_1(a_2), \ldots, F_n = F_{n-1}(a_n)$. Každé F_i $(i > 0)$ je jednoduchým rozšírením predchádzajúceho a $[F_i : F_{i-1}]$ je buď 1 (to jest, $F_i = F_{i-1}$, takže vlastne k žiadnemu skutočnému

rozšíreniu na tomto kroku nedošlo), alebo 2. Prípad $[F_i : F_{i-1}] = 2$ nastane práve vtedy, keď $a_i \notin F_{i-1}$ a a_i je druhou odmocninou nejakého prvku z F_{i-1}. Podľa viet z predošlej kapitoly je pole F_n konečným rozšírením poľa $\mathbb{Q}$ stupňa

$$[F_n : F_0] = [F_1 : F_0] \cdot [F_2 : F_1] \cdot \cdots \cdot [F_n : F_{n-1}] = 2^k$$

pre vhodné k. Na druhej strane, F_n obsahuje $a_n = \sqrt[3]{2}$, takže je aj rozšírením poľa $\mathbb{Q}(\sqrt[3]{2})$ a musí platiť

$$[F_n : F_0] = [\mathbb{Q}(\sqrt[3]{2}) : F_0] \cdot [F_n : \mathbb{Q}(\sqrt[3]{2})] = 3 \cdot [F_n : \mathbb{Q}(\sqrt[3]{2})].$$

To je spor, lebo 3 nedelí 2^k.

Trisekcia uhla. Máme pomocou pravítka a kružidla rozdeliť daný uhol na 3 rovnaké časti.

Opäť dokážeme neriešiteľnosť úlohy. Konkrétne, ukážeme, že uhol 30^o sa pravítkom a kružidlom nedá rozdeliť na 3 rovnaké časti. (Niektoré iné uhly, napr. 90^o, sa rozdeliť dajú.) Ak by sme vedeli zostrojiť uhol 10^o, vedeli by sme aj zostrojiť úsečku dĺžky $\sin 10^o$.

Podľa známych vzorcov máme

$$\sin 3\alpha = \sin(2\alpha + \alpha) = \sin 2\alpha \cos\alpha + \cos 2\alpha \sin\alpha =$$

$$= 2\sin\alpha\cos^2\alpha + (1 - 2\sin^2\alpha)\sin\alpha = 3\sin\alpha - 4\sin^3\alpha.$$

Dosadením $\alpha = 10^o$ dostávame, že $\sin\alpha$ je koreňom polynómu $4x^3 - 3x + 1/2$. Ľahko sa možno presvedčiť, že tento polynóm je nad $\mathbb{Q}$ ireducibilný, teda číslo $u = \sin 10^o$ je algebraický prvok nad $\mathbb{Q}$ stupňa 3, takže $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Zvyšok dôkazu je rovnaký ako pre zdvojenie kocky. (Pričom u bude hrať úlohu $\sqrt[3]{2}$.)

Kvadratúra kruhu. Máme pomocou pravítka a kružidla nakresliť štvorec, ktorý má rovnaký obsah ako daný kruh.

Môžeme zvoliť jednotku dĺžky tak, aby polomer kruhu bol 1. Obsah kruhu potom bude π, takže máme zostrojiť štvorec o strane $\sqrt{\pi}$. Argument prečo sa to nedá je podobný ako v predošlých dvoch prípadoch. Každá úsečka, ktorú vieme zostrojiť, má dĺžku, ktorá patrí do nejakého konečného rozšírenia poľa $\mathbb{Q}$ (stupňa 2^k). Keďže π je transcendentné, nemôže patriť do takého rozšírenia. A potom tam nemôže patriť ani $\sqrt{\pi}$.

8. Algebraické čísla

Veta 8.1. *Nech pole K je rozšírením poľa F. Nech A je množina tých prvkov K, ktoré sú algebraické nad F. Potom A je pole.*

D ô k a z. Treba dokázať, že ak $a, b \in A$, tak aj $a + b \in A$, $ab \in A$, $-a \in A$ a (ak $a \neq 0$) $a^{-1} \in A$.

Pretože a, b sú algebraické, tak $F(a, b)$ je konečné rozšírenie F. Nech jeho stupeň je n. Označme $c = a + b$. Potom $1, c, c^2, \ldots, c^n \in F(a, b)$ musia byť lineárne závislé, preto existujú $a_0, a_1, \ldots, a_n \in F$ tak, že $a_0 + a_1 c + \cdots + a_n c^n = 0$ a nie všetky a_i sú 0. Takže prvok c je algebraický. Dôkaz pre súčin, opačný a inverzný prvok je podobný. ∎

Algebraické čísla sú tie komplexné čísla, ktoré sú koreňmi polynómov a racionálnymi koeficientmi. V našej novej terminológii algebraické čísla sú algebraické prvky $\mathbb{C}$ nad $\mathbb{Q}$. Z predchádzajúcej vety dostávame dôsledok.

Veta 8.2. *Algebraické čísla tvoria pole.*

Teraz ešte ukážeme, že pole algebraických čísel má podobnú vlastnost ako $\mathbb{C}$.

Lema 8.3. *Každý koreň polynómu s algebraickými koeficientmi je algebraické číslo.*

D ô k a z. Nech u je koreňom polynómu $a_0 + a_1 x + \cdots + a_n x^n$, kde všetky a_i sú algebraické. Potom $K = \mathbb{Q}(a_0, a_1, \ldots, a_n)$ je konečné rozšírenie poľa $\mathbb{Q}$ a $K(u)$ je konečné rozšírenie poľa K. Podľa vety 6.4 je $K(u)$ konečné rozšírenie $\mathbb{Q}$ a podla vety 6.2 je každý jeho prvok, špeciálne aj u, algebraický nad $\mathbb{Q}$. ∎

Podľa hlavnej vety algebry má každý polynóm stupňa aspoň 1 nad $\mathbb{C}$ koreň v $\mathbb{C}$. Keď ten polynóm má algebraické koeficienty, tak podľa 8.3 je ten koreň algebraický. Dostávame nasledujúci dôsledok.

Veta 8.4. *Každý polynóm s algebraickými koeficientmi stupňa aspoň* 1 *má v poli algebraických čísel koreň.*

9. Rozkladové polia

Definícia 9.1. *Nech f je polynóm nad F. Pole $N \supseteq F$ sa nazýva rozkladovým poľom f nad F ak*

(i) *f sa nad N rozkladá na súčin polynómov 1.stupňa;*
(ii) *N je nad F generované koreňmi polynómu f, t.j. $N = F(u_1, \ldots, u_n)$, kde $u_1, \ldots, u_n$ sú korene f.*

Rozkladové pole vždy existuje (jednoznačnosť prediskutujeme neskôr). Je to zrejme konečné rozšírenie poľa F. Podmienka (ii) znamená, že každý prvok $x \in N$ sa dá vyjadriť v tvare $x = h(u_1, \ldots, u_n)$, kde h je nejaký polynóm n premenných s koeficientmi z F.

Postup pri hľadaní rozkladového poľa je nasledovný. Rozložíme f na ireducibilné činitele nad F. Ak sú všetky činitele 1. stupňa, tak rozkladové pole je $N = F$. Ak sa v rozklade vyskytuje činiteľ $p(x)$ stupňa aspoň 2, tak ku F adjungujeme koreň u, polynómu p, t.j. vytvoríme $F(u)$. Potom nájdeme rozklad f na ireducibilné činitele nad $F(u)$. Ak sú teraz všetky činitele lineárne, tak $N = F(u)$. Ak stále existuje nelineárny činiteľ $q(x)$, tak k poľu $F(u)$ adjungujeme jeho koreň v, t.j. vytvoríme $F(u, v)$, a rozložíme f nad $F(u, v)$. Tieto kroky opakujeme dovtedy, kým nedostaneme rozklad f na činitele 1. stupňa.

Výpočtová zložitosť tohto postupu záleží na tom, ako efektívne vieme rozkladať polynómy nad F a nad rozšíreniami F. Ukážeme si výpočet na príklade polynómu $f(x) = x^4 - 2$ nad $\mathbb{Q}$. Tento polynóm je nad $\mathbb{Q}$ ireducibilný, takže adjungujeme jeho koreň $u = \sqrt[4]{2}$. Pole $\mathbb{Q}(u)$ je rozšírenie 4. stupňa a f sa nad ním rozkladá

$$f(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2}).$$

Vidíme, že rozklad obsahuje nelineárny činiteľ $p(x) = x^2 + \sqrt{2}$, treba teda ešte adjungovať jeho koreň $v = i\sqrt[4]{2}$. Je to rozšírenie stupňa 2, takže $\mathbb{Q}(u, v)$ je rozšírenie stupňa 8. Polynóm f už v ňom má všetky svoje korene, takže je to rozkladové pole. Opis tohoto poľa možno ešte trochu zjednodušiť, keď si všimneme, že $v = iu$, takže $\mathbb{Q}(u, v) = \mathbb{Q}(u, i)$.

Lema 9.2. *Nech $\varphi : F_1 \to F_2$ je izomorfizmus polí. Predpokladajme, že φ zobrazuje koeficienty ireducibilného polynómu $p_1(x) \in F_1[x]$ na im zodpovedajúce koeficienty polynómu $p_2(x) \in F_2[x]$. Nech $F_1(u_1)$ a $F_2(u_2)$ sú jednoduché rozšírenia generované koreňmi tých polynómov. Potom φ možno rozšíriť na izomorfizmus $\psi : F_1(u_1) \to F_2(u_2)$, pričom $\psi(u_1) = u_2$.*

D ô k a z. ψ je dané predpisom

$$\psi(a_0 + a_1u_1 + \cdots + a_{n-1}u_1^{n-1}) = \varphi(a_0) + \varphi(a_1)u_2 + \cdots + \varphi(a_{n-1})u_2^{n-1},$$

kde n je stupeň polynómu p_1. Bijektívnosť ψ je zrejmá, zachovanie súčtu vyjde ľahko. Overíme zachovanie súčinu.

Pre každé $f = a_0 + a_1x + \cdots + a_kx^k \in F_1[x]$ položme

$$f_\varphi = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_k)x^k \in F_2[x].$$

Ľahko sa overí, že $(f + g)_\varphi = f_\varphi + g_\varphi$ a $(fg)_\varphi = f_\varphi g_\varphi$ pre každé $f, g \in F_1[x]$. Predpoklad našej vety hovorí, že $(p_1)\varphi = p_2$.

Nech teraz $f = a_0+a_1x+\cdots+a_{n-1}x^{n-1}$, $g = b_0+b_1x+\cdots+b_{n-1}x^{n-1}$, $a_i, b_i \in F_1$. Chceme dokázať, že $\psi(f(u_1)g(u_1)) = \psi(f(u_1))\psi(g(u_1))$.

Podľa Vety o delení so zvyškom existujú polynómy $q, z \in F_1[x]$ tak, že $fg = p_1 q + z$, kde $z(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ pre nejaké $c_0, \ldots, c_{n-1} \in F_1$. Pretože $p_1(u_1) = 0$, dostávame

$$\psi(f(u_1)g(u_1)) = \psi(p_1(u_1)q(u_1) + z(u_1)) = \psi(z(u_1)) = z_\varphi(u_2).$$

Na druhej strane,

$$\psi(f(u_1))\psi(g(u_1)) = f_\varphi(u_2)g_\varphi(u_2) =$$

$$= (fg)_\varphi(u_2) = (p_1 q + z)_\varphi(u_2) = p_2(u_2)q_\varphi(u_2) + z_\varphi(u_2) = z_\varphi(u_2).$$

(Využili sme, že $(p_1)_\varphi = p_2$ a $p_2(u_2) = 0$.) ∎

Lema 9.3. *Nech $\varphi : F_1 \to F_2$ je izomorfizmus polí. Predpokladajme, že φ zobrazuje koeficienty polynómu $f_1(x) \in F_1[x]$ na im zodpovedajúce koeficienty polynómu $f_2(x) \in F_2[x]$. Nech N_1 a N_2 sú rozkladové polia polynómu f_1 nad F_1 a f_2 nad F_2. Potom φ možno rozšíriť na izomorfizmus $\psi : N_1 \to N_2$, pričom ak f_1 je separabilný, tak to možno urobiť $[N_1 : F_1]$ spôsobmi.*

D ô k a z. Urobíme indukciu podľa $m = [N_1 : F_1]$. Ak $m = 1$, tak $N_1 = F_1$, potom f_1 má všetky korene vo F_1 a teda aj f_2 má všetky korene vo F_2, takže $N_2 = F_2$. Jediná možnosť pre ψ je $\psi = \varphi$.

Nech teraz $m > 1$ a predpokladajme, že tvrdenie platí pre rozkladové polia nižších stupňov. Polynóm f_1 má nad F_1 nejakého ireducibilného deliteľa p_1 stupňa $d > 1$. Izomorfizmus φ zobrazuje koeficienty p_1 na koeficienty ireducibilného polynómu $p_2 \in F_2[x]$. Nech $u_1 \in N_1$ je ľubovoľný koreň p_1. Pre každý koreň $u_2 \in N_2$ polyómu p_2 existuje podľa Lemy 9.2 izomorfizmus $\varphi_1 : F_1(u_1) \to F_2(u_2)$ ktorý predlžuje φ a zobrazuje u_1 do u_2. Naviac, keď f_1 je separabilný, tak aj f_2, p_1, p_2 sú separabilné, a preto p_2 má d rôznych koreňov a teda máme d možností pre φ_1.

Teraz, N_1 je rozkladové pole f_1 aj nad $F_1(u)$. A podobne, N_2 je rozkladové pole f_2 nad $F_2(u_2)$. Platí ale $[N_1 : F_1(u_1)] \cdot [F_1(u_1) : F_1] = [N_1 : F_1]$, preto $[N_1 : F_1(u_1)] = m/d < m$ a môžeme použiť indukčný predpoklad. Ten hovorí, že izomorfizmus φ_1 možno predĺžiť do izomorfizmu $\psi : N_1 \to N_2$ a to (v prípade separabilného f_1) m/d spôsobmi. Takže máme d možností ako rozšíriť φ na φ_1 a každá z nich nám dá m/d možností na rozšírenie do ψ. Dohromady je to m možnosti ako rozšíriť φ do ψ. ∎

Veta 9.4. *Rozkladové pole polynómu f nad F je určené jednoznačne až na izomorfizmus.*

D ô k a z. Stačí použiť Lemu 9.3 na prípad, že $\varphi : F \to F$ je identické zobrazenie. Potom $f_1 = f_2 = f$ a N_1 a N_2 sú rozkladové polia toho istého polynómu. ∎

10. Galoisove grupy

Pripomeňme si, že automorfizmus je izomorfizmus $F \to F$. Ľahko sa overí, že platí

Veta 10.1. (i) *Všetky automorfizmy poľa F tvoria grupu (vzhľadom na skladanie).*
(ii) *Všetky automorfizmy poľa F, ktoré zachovávajú množinu A tvoria grupu.*

Definícia 10.2. *Nech f je polynóm nad F. Galoisova grupa polynómu f nad F je grupa všetkých automorfizmov rozkladového poľa N, ktoré zachovávajú množinu F.*

Galoisovu grupu f nad F budeme označovat $\mathrm{Gal}(f, F)$. Všimnime si, že $\mathrm{Gal}(f, F)$ závisí nielen na f, ale aj na F. Galoisova grupa polynómu $x^2 + 1$ nad $\mathbb{C}$ je iná ako Galoisova grupa toho istého polynómu nad $\mathbb{R}$.

Ak $\varphi \in \mathrm{Gal}(f, F)$, tak podľa 3.1 φ zobražuje korene polynómu f do koreňov polynómu f. To znamená, že na množine všetkých koreňov f pôsobí φ ako permutácia. Naopak, φ je touto permutáciou jednoznačne určené. To je preto, lebo N je nad F generované množinou koreňov polynómu f. Dostávame tak nasledujúce tvrdenie.

Veta 10.3. *Grupa $\mathrm{Gal}(f, F)$ je izomorfná s nejakou grupou permutácií na množine koreňov polynómu f.*

Slovné spojenie "nejaká grupa permutácií" znamená, že môže ísť o grupu všetkých permutácií, ale aj nemusí. Vo všeobecnosti nie každú permutáciu koreňov vieme dostať z nejakého $\varphi \in \mathrm{Gal}(f, F)$.

Veta 10.4. *Rád Galoisovej grupy separabilného polynómu nad F sa rovná stupňu $[N : F]$ jeho rozkladového poľa.*

D ô k a z. Prvky Galoisovej grupy $\mathrm{Gal}(f, F)$ sú všetky automorfizmy N, ktoré zachovávajú F. Inými slovami, sú to všetky predĺženia identického automorfizmu $F \to F$. Keď použijeme Lemu 9.3, na prípad $N_1 = N_2$, dostávame, že existuje $[N : F]$ izomorfizmov $N \to N$, ktoré predlžujú identitu $F \to F$. ∎

Veta 10.5. *Nech N je rozkladové pole separabilného polynómu f nad F. Potom pre každé $x \in N \setminus F$ existuje $\varphi \in \mathrm{Gal}(f, F)$ také, že $\varphi(x) \neq x$.*

D ô k a z. Označme

$$P = \{x \in N \mid \varphi(x) = x \text{ pre každé } \varphi \in \mathrm{Gal}(f, F)\}.$$

Ľahko sa overí, že P je pole (porovnajte s Vetou 11.1) a $F \subseteq P \subseteq N$. Potom $[N : F] = [N : P] \cdot [P : F]$. Ale N je rozkladové pole pre f aj nad P a $\mathrm{Gal}(f, F) = \mathrm{Gal}(f, P)$, takže podľa Vety 10.4 platí $[N : F] = [N : P]$. Potom $[P : F] = 1$, teda $P = F$. ∎

Úloha popísať Galoisovu grupu polynómu f nad F môže byť výpočtovo veľmi náročná, a nebudeme sa ňou vo všeobecnosti zaoberať. V konkrétnych príkladoch (pri $F \subseteq \mathbb{C}$) nám výdatne pomôže znalosť komplexných koreňov polynómu f.

Popíšeme teraz Galoisovu grupu polynómu $f(x) = x^4 - 2$ nad $\mathbb{Q}$. Tento polynóm má korene $x_1 = \sqrt[4]{2}$, $x_2 = i\sqrt[4]{2}$, $x_3 = -\sqrt[4]{2}$ a $x_4 = -i\sqrt[4]{2}$. Rozkladové pole je $N = \mathbb{Q}(\sqrt[4]{2}, i)$. (Namiesto $\sqrt[4]{2}$ tam môže vystupovať aj hociktoré iné x_k.) Každý automorfizmus $\varphi \in \mathrm{Gal}(f, \mathbb{Q})$ je určený tým, kam sa zobrazia $\sqrt[4]{2}$ a i. Podľa 3.1 musí platiť $\varphi(x_1) \in \{x_1, x_2, x_3, x_4\}$ a, keďže i je koreňom $x^2 + 1$, $\varphi(i) \in \{i, -i\}$. To nám dáva 8 možných kombinácií. To, že každá z nich sa naozaj realizuje nejakým $\varphi \in \mathrm{Gal}(f, \mathbb{Q})$ nie je triviálne, ale vyplýva z vety, že rád (počet prvkov) grupy $\mathrm{Gal}(f, \mathbb{Q})$ sa rovná stupňu rozšírenia $[N : F]$, a ten je 8. (Polynóm $x^4 - 2$ je nad $\mathbb{Q}$ ireducibilný, takže adjungovaním $\sqrt[4]{2}$ urobíme rozšírenie stupňa 4, adjungovaním i ďalšie rozšírenie stupňa 2.) Všetkých 8 automorfizmov je popísaných v nasledujúcej tabuľke. Každý riadok zodpovedá jednému automorfizmu. V stĺpcoch pod i a x_1 sú zvolené hodnoty $\varphi(i)$ a $\varphi(x_1)$, ostatné hodnoty sú dopočítané zo vzťahov $\varphi(x_2) = \varphi(i)\varphi(x_1)$, $\varphi(x_3) = -\varphi(x_1)$, $\varphi(x_4) = -\varphi(i)\varphi(x_1)$.

	i	x_1	x_2	x_3	x_4
e	i	x_1	x_2	x_3	x_4
r_1	i	x_2	x_3	x_4	x_1
r_2	i	x_3	x_4	x_1	x_2
r_3	i	x_4	x_1	x_2	x_3
s_1	$-i$	x_1	x_4	x_3	x_2
s_2	$-i$	x_2	x_1	x_4	x_3
s_3	$-i$	x_3	x_2	x_1	x_4
s_4	$-i$	x_4	x_3	x_2	x_1

Vidíme, že permutácie na množine $\{x_1, x_2, x_3, x_4\}$ presne zodpovedajú symetriám štvorca s vrcholmi x_1, x_2, x_3, x_4, v ktorom vrchol x_1 je oproti vrcholu x_3. Teda $\mathrm{Gal}(f, \mathbb{Q})$ je izomorfná s D_4.

Všimnime si ešte, že na množine $\{x_1, x_2, x_3, x_4\}$ existuje 24 permutácií. Z nich však iba našich 8 určuje automorfizmus poľa N. Zvyšných 16 sa realizovať nedá, napr. pre žiaden automorfizmus nemôže platiť $\varphi(x_1) = x_1$, $\varphi(x_3) = x_2$, keďže $x_3 = -x_1$.

Cvičenie. Popíšte Galoisovu grupu polynómu $x^4 - 2$ nad poľom $\mathbb{Q}(i)$.

11. Hlavná veta Galoisovej teórie

Hlavná veta Galoisovej teórie je nasledujúce tvrdenie.

Veta 11.1. *Nech N je rozkladové pole polynómu f nad F. Potom platí:*

(i) *Pre každé pole K medzi F a N (t.j. $F \subseteq K \subseteq N$) je $G(K) = \{\varphi \in \mathrm{Gal}(f, F) \mid \varphi$ zachováva $K\}$ je podgrupa grupy $\mathrm{Gal}(f, F)$.*

(ii) *Pre každú podgrupu H grupy $\mathrm{Gal}(f, F)$ je $P(H) = \{x \in N \mid \varphi(x) = x$ pre každé$\varphi \in H\}$ pole medzi F a N.*

(iii) *Priradenia P a G sú navzájom inverzné, t.j. $P(G(K)) = K$ a $G(P(H)) = H$ pre každé H a K.*

D ô k a z. (i) Podľa Vety 10.1 je $G(K)$ podgrupa $\mathrm{Gal}(f, F)$ dokonca aj pre každú množinu K, nielen pre polia.

(ii) Treba overiť, že pre každé $x, y \in P(H)$ platí $x + y \in P(H)$, $xy \in P(H)$, $-x \in P(H)$ a (ak $x \neq 0$) $x^{-1} \in P(H)$. Všetko toto je ľahké.

(iii) Ak $x \in K$, tak podľa definície $G(K)$ platí, že $g(x) = x$ pre každé $g \in \mathrm{Gal}(f, F)$, a to znamená, že $x \in P(G(K))$. Tým sme dokázali, že $K \subseteq P(G(K))$. Podobne sa ukáže inklúzia $H \subseteq G(P(H))$. Inklúzia $P(G(K)) \subseteq K$ vyplýva z Vety 10.5, keď si uvedomíme, že N je rozkladovým poľom polynómu f aj nad K. Dôkaz inklúzie $G(P(H)) \subseteq H$ sme vynechali. ∎

Takže existuje bijekcia medzi podgrupami Galoisovej grupy $\mathrm{Gal}(f, F)$ a poľami K medzi F a N. Preskúmame podrobne túto bijekciu na príklade polynómu $f(x) = x^4 - 2$ nad $\mathbb{Q}$.

Už vieme, že $\mathrm{Gal}(f, \mathbb{Q})$ je izomorfná s D_4.Jej podgrupy sú nasledovné.

(1) $G_0 = \{e\}$. Identita zachováva všetky prvky $N = \mathbb{Q}(\sqrt[4]{2}, i)$, takže $P(G_0) = N$.

(2) $G_1 = \{e, s_1\}$. Automorfizmus s_1 posiela i do $-i$ a $u = \sqrt[4]{2}$ necháva na mieste. Prvky N sa dajú vyjadriť v tvare

$$x = a_0 + a_1 u + a_2 u^2 + a_3 u^3 + a_4 i + a_5 iu + a_6 iu^2 + a_7 iu^3,$$

a potom

$$s_1(x) = a_0 + a_1 u + a_2 u^2 + a_3 u^3 - a_4 i - a_5 iu - a_6 iu^2 - a_7 iu^3.$$

Preto $s_1(x) = x$ práve vtedy, keď $a_4 = a_5 = a_6 = a_7 = 0$. Dostávame

$$P(G_1) = \{a_0 + a_1u + a_2u^2 + a_3u^3 \mid a_0, \ldots, a_3 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt[4]{2}).$$

(3) $G_2 = \{e, s_2\}$. Teraz $s_2(i) = -i$, $s_2(u) = iu$, preto

$$s_2(x) = a_0 + a_1iu - a_2u^2 - a_3iu^3 - a_4i + a_5u + a_6iu^2 + a_7u^3.$$

Rovnosť $s_2(x) = x$ platí práve vtedy, keď $a_1 = a_5$, $a_2 = -a_2$, $a_3 = -a_7$, $a_4 = -a_4$. Takže $P(G_2)$ pozostáva zo všetkých prvkov tvaru $a_0+a_1(u+iu)+a_3(u^3-iu^3)+a_6iu^2$. Toto sa dá ešte zjednodušiť. Keď označíme $w = u + iu$, tak potom $w^2 = 2iu^2$, $w^3 = -2(u^3 - iu^3)$, preto

$$P(G_2) = \{a_0 + a_1w + \frac{1}{2}a_6w^2 - \frac{1}{2}a_3w^3 \mid a_0, a_1, a_3, a_6 \in \mathbb{Q}\} = \mathbb{Q}(w).$$

Na toto sa dalo prísť aj geometricky: s_2 mení x_1 a x_2, preto s_2 zachováva $w = x_1 + x_2$, takže $\mathbb{Q}(w) \subseteq P(G_2)$, ale medzi $\mathbb{Q}(w)$ a N žiadne pole nie je (dimenzie!), musí platiť rovnosť.

(4) $G_3 = \{e, s_3\}$. Podobne ako v prípade (1) dostávame $P(G_3) = \mathbb{Q}(i\sqrt[4]{2})$.

(5) $G_4 = \{e, s_4\}$. Podobne ako v (2) dostaneme $P(G_4) = \mathbb{Q}(t)$, kde $t = x_1 + x_4 = u - iu$.

(6) $G_5 = \{e, r_2\}$. Do $P(G_5)$ budú patriť tie $x \in N$, pre ktoré $a_1 = a_3 = a_5 = a_7 = 0$. Preto

$$P(G_5) = \{a_0+a_2u^2+a_4i+a_6iu^2 \mid a_0, a_2, a_4, a_6 \in \mathbb{Q}\} = \mathbb{Q}(u^2, i) = \mathbb{Q}(\sqrt{2}, i).$$

Samozrejme, pole $\mathbb{Q}(\sqrt{2}, i)$ sa dá nad $\mathbb{Q}$ generovať aj jedným prvkom, napríklad $\sqrt{2} + i$.

(7) $G_6 = \{e, r_1, r_2, r_3\}$. Už vieme, že r_2 zachováva prvky tvaru

$$y = a_0 + a_2u^2 + a_4i + a_6iu^2.$$

Automorfizmus r_1 (podobne r_3) takýto prvok zobrazuje na

$$r_1(y) = a_0 - a_2u^2 + a_4i - a_6iu^2.$$

Rovnosť $r_1(y) = y$ nastane práve vtedy, keď $a_2 = a_6 = 0$, takže

$$P(G_6) = \{a_0 + a_4i \mid a_0, a_4 \in \mathbb{Q}\} = \mathbb{Q}(i).$$

(8) $G_7 = \{e, r_2, s_1, s_3\}$. Pre y ako v (7) dostávame

$$s_1(y) = s_3(y) = a_0 + a_2u^2 - a_4i - a_6iu^2,$$

odkiaľ

$$P(G_7) = \{a_0 + a_2u^2 \mid a_0, a_2 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}).$$

(9) $G_8 = \{e, r_2, s_2, s_4\}$. Pre y ako v (7) dostávame

$$s_2(y) = s_4(y) = a_0 - a_2u^2 - a_4i + a_6iu^2,$$

odkiaľ

$$P(G_8) = \{a_0 + a_6 i u^2 \mid a_0, a_6 \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{2}).$$

(10) $G_{10} = \mathrm{Gal}(f, \mathbb{Q})$. Podľa Vety 10.5, $P(G_{10}) = \mathbb{Q}$.

12. Neriešiteľnosť rovníc 5. stupňa

Pod riešením polynomickej rovnice v radikáloch myslíme nájdenie vzorca, ktorý vyjadruje korene polynómu pomocou jeho koeficientov použitím operácií $+, \cdot, -, :$ a $\sqrt[n]{}$. Také riešenie bolo od antických čias známe pre polynómy 2. stupňa, a od 16. storočia pre polynómy 3. a 4. stupňa. Pre polynómy vyšších stupňov sa také riešenie nenašlo, a v 19. storočí dokázal E. Galois, že ani neexistuje. Jeho práca sa stala základom teórie grúp.

V nasledujúcom tvrdení sa zaoberáme rozkladovým poľom binomického polynómu $x^n - a$ nad $F \subseteq \mathbb{C}$. Označme

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

(primitívna n-tá odmocnina z jednotky). Ak $a = 1$, tak korene polynómu sú j, j^2,..., j^n. Ak $a \neq 1$, tak zvolíme ľubovoľný koreň u a potom ostatné korene sú uj, uj^2,..., uj^{n-1}.

Lema 12.1. *Nech u je koreň polynómu $f(x) = x^n - a$ nad $F \subseteq \mathbb{C}$. Predpokladajme, že $j \in F$ alebo $u = j$. Nech $N \supseteq F(u)$ je ľubovoľné pole. Označme G grupu všetkých automorfizmov poľa N ktoré zachovávajú F a H grupu všetkých automorfizmov N, ktoré zachovávajú $F(u)$. Potom*

(i) *H je normálna podgrupa grupy G;*
(ii) *faktorová grupa G/H je komutatívna.*

D ô k a z. Z našich predpokladov vyplýva, že $F(u)$ obsahuje všetky korene polynómu f.

Je jasné, že G a H sú grupy a $H \subseteq G$. Overíme teraz normálnosť. Nech $\alpha \in G$, $\varphi \in H$. Chceme dokázať, že $\alpha^{-1}\varphi\alpha$ patrí do H, teda že zachováva všetky prvky $F(u)$. Každý prvok $F(u)$ sa dá vyjadriť v tvare

$$x = a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$$

pre nejaké $n \in \mathbb{N}$, $a_0, \ldots, a_n \in F$. Pretože α zachováva F, dostávame

$$\alpha(x) = a_0 + a_1\alpha(u) + a_2\alpha(u)^2 + \cdots + a_{n-1}\alpha(u)^{n-1}.$$

Podľa 3.1 je $\alpha(u)$ koreňom f, takže podľa predpokladu našej lemy $\alpha(u) \in F(u)$. Potom ale $\alpha(x) \in F(u)$. Pretože φ zachováva $F(u)$, dostávame $\varphi(\alpha(x)) = \alpha(x)$, a teda

$$\alpha^{-1}(\varphi(\alpha(x))) = \alpha^{-1}(\alpha(x)) = x.$$

Tým je ukončený dôkaz (i).

Prvky grupy G/H sú triedy rozkladu φH, $\varphi \in G$. Máme teda dokázať, že pre všetky $\varphi, \psi \in G$ platí

$$\varphi H \cdot \psi H = \psi H \cdot \varphi H.$$

To nastane práve vtedy, keď $\varphi\psi H = \psi\varphi H$, teda keď automorfizmy $\varphi\psi$ a $\psi\varphi$ patria do tej istej triedy rozkladu podľa H. Ekvivalentne, máme overiť, že automorfizmus $\alpha = \varphi^{-1}\psi^{-1}\varphi\psi$ patri do H.

Najprv overíme, že $\varphi\psi(u) = \psi\varphi(u)$. Automorfizmy φ a ψ zobrazujú u do koreňov polynómu f. V prípade $u = j$ to znamená, že $\varphi(u) = j^k$, $\psi(u) = j^l$ pre nejaké prirodzené k, l, a teda

$$\varphi(\psi(u)) = \varphi(j^l) = \varphi(j)^l = (j^k)^l = j^{kl} = \psi(\varphi(u)).$$

V prípade $j \in F$ máme $\varphi(u) = uj^k$, $\psi(u) = uj^l$ pre nejaké $k, l \in \mathbb{N}$, takže

$$\varphi(\psi(u)) = \varphi(uj^l) = \varphi(u) \cdot j^l = uj^k j^l = uj^{k+l} = \psi(\varphi(u)).$$

V oboch prípadoch teda $\varphi\psi(u) = \psi\varphi(u)$, a potom aj

$$\alpha(u) = \varphi^{-1}\psi^{-1}\varphi\psi(u) = \varphi^{-1}\psi^{-1}\psi\varphi(u) = u.$$

Pre každé $x = a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1} \in F(u)$ potom

$$\alpha(x) = a_0 + a_1\alpha(u) + a_2\alpha(u)^2 + \cdots + a_{n-1}\alpha(u)^{n-1} = x.$$

Takže α zachováva $F(u)$, teda patrí do H, čo sme chceli dokázať. ∎

Veta 12.2. *Nech f je polynóm nad $F \subseteq \mathbb{C}$, ktorý je riešiteľný v radikáloch. Potom jeho Galoisova grupa je riešiteľná.*

D ô k a z. Riešiteľnost v radikáloch znamená, že existuje postupnosť polí

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n,$$

tak, že $K_{i+1} = K_i(u_i)$, kde u_i je koreň nejakého binomického polynómu nad K_i, a že K_n obsahuje všetky korene polynómu f. Môžeme naviac predpokladať, že všetky u_i spĺňajú podmienku z predošlej lemy, teda že $u_i = j$ je primitívna n-tá odmocnina z jednotky, alebo $j \in K_i$. Definujme G_i ako grupu všetkých automorfizmov poľa K_n, ktoré zachovávajú K_i. Dostávame reťazec grúp

$$G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n.$$

Podľa predchádzajúcej lemy je G_{i+1} normálna podgrupa G_i a G_i/G_{i+1} je komutatívna. Grupa G_n pozostáva z jediného prvku (identita), podľa definície je teda G_0 riešiteľná grupa.

Grupa G_0 ale nemusí byť Galoisovou grupou polynómu f. To je preto, lebo K_n nemusí byť rozkladovým poľom polynómu f. Vo všeobecnosti je len $N \subseteq K_n$. (Rozkladové pole sme označili N.) Dôležité je, že každý automorfizmus $\varphi \in G_0$ možno zúžiť na N. Také φ totiž zachováva F a korene f zobrazuje do koreňov f. Takže $\varphi(x) \in N$ pre každé $x \in N$ a teda môžeme definovať automorfizmus

$$\varphi^* : \ N \to N$$

predpisom $\varphi^*(x) = \varphi(x)$. Naopak, každý automorfizmus z Galoisovej grupy je tvaru φ^* pre nejaké $\varphi \in G_0$. (To vyplýva z tvrdení o predlžovaní.) Teda Galoisova grupa polynómu f je

$$H_0 = \{\varphi^* \mid \varphi \in G_0\}.$$

Podobne, pre každé i nech $H_i = \{\varphi^* \mid \varphi \in G_i\}$. Reťazec

$$H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n$$

dokazuje, že grupa H_0 je riešiteľná. ∎

Veta 12.3. *Existuje polynóm 5. stupňa, ktorého Galoisova grupa nie je riešiteľná.*