RNDr. Libor Polák.

Algebra I

Zápisky z přednášky zpracoval:
Jiří Dobeš

20. dubna 1995

Obsah

1 Grupy

Nejdříve uvedeme některé základní pojmy:

Binární operace na množině A je zobrazení $\cdot : A \times A \to A$. Místo $\cdot(a, b)$ píšeme $a \cdot b$.

$(A, \cdot)$ Množina A s operací $\cdot$ se nazývá **grupoid**.

- Operace $\cdot$ je **komutativní**, platí-li $\forall a, b \in A : a \cdot b = b \cdot a$.
- Operace $\cdot$ je **asociativní**, platí-li $\forall a, b, c \in A : (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Pologrupa je grupoid s asociativní operací.

Levý neutrální prvek $e \in A$ splňuje $\forall a \in A : e \cdot a = a$.

Pravý neutrální prvek $e \in A$ splňuje $\forall a \in A : a \cdot e = a$.

Neutrální prvek je levý neutrální a pravý neutrální.

Monoid je pologrupa s neutrálním prvkem.

Věta 1.1
Nechť e je levý neutrální prvek a f pravý neutrální prvek grupoidu $(A, \cdot)$. Pak $e = f$.

Důkaz:

$$e = \underline{e \cdot f} = f$$

grupoid může mít více např. levých neutrálních prvků, má-li i nějaký pravý neutrální prvek, pak má jediný neutrální prvek, tedy i jediný levý neutrální prvek. □

Definice 1.2
Nechť $(A, \cdot)$ je grupoid s neutrálním prvkem e, $a \in A$. $b \in A$ se nazývá levý (resp. pravý) inverzní prvek k a, platí-li $b \cdot a = e$ $(a \cdot b = e)$. Prvek b se nazývá inverzní, splňuje-li $a \cdot b = b \cdot a = e$.

Věta 1.3
Nechť $(A, \cdot, e)$ je monoid, $a \in A$, nechť b je levý inverzní k a, c je pravý inverzní k a. Pak $b = c$.

Důkaz:

$$c = e \cdot c = \underline{(b \cdot a) \cdot c} = b \cdot (a \cdot c) = b \cdot e = b$$

□

Definice 1.4
Permutace na množině X je bijekce $f : X \to X$. $S(X)$ označme jako množinu všech permutací na množině X.

Zřejmě platí $f, g \in S(X)$, pak $g \circ f \in S(X)$.

Definice 1.5
Grupa je pologrupa s neutrálním prvkem taková, že ke každému prvku existuje prvek inverzní.

Poznámka 1.6
Grupa $(S(X), \circ)$ se nazývá symetrická grupa na množině X. Jde o grupu všech permutací na množině X. Je komutativní právě, když $|X| \leq 2$. Pro X konečnou lze předpokládat, že $X = \{1, 2, \ldots, n\}$, píšeme S_n. $|S_n| = n!$

Definice 1.7
Nechť $(i_1, i_2, \ldots, i_k)$, $k \geq 2$ jsou po dvou různé prvky z $\{1, \ldots, n\}$. Permutaci danou předpisem:

$$\begin{aligned} f(i_j) &= i_{j+1}, \text{pro} \qquad j = 1, \ldots, k-1, \\ f(i_k) &= i_1, \\ f(i) &= i, \text{pro} \qquad i \in \{1, 2, \ldots, n\} - \{i_1, i_2, \ldots, i_k\} \end{aligned}$$

nazýváme cyklem. Cyklus délky 2 nazýváme transpozicí. Cykly $(i_1, \ldots, i_k)$ a $(j_1, \ldots, j_l)$ nazýváme nezávislé, platí-li $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \phi$

Věta 1.8
Libovolnou neidentickou permutaci f množiny $X = \{1, 2, \ldots, n\}$ lze psát jako součin po 2 nezávislých cyklů. Tento rozklad je jednoznačný až na pořadí činitelů.

Věta 1.9
Každá $f \in S_n$ je součinem transpozic.

Definice 1.10
Nechť $f \in S_n$, $1 \leq i < j \leq n$. Dvojice (i, j) je inverzí v f, platí-li $f(i) > f(j)$. Permutace se sudým (lichým) počtem inverzí se nazývá sudá (lichá).

Věta 1.11
Permutace je sudá právě, když je součinem sudého počtu transpozic.

Důkaz: Identická permutace je sudá a je součinem nula transpozic. Stačí ukázat, že násobení transpozicí mění paritu. □

1.1 Grupy zbytkových tříd

Definice 1.12
Nechť $a, b \in \mathbf{Z}$, $a|b$ (a dělí b) právě,když $\exists c \in \mathbf{Z} : c \cdot a = b$.

Poznámka 1.13
Jen na okraj:
$a|0$ pro $\forall a \in \mathbf{Z}$
$0|a$ právě pro $a = 0$.

Věta 1.14
Nechť $a \in \mathbf{N}, b \in \mathbf{Z}$. Pak existuje $q \in \mathbf{Z}$, $r \in \{0, 1, \ldots, a-1\}$ tak,že $b = q \cdot a + r$. Přitom q i r jsou určeny jednoznačně.

Důkaz:

1. $b \geq 0$ indukcí vzhledem k b
   (a) $b < a$ stačí psát $b = 0 \cdot a + b$, kde $q = 0, r = b$.
   (b) $b \geq a$ podle indukčního předpokladu

$$b - a = q \cdot a + r, \qquad q \in \mathbf{Z}, r \in \{0, \ldots, a-1\}$$

$$b = (q+1) \cdot a + r$$

2. $b < 0$ podle prvního bodu $-b = q \cdot a + r$

$$\begin{aligned} b &= (-q) \cdot a - r, \qquad pro \quad r = 0 \\ b &= (-q-1) \cdot a + (a - r), \qquad pro \quad r > 0 \end{aligned}$$

Jednoznačnost:

$$b = q \cdot a + r = q' \cdot a + r', \qquad q, q' \in \mathbf{Z}, r, r' \in \{0, \ldots, a-1\}$$

Lze předpokládat, že $r \geq r'$.

$$r - r' = (q' - q) \cdot a, \qquad r - r' \in \{0, 1, \ldots, a-1\}$$

jediný celý násobek a v množině na předcházejícím řádku je 0, tedy $r = r', q = q'$
□

Definice 1.15

Nechť $a, b \in \mathbf{Z}$. d nazveme společným dělitelem čísel a,b, platí-li $d|a \wedge d|b$. d nazveme největším společným dělitelem čísel a,b, je-li mezi společnými děliteli největší. Označujeme (a, b).

Věta 1.16 EUKLIDŮV ALGORITMUS

Nechť $a, b \in \mathbf{N}$.

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\dots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} \cdot r_n \end{aligned}$$

Platí $r_1 \in \langle 0, b)$,$r_2 \in \langle 0, r_1)$,$r_3 \in \langle 0, r_2)$, atd. Pak $r_n = (a, b)$.

Důkaz:

1. dokážeme, že r_n je společný dělitel a,b

   z poslední rovnosti $r_n|r_{n-1}$
   z předposlední $r_n|r_{n-2}$
   $\vdots$ $\vdots$
   3. $r_n|r_1$
   2. $r_n|b$
   1. $r_n|a$

2. a že r_n je největším společným dělitelem:
   Nechť $d|a$ a zároveň $d|b$,

   z 1.rovnosti $d|r_1$ $\quad r_n \in \mathbf{N} \Leftrightarrow d \leq r_n$
   z 2. $d|r_2$
   $\vdots$ $\vdots$
   z předp. $d|r_n$

□

Věta 1.17

Bezoutova rovnost Nechť $a, b \in \mathbf{N}$. Pak existuje $u, v \in \mathbf{Z}$ tak,že $u \cdot a + v \cdot b = (a, b)$.

Důkaz: Vyplývá z Euklidova algoritmu. □

Definice 1.18

Čísla $a, b \in \mathbf{Z}$ nazýváme nesoudělná, platí-li, že $(a, b) = 1$

Důsledek 1.19

Čísla $a, b \in \mathbf{Z}$ jsou nesoudělná právě, když $\exists u, v \in \mathbf{Z}$ taková, že $u \cdot a + b \cdot v = 1$.

Důsledek 1.20

Nechť $a, b, c \in \mathbf{N}$, $a|b \cdot c$, $(a, b) = 1$. Pak $a|c$.

Definice 1.21
$a \geq 2, a \in \mathbf{N}$ se nazývá prvočíslo, platí-li: $a = b \cdot c$, $b, c \in \mathbf{N} \Rightarrow b = 1$ nebo $c = 1$.

Lemma 1.22
Nechť $a \in \mathbf{N}, a \geq 2$. Pak lze vyjádřit a jako součin prvočísel. Tento rozklad je jednoznačný až na pořadí činitelů.

Důkaz: existence indukcí vzhledem k a, jednoznačnost indukcí □

Definice 1.23
Nechť $a, b \in \mathbf{Z}, n \in \mathbf{N}$. $a \equiv b \pmod{n} \Leftrightarrow n|(a-b)$ je kongruentní modulo ("a je kongruentní s b modulo n"). Označíme $[a]_n := \{k \cdot n + a | k \in \mathbf{Z}\}$.

Lemma 1.24
Je ekvivalentní :

1. $a \equiv b \pmod{n}$
2. a,b dávají při dělení n stejný zbytek.
3. $[a]_n = [b]_n$

Definice 1.25
Definujeme následující množinu:
$\mathbf{Z_n} := \{[a]_n | a \in \mathbf{Z}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$; v první množině vypočítáváme i prvky, které jsou shodné, zato druhá už je přesným výčtem (vzájemně různé třídy tvořící rozklad $\mathbf{Z_n}$), obsahuje jen zbytky po dělení.
Na $\mathbf{Z_n}$ definujeme operaci + předpisem: $[a]_n + [b]_n := [a+b]_n$, a dále operaci $\cdot$ takto: $[a]_n \cdot [b]_n := [a \cdot b]_n$.

Věta 1.26
Pro libovolné $n \in \mathbf{N}$ je $(\mathbf{Z_n}, +)$ komutativní grupa.

Věta 1.27
Pro libovolné $n \in \mathbf{N}$ je $(\mathbf{Z_n}, \cdot)$ komutativní monoid. $[a]_n$ má inverzi $\Leftrightarrow (a, n) = 1$.

Důsledek 1.28
$(\mathbf{Z_n^*} = \{[1]_n, [2]_n, \ldots, [n-1]_n\}, \cdot)$ je pro prvočíselné n grupou.

Poznámka 1.29
$*$ znamená, že jde o množinu bez nulové třídy. Pouze je-li n prvočíslo, je příslušná $\mathbf{Z_n^*}$ uzavřená na operaci $\cdot$ a je tedy grupou.

Definice 1.30
Pro $n \in \mathbf{N}$ definujeme tzv. Eulerovu funkci $\varphi(n)$ jako počet čísel z množiny $\{1, 2, \ldots, n-1\}$, která jsou nesoudělná s n.

Věta 1.31
Pro prvočíselná p platí $\varphi(p^n) = p^{n-1}.(p-1)$. Pro a,b nesoudělná platí $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Příklad 1.1
$\varphi(1000) = \varphi(2^3.5^3) = 2^2.1.5^2.4$

1.2 Základní vlastnosti grup

Věta 1.32
Nechť $(s,\cdot)$ je pologrupa, $n \in \mathbf{N}$, $a_1, a_2, \ldots, a_n \in S$. Pak součin prvků $a_1, a_2, \ldots, a_n$ v daném pořadí nezávisí na uzávorkování.

Důkaz: indukcí vzhledem k n

1. pro $n = 1, 2$ není co dokazovat
2. pro $n \geq 3$ a tvrzení platí pro menší n:
   nechť $a_1, a_2, \ldots, a_n \in S$, uvažujme součin

   $$(a_1 \ldots a_k) \cdot (a_{k+1} \cdot a_n) =$$

   podle indukčního předpokladu nezávisí obsah 1. závorky na uzávorkování (ani 2. závorky),

   $$= (a_1 \cdot (a_2 \ldots a_k)) \cdot (a_{k+1} \ldots a_n) = a_1 \cdot (a_2 \ldots a_k) \cdot (a_{k+1} \ldots a_n)$$

   pro $k \geq 2$ nemusíme používat závorek a pro $k = 1$ už máme požadovaný tvar.

□

Věta 1.33
Je-li $(S,\cdot)$ komutativní pologrupa, $n \in \mathbf{N}$ $a_1, a_2, \ldots, a_n \in S$. Pak výsledek součinu prvků $a_1, a_2, \ldots, a_n$ nezávisí na jejich pořadí.

Definice 1.34
Buď $(s,\cdot)$ pologrupa $a \in S$, $n \in \mathbf{N}$. Definujeme $a^n := \underbrace{a \cdot a \cdot \cdots a}_{n\ initel}$. Pokud má pologrupa neutrální prvek 1, klademe též $a^0 := 1$.

Lemma 1.35
Zřejmě $\forall n, m \in \mathbf{N_0}$ platí

$$a^m \cdot a^n = a^{m+n}$$
$$(a^m)^n = a^{m \cdot n}$$

Lemma 1.36
Mají-li a,b inverzi, řekněme a^{-1}, b^{-1}, platí, že $b^{-1} \cdot a^{-1}$ je inverze $a \cdot b$.

Definice 1.37
Pro $n \in \mathbf{N}$ klademe $a^{-n} := (a^-1)^n$. Což je samozřejmě rovno $(a^n)^{-1}$.

Lemma 1.38
Opět se snadno vidí, že $\forall m, n \in \mathbf{Z}$

$$a^m \cdot a^n = a^{m+n}$$

$$(a^m)^n = a^{m \cdot n}$$

Definice 1.39
Řád prvku a grupy $(G,\cdot)$ je nejmenší přirozené číslo n takové, že $a^n = 1$. Pokud takové n neexistuje, pravíme, že a má řád 0.

Příklad 1.2
V $(\mathbf{Z}, +)$ má $a = 2$ řád 0.
V $(\mathbf{Z}_6, +)$ je to takto:

$[0]_6$ má řád 1.
$[1]_6$ má řád 6.
$[2]_6$ má řád 3.
$[3]_6$ má řád 2.
$[4]_6$ má řád 1.
$[5]_6$ má řád 6.

Lemma 1.40
Nechť $(G,\cdot)$ je grupa, $a \in G$.

1. Nechť a je řádu n, $k \in \mathbf{Z}$, $k = qn + r, q \in \mathbf{Z}, 0 \leq r < n$, pak

$$a^k = a^r$$

   $1, a, a^2, \ldots, a^{n-1}$ jsou po 2 různé.

2. Nechť a je řádu 0, pak pro libovolné $k, l \in \mathbf{Z}, k \neq l$ je $a^k \neq a^l$

1.3 Podgrupy

Definice 1.41
Nechť $(G,\cdot)$ je grupa a $H \subseteq G$. H nazýváme nosičem podgrupy grupy $(G,\cdot)$, je-li

- $1 \in H$
- $a \in H \Rightarrow a^{-1} \in H$
- $a, b \in H \Rightarrow a \cdot b \in H$

Definice 1.42
Grupu $(H,\circ)$ nazveme podgrupou grupy $(G,\cdot)$ platí-li: $H \subseteq G, a, b \in H \Rightarrow a \circ b = a \cdot b$.

Pak $1_G = 1_H : 1_H \cdot 1_G = 1_H = 1_H \circ 1_H = 1_H \cdot 1_H$. Pro libovolné $a \in H$ je inverze a^{-1} v $(H,\circ)$ rovna inverzi a^{-1} v $(G,\cdot)$. Odvození je analogické.

Věta 1.43
V dalším nebudeme mezi těmito pojmy rozlišovat.

Lemma 1.44
Nechť $(G,\cdot)$ je grupa. $(H_i)_{i\in I}$ je systém podgrup, $I \neq \phi$. Pak $H = \bigcap_{i\in I} H_i$ je opět podgrupa.

Věta 1.45
Nechť $(G,\cdot)$ je grupa, $M \subseteq G$. Pak existuje (vzhledem k inkluzi) nejmenší podgrupa grupy obsahující množinu M. Je rovna $\bigcap_{i\in I} H_i$, kde $(H_i)_{i\in I}$ je systém všech podgrup, které obsahují množinu M.

Důkaz: $I \neq \phi$, neboť samo G je takovou podgrupou.
$H = \bigcap_{i\in I} H_i$ je podgrupa podle předchozího lemmatu. Zřejmě $M \subseteq H$. Chci dokázat, že H je nejmenší taková. Nechť H' je podgrupa obsahující M. A zřejmě $\exists i_0 \in I : H' = H_{i_0}$, ale platí, že $\bigcap_{i\in I} H_i \subseteq H_{i_0}$. □

Definice 1.46
Podgrupu z předcházející věty nazýváme podgrupou generovanou množinou M, označujeme $\langle M \rangle$.

Příklad 1.3

$(\mathbf{Z}, +)$ je generována například množinou $\{-1\}$ nebo $\{2, 3\}$. Nestačí množina $\{2\}$. Ta generuje jen podgrupu sudých čísel.

Definice 1.47
Grupa generovaná jednoprvkovou množinou se nazývá cyklická.

Věta 1.48
Nechť $(G, \cdot)$ je grupa, $M \subseteq G$. Pak

$$\langle M \rangle = \{a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots a_n^{\varepsilon_n} | n \in \mathbf{N_0},\ a_1, \ldots a_n \in M,\ \varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}\}$$

Součin délky 0 interpretujeme jako jedničku 1.

Důsledek 1.49
$\langle a \rangle = \{a^k | k \in \mathbf{Z}\}$. Místo $\langle \{a\} \rangle$ píšeme $\langle a \rangle$.

1.4 Morfismy

Definice 1.50
Nechť $(G, \cdot)$, $(H, \circ)$ jsou grupy. Zobrazení $\alpha : G \to H$ se nazývá homomorfismem grupy $(G, \cdot)$ do grupy $(H, \circ)$, platí-li $\forall a, b \in G : \alpha(a \cdot b) = \alpha(a) \circ \alpha(b)$. Píšeme $\alpha : (G, \cdot) \to (H, \circ)$
Dále označujeme vnoření jako prostý homomorfismus, izomorfismus jako bijektivní homomorfismus.
Říkáme, že $(G, \cdot)$ je izomorfní s $(H, \circ)$, existuje-li izomorfismus $(G, \cdot)$ na $(H, \circ)$, píšeme $(G, \cdot) \cong (H, \circ)$.

Lemma 1.51
Přirozený logaritmus $\ln : (\mathbf{R}^+, \cdot) \to (\mathbf{R}, +)$ je izomorfismus. Platí také $(\mathbf{Z_6}, \cdot) \cong (\mathbf{Z_7^*}, \cdot)$

Věta 1.52
Nechť $\alpha : (G, \cdot) \to (H, \circ)$ je homomorfismem grup. Pak $\alpha(1_G) = 1_H$, pro lib. $a \in G\ \alpha(a^{-1}) = (\alpha(a))^{-1}$

Poznámka 1.53

Složení homomorfismů je opět homomorfismus. Zobrazení inverzní k izomorfismu je izomorfismus. Je-li H podgrupa grupy $(G, \cdot)$, pak inkluze je vnořením $(a \mapsto a)$.

1.5 Cayleho věty

Budeme pracovat s touto strukturou: nechť A je množina. $(A^A, \circ)$ je pologrupa.

Věta 1.54
Libovolná pologrupa je izomorfní podpologrupě pologrupy $(A^A, \cdot)$ pro vhodnou množinu A.

Důkaz: Nechť $(S,\cdot)$ je pologrupa. Definujeme pro $a \in S$ zobrazení $\rho_a : S \to S$ vztahem $f_a(x) = a \cdot x$ pro libovolné $x \in S$. ρ je vnoření $(S,\cdot)$ do $(S^S,\circ)$.

Chceme dokázat, že ρ je homomorfismus:

Pro $a,b \in S$, $x \in S$, pak $\rho_{a.b}(x) = a.b.x$. Platí $\rho_a \circ \rho_b(x) = \rho_a(\rho_b(x)) = \rho_a(b.x) = a.b.x$. Tedy jde skutečně o homomorfismus. Chceme navíc, že ρ je prosté:

$a,b \in S$, $\rho_a = \rho_b$. Lze předpokládat, že naše pologrupa S je monoid, není-li, pak přidáme 1. Platí $\rho_a(1) = \rho_b(1)$, z toho $a.1 = b.1$, a tedy $a = b$. A máme izomorfismus.

□

Věta 1.55

Libovolná grupa $(G,\cdot)$ je izomorfní s podgrupou (=lze vnořit do) grupy $(PermA,\circ)$ pro vhodnou množinu A. Za A lze vzít G.

1.6 Klasifikace cyklických grup

Věta 1.56

Libovolná nekonečná cyklická grupa je izomorfní grupě $(\mathbf{Z},+)$.

Libovolná n-prvková ($n \in \mathbf{N}$) cyklická grupa je izomorfní grupě $(\mathbf{Z_n},+)$.

1.7 Součiny grup

Definice 1.57

Nechť $(G,\cdot)$, $(H,\circ)$ jsou grupy. Na množině $G \times H$ definujeme operaci $\diamond$ takto: $(a,b) \diamond (a',b') := (a \cdot a', b \circ b')$. (násobení po složkách)

Lemma 1.58

$(G \times H,\diamond)$ je grupa. Zobrazení $\epsilon : G \times H \to G$ $(a,b) \mapsto a$, $\eta : G \times H \to H$ $(a,b) \mapsto b$ jsou surjektivní homomorfismy grupy $(G \times H,\diamond)$ na $(G,\cdot)$ respektive $(H,\circ)$.

Věta 1.59

Nechť $(G,\cdot)$ je komutativní grupa, H a K její podgrupy. Nechť $H \cap K = \{1\}, G \subseteq H \cdot K$ $(= \{h \cdot k | h \in H, k \in K\})$ Pak $(G,\cdot) \cong (H,\cdot) \times (K,\cdot)$.

1.8 Klasifikace konečných komutativních grup

Věta 1.60

Nechť $(G,\cdot)$ je konečná komutativní grupa, $|G| \geq 2$. Pak

$$(G,\cdot) \cong (\mathbf{Z}_{p_1^{k_1}},+) \times \ldots \times (\mathbf{Z}_{p_m^{k_m}},+)$$

kde $m,k_1,\ldots,k_m \in \mathbf{N}$, $p_1,\ldots,p_m$ jsou prvočísla. Tento rozklad je jednoznačný až na pořadí činitelů.

1.9 Lagrangeova věta

Definice 1.61

Nechť $(G,\cdot)$ je grupa, H její podgrupa, definujme $aH := \{a \cdot h | h \in H\}$, $G/H := \{aH | a \in G\}$.

Lemma 1.62

Pro $a,b \in G$ je ekvivalentní :

1. $aH = bH$

2. $a \in bH$
3. $b^{-1}a \in H$

Věta 1.63
G/H je rozklad na množině G. Libovolné dvě třídy jsou stejně mohutné.

Důkaz:

- $\bigcup_{a\in G} aH \supseteq G$, neboť $a \in aH$.
- nechť $c \in aH \cap bH$, pak $\exists h, k \in H$ tak,že

$$\begin{aligned} c = ah &= b \cdot k \qquad | \cdot h^{-1} zprava \\ a &= b \cdot k \cdot h^{-1} \quad \in bH; \quad k \cdot h^{-1} \in H \end{aligned}$$

Tedy $aH = bH$ a jde o rozklad.

Nechť $a \in G$, $\alpha : H \to aH, h \mapsto ah$. α je surjektivní a injektivní. Tedy bijekce a mezi lib. dvěma třídami. Proto jsou lib. dvě třídy stejně velké.

□

Důsledek 1.64
Nechť $(G, \cdot)$ je komutativní grupa, $|G| = n$. Pak

1. $|G| = |G/H| \cdot |H|$, pro libovolnou podgrupu H.
2. (LAGRANGEOVA VĚTA) $|H|$ dělí $|G|$, pro libovolnou podgrupu H.
3. $a \in G$ řádu m, pak $m|n$.
4. je-li n prvočíslo, je $(G, \cdot)$ cyklická.
5. (FERMATOVA VĚTA) $a \in G$, pak $a^n = 1$.

Důsledek 1.65 (EULER)
Nechť $a, n \in \mathbf{N}$, $(a, n) = 1$. Pak $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Důkaz: uvažujme grupu invertibilních prvků v $(\mathbf{Z}_n, \cdot)$. Tato grupa má $\varphi(n)$ prvků ($[a]_n$ má inverzi $\Leftrightarrow (a, n) = 1$) $[a]_n^{\varphi(n)} = [1]_n$ □

1.10 Faktorové grupy

Definice 1.66
Podgrupa H grupy $(G, \cdot)$ se nazývá normální, platí-li $\forall a \in G : \forall h \in H : a^{-1}ha \in H$.
$G/H := \{aH | a \in G\}$ - levý rozklad
$H\backslash G := \{Ha | a \in G\}$ - pravý rozklad

Lemma 1.67
Je ekvivalentní:

1. H je normální grupa.
2. $\forall a \in G : aH = Ha (\Leftrightarrow G/H = H\backslash G)$
3. Na G/H definujeme takto operaci: $aH \cdot bH := (a \cdot b)H$.

Věta 1.68
Je-li $(G,\cdot)$ grupa, H její normální podgrupa, pak G/H s operací definovanou výše je grupa. Zobrazení $natH : G \to G/H, a \mapsto aH$ je surjektivní homomorfismus grupy $(G,\cdot)$ na grupu $(G/H,\cdot)$.

Definice 1.69
Nechť $\alpha : (G,\cdot) \to (H,\cdot)$ je homomorfismus grup, klademe $J(\alpha) := \{a \in G | \alpha(a) = 1\}$.

Lemma 1.70
Nechť $(G,\cdot)$ je grupa. Normální podgrupy v $(G,\cdot)$ jsou právě jádra homomorfismů vedoucích z $(G,\cdot)$.

Důkaz: nechť H je normální podgrupa v $(G,\cdot)$. $natH : (G,\cdot) \to (G/H,\cdot)$

$$\begin{aligned} J(natH) &= \{a \in G | (natH)(a) = H\} \\ &= \{a \in G | aH = H\} = H \end{aligned}$$

Naopak, buď $\alpha : (G,\cdot) \to (H,\cdot)$ homomorfismus, dokážeme, že $J(\alpha)$ je normální podgrupa v $(G,\cdot) : 1 \in J(\alpha)$
$a, b \in J(\alpha) \Rightarrow \alpha(a) = \alpha(b) = 1 \Rightarrow \alpha(ab) = \alpha(a) \cdot \alpha(b) = 1$
$\alpha(a^{-1}) = (\alpha(a))^{-1} = 1^{-1} = 1$ a máme podgrupu.
Normálnost: $a \in G$, $b \in J(\alpha)$. Chceme $a^{-1}ba \in J(\alpha)$. $\alpha(a^{-1} \cdot b \cdot a) = (\alpha(a))^{-1} \cdot \alpha(b) \cdot \alpha(a) = 1$. □

Lemma 1.71
$J(\alpha) = \{1\} \Leftrightarrow$ α je prosté.

Věta 1.72
Nechť $\alpha : (g,\cdot) \to (H,\cdot)$ je homomorfismus grup. G' je normální podgrupa $(G,\cdot)$, nechť $G' \subseteq J(\alpha)$. Pak existuje jediný homomorfismus $\beta : (G/G',\cdot) \to (H,\cdot)$ takový, že $\beta \circ natG' = \alpha$.

Důsledek 1.73
Nechť $\alpha : (G,\cdot) \to (H,\cdot)$ je surjektivní homomorfismus. Pak $(G,\cdot)/J(\alpha) \cong (H,\cdot)$.

2 Okruhy a polynomy

2.1 Zavedení pojmu okruh

Definice 2.1
Uspořádanou trojici $\mathcal{R} = (R,+,\cdot)$ nazýváme okruh, je-li $(R,+)$ komutativní grupa, $(R,\cdot)$ monoid a jsou-li splněny tzv. distributivní zákony:

$$\begin{aligned} \forall a,b,c \in R : a(b+c) &= ab + ac \\ (a+b)c &= ac + bc. \end{aligned}$$

$\mathcal{R}$ se nazývá komutativní okruh, je-li $(R,\cdot)$ komutativní.

Označení:

- 0 ... je neutrální prvek vzhledem k +,
- $-a$ ... inverzi prvku a vzhledem k + nazýváme opační prvek,

- 1 . . . je neutrální prvek vzhledem k $\cdot$,
- $\mathcal{R}$ se nazývá triviální, je-li $|R| = 1$,
- $a - b := a + (-b)$.

Lemma 2.2
Nechť $\mathcal{R} = (R, +, \cdot)$ je okruh. Pak

1. $0a = a0 = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $a(b - c) = ab - ac$
4. $\mathcal{R}$ je triviální $\Leftrightarrow 0 = 1$

Definice 2.3
Okruh $\mathcal{R}$ se nazývá obor integrity, je-li netriviální, komutativní a platí $\forall a, b \in R : (ab = 0 \Rightarrow a = 0 \vee b = 0)$.

Tedy v oboru integrity se nevyskytují dělitelé nuly nebo také, analogicky, nenulové prvky jsou uzavřeny vzhledem k násobení.

Lemma 2.4
$(\mathbf{Z_n}, +, \cdot)$ je obor integrity $\Leftrightarrow$ n je prvočíslo.

Definice 2.5
Okruh $\mathcal{R}$ se nazývá těleso, je-li $(R^*, \cdot)$ komutativní grupa.

$\mathbf{Q}, \mathbf{R}, \mathbf{C}$ jsou tělesa. Naprosto zřejmé je, že je-li $\mathcal{R}$ těleso, pak $\mathcal{R}$ je i oborem integrity.

2.2 Základní vlastnosti

Definice 2.6
Charakteristika okruhu $\mathcal{R}$ je řád 1 v $(R, +)$. Značíme $char\mathcal{R}$.

Příklad 2.1
$char\mathbf{Z_n} = n$, číselné okruhy mají charakteristiku 0.

Lemma 2.7
Nechť $char\mathcal{R} = n$, $a \in R$, pak platí $n \cdot a = 0$. ($n \cdot a$ znamená $\overbrace{a + a \cdots + a}^{n}$).

Lemma 2.8
Charakteristika oboru integrity je 0 nebo prvočíslo.

Definice 2.9
Buď $\mathcal{R}$ komutativní okruh, $a, b \in R$. a dělí b, jestliže $\exists c \in R : \ a \cdot c = b$. Píšeme $a|b$. Prvky a,b nazýváme asociované, je-li $a|b$, $b|a$. Píšeme $a \sim b$. Prvek $e \in R$ nazýváme jednotkou (v libovolném okruhu), má-li v $(R^*, \cdot)$ inverzi.

V $\mathbf{R}$ jsou jednotky všechna čísla mimo 0 a asociované prvky jsou všechny dvojice nenulových čísel.

Lemma 2.10
Platí:

1. $\sim$ je relace ekvivalence na R.

2. $\mathcal{R}$ obor integrity. Pak $a \sim b$ právě, když existuje jednotka c tak, že $b = a \cdot c$.

Definice 2.11

Buď $\mathcal{R}$ komutativní okruh, $a, b, c, d \in R$.

Prvek c je společný dělitel prvků a,b, platí-li $c|a, c|b$.

Prvek c je největší společný dělitel, je-li společný dělitel a pro libovolný jiný společný dělitel d platí $d|c$.

Definice 2.12

Libovolný prvek $a \in R$ je dělitelný libovolnou jednotkou a libovolným prvkem asociovaným s a, tyto dělitele nazýváme nevlastní dělitele.

Definice 2.13

Prvek $a \in R$ se nazývá ireducibilní, je-li různý od 0, není jednotkou a má jen nevlastní dělitele.

Lemma 2.14

Nechť $\mathcal{R}$ je komutativní okruh, pak

1. pokud existuje největší společný dělitel prvků a,b je určen jednoznačně až na asociovanost.
2. je-li a ireducibilní, $a \sim b$, pak je prvek b také ireducibilní.

2.3 Vítaná vlastnost okruhů

Vlastnost, která je u okruhů tak ceněná, je jednoznačnost rozkladu. Uvedeme si definici, která tento pojem zavádí přesně.

Definice 2.15

Libovolný prvek $a \in R^*$, který není jednotkou, lze psát ve tvaru $a = p_1 \dots p_k$, kde $k \in \mathbf{N}$, $p_1, \dots, p_k$ jsou ireducibilní prvky. Pokud též $a = q_1 \cdots q_l$, kde $l \in \mathbf{N}$, $q_1, \dots, q_l$ jsou ireducibilní, potom $l = k$ a zároveň existuje permutace π množiny $\{1, \cdots, k\}$ tak, že $q_i \sim p_{\pi(i)}$.

Příklad 2.2

Okruh $(\mathbf{Z}, +, \cdot)$ je s jednoznačným rozkladem, libovolné těleso je okruhem s jednoznačným rozkladem.

2.4 Podokruhy

Definice 2.16

Nechť $\mathcal{R} = (R, +, \cdot)$ je okruh, množina M se nazývá podokruhem okruhu $\mathcal{R}$, platí-li $M \subseteq R$, $0, 1 \in M$, a jestliže $a, b \in M$, pak platí $a + b, a \cdot b, -a \in M$.

Poznámka 2.17

Zejména $(M, +)$ je podgrupa grupy $(R, +)$. Zřejmě i $(M, +/M \times M, \cdot/M \times M)$ je okruh.

Lemma 2.18

Nechť S_i pro $i \in I, I \neq \phi$ je podokruh okruhu $\mathcal{R} = (R, +, \cdot)$. Pak také $\bigcap_{i \in I} S_i$ je podokruh.

Zavedeme následující označení: Pro libovolnou množinu $M \subseteq R$ existuje nejmenší podokruh okruhu R obsahující M. Nazveme ho podokruh generovaný množinou M, označíme $[M]$. Dále nechť S je podokruh okruhu $\mathcal{R}$, $a \in R$; místo $[S \cup \{a\}]$ píšeme $S[a]$.

Lemma 2.19

$S[a] = \{\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n | n \in \mathbf{N}_0, \alpha_0, \ldots, \alpha_n \in S\}$.

2.5 Homomorfismy okruhů, podílové těleso

Definice 2.20

Nechť $\mathcal{R} = (R, +, \cdot)$, $\mathcal{S} = (S, +, \cdot)$ jsou okruhy. Zobrazení $\alpha : R \to S$ se nazývá homomorfismus okruhu $\mathcal{R}$ do okruhu $\mathcal{S}$, platí-li:

- $\alpha(a + b) = \alpha(a) + \alpha(b)$
- $\alpha(a \cdot b) = \alpha(a) \cdot \alpha(b)$
- $\alpha(1) = 1_{\mathcal{R}}$, kde $a, b \in R$.

Zejména se jedná o homomorfismus grupy $(R, +)$ do grupy $(S, +)$. Dále α se nazývá izomorfismus, je-li α bijektivní. $\mathcal{R}$ a $\mathcal{S}$ se nazývají izomorfní, existuje-li izomorfismus $\mathcal{R}$ na $\mathcal{S}$.

Lemma 2.21

Nechť $\alpha : \mathcal{R} \to \mathcal{S}$ je homomorfismus okruhů.

- α je prosté $\Leftrightarrow J(\alpha) := \{a \in R | \alpha(a) = 0\} = \{0\}$
- Libovolný homomorfismus těles je prostý a pro $a \in R^*$ platí $\alpha(a^{-1}) = (\alpha(a))^{-1}$

Lemma 2.22

Nechť $\mathcal{R} = (R, +, \cdot)$ je obor integrity. Na množině $R \times R^*$ definujeme relaci $\sim$ takto:

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Pak $\sim$ je relace ekvivalence.

Označíme třídu ekvivalence takto: $\frac{a}{b} = [(a, b)]_{\sim}$

Definice 2.23

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

$$Q(\mathcal{R}) := \{\frac{a}{b} | (a, b) \in R \times R^*\}$$

Množina $Q(\mathcal{R})$ se označuje také jako podílové těleso.

Věta 2.24

$+, \cdot$ jsou korektně definované operace na $Q(\mathcal{R})$.
$(Q(\mathcal{R}), +, \cdot)$ je těleso.

Definice 2.25 RACIONÁLNÍ ČÍSLA

$$\mathbf{Q} := Q((\mathbf{Z}, +, \cdot))$$

Věta 2.26

Nechť $\mathcal{R} = (R, +, \cdot)$ je obor integrity, $\sim : R \to Q(\mathcal{R}); a \mapsto \frac{a}{1}$ je prostý homomorfismus $\mathcal{R}$ do $Q(\mathcal{R})$. Je-li $\alpha : \mathcal{R} \to \mathcal{T}$ prostý homomorfismus do tělesa $\mathcal{T}$, existuje jediný homomorfismus $\beta : Q(\mathcal{R}) \to \mathcal{T}$ takový, že $\beta \circ \sim = \alpha$.

Definice 2.27 ZAVEDENÍ PŘIROZENÝCH ČÍSEL

$\mathbf{N}_0$ je nejmenší množina obsahující ϕ a uzavřená vzhledem k (unární) operaci $a \mapsto a \cup \{a\}$.

Definice 2.28
Zavedeme relaci $\sim$ na $\mathbf{N}_0 \times \mathbf{N}_0$ takto:

$$(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$$

Jde zřejmě o relaci ekvivalence.

Definice 2.29

$$\mathbf{Z} := (\mathbf{N}_0 \times \mathbf{N}_0)/\sim$$

Prvek této množiny vyjádříme jako $a-b := [(a,b)]_\sim$. Operace budou zavedeny takto:

$$(a-b)+(c-d) := (a+c)-(b+d) \qquad (a-b)\cdot(c-d) := (ac+bd)-(ad+bc)$$

2.6 Polynomy

Definice 2.30
Nechť $\mathcal{R} = (R,+,\cdot)$ je okruh. Polynomem nad $\mathcal{R}$ nazýváme posloupnost $f = (f_0, f_1, \ldots)$ prvků z R takovou, že skoro všechny jsou rovny 0 (tzn. všechny až na konečný počet; nebo od jistého místa jsou všechny nulové).
$R[x]$ — je množina všech polynomů na $\mathcal{R}$.
Na $R[x]$ definujeme operace $+,\cdot$ takto:

$$(f_0, f_1, \ldots) + (g_0, g_1, \ldots) = (f_0+g_0, f_1+g_1, \ldots)$$

$$(f_0, f_1, \ldots) \cdot (g_0, g_1, \ldots) = (h_0, h_1, \ldots),$$

kde $h_i := \sum_{j=0}^{i} f_j g_{i-j}$ pro $i = 0,1,\ldots$. Zřejmě je $h_0 = f_0 g_0$; $h_1 = f_0 g_1 + f_1 g_0$; $\ldots$

Lemma 2.31
$\mathcal{R}[x] = (R[x],+,\cdot)$ je okruh. Je-li $\mathcal{R}$ komutativní, je i $\mathcal{R}[x]$ komutativní. Je-li $\mathcal{R}$ obor integrity, je i $\mathcal{R}[x]$ obor integrity (toto neplatí pro těleso !).

Definice 2.32
Stupeň polynomu f, $st(f)$ je největší $n \in \mathbf{N}$ takové, že $f_n \neq 0$, kde f_n je vedoucí koeficient polynomu f. Stupeň polynomu $(0,0,\ldots)$ klademe $-\infty$.

Lemma 2.33
Nechť f,g jsou polynomy.

$$st(f+g) \leq max\{st(f), st(g)\}$$

$$st(f.g) \leq st(f) + st(g)$$

Je-li R obor integrity, platí ve 2. případě rovnost.

Lemma 2.34
Nechť R je obor integrity,$f \in R[x]$. f je jednotka v $R[x]$ právě tehdy, když je konstantní a je jednotkou v R.
(jen na okraj: ztotožňujeme prvky z R a konstantní polynomy)

Příklad 2.3
v okruhu $(\mathbf{Z}_n,+,\cdot)$ platí:
$(2x+1)(2x+1) = 1$ — tento nekonstantní polynom je jednotkou

Lemma 2.35

Nechť R je obor integrity, $f, g \in R[x]$. Nechť vedoucí koeficient polynomu g je jednotkou v R. Pak existují, a to jednoznačně polynomy $q, r \in R[x]$ takové, že $f = q \cdot q + r$, $st(r) < st(g)$.

Příklad 2.4

Nejsme-li nad oborem integrity, není jednoznačnost:

$$2x + 1 = 1(2x + 1) + 0 = 2x(2x + 1) + 1$$

Věta 2.36

Je-li R těleso, $f, g \in R[x]$. Pak existuje největší společný dělitel h těchto polynomů a existují polynomy u,v tak,že $u \cdot f + v \cdot g = h$

Důkaz: viz Euklidův algoritmus a důkaz Bezoutovy rovnosti □

Lemma 2.37

Nechť R je obor integrity. $f, g \in R[x]$ jsou asociovány právě tehdy,když existuje jednotka $c \in R$ tak, že $g = c \cdot f$.

Definice 2.38

Normovaný polynom má vedoucí koeficient roven 1 (jedné).

Věta 2.39

Nechť R je těleso, $f, g \in R[x] \setminus \{0\}$. Pak existuje jediný jejich normovaný největší společný dělitel, označujeme ho (f, g).

Důkaz: plyne z předchozí věty a lemmatu o jednoznačnosti NSD □

Definice 2.40

Polynomy f,g se nazývají nesoudělné, platí-li $(f, g) = 1$.

Věta 2.41

Nechť R je těleso, $f, g, h \in R[x]$. Jestliže $f|g \cdot h$, $(f, g) = 1$, pak platí $f|h$.

Důkaz: viz Bezoutova rovnost □

Definice 2.42

Polynom f se nazývá ireducibilní, je-li nekonstantní a není-li součinem dvou nekonstantních polynomů.

Příklad 2.5

V polynomech $\mathbf{Z}[x]$: 2 — je ireducibilní prvek (nad $\mathbf{Z}$), není ireducibilní polynom.

2x — je ireducibilní polynom, není ireducibilní prvek.

Lemma 2.43

Nechť R je těleso. Pak $f \in R[x]$ je ireducibilní polynom $\Leftrightarrow$ je ireducibilní prvek.

Poznámka 2.44

Nad oborem integrity je libovolný lineární polynom ireducibilní.

Věta 2.45

Nechť R je těleso. Pak $R[x]$ je okruh s jednoznačným rozkladem.

($f \in R[x]$ nekonstantní, f lze psát ve tvaru $f = a \cdot p_1 p_2 \dots p_k$ a to jediným způsobem až na pořadí činitelů; $a \in \mathbf{R}$, $p_1 p_2 \dots p_k$ jsou normované ireducibilní polynomy)

Důkaz: Existence: $f \in R[x]$ nekonstantní; indukcí vzhledem ke n:= st(f)

- $n = 1$, f se normuje
- $n \geq 2$ buď f je ireducibilní, pak se f normuje, nebo $f = g \cdot h$, $st(g), st(h) \geq 1$ a použiji indukční předpoklad.

Jednoznačnost: $f = a \cdot p_1 \dots p_k = b \cdot q_1 \dots q_l$

Zřejmě $a = b$ jako koeficienty nejvyšší mocniny.

Kdyby $p_k \neq q_1, \dots, q_l$ bylo by $(p_k, q_1) = \dots (p_k, q_l) = 1$, $(p_k, b) = 1$ a NSD je konstantní polynom. (Platí $f|gh, (f,g) = 1 \Rightarrow f|h$) l-krát aplikovat, dostali bychom $p_k|1$ tedy spor. Proto musí $p_k = q_m, \quad (1 \leq m \leq l)$

$$p_1 \dots p_{k-1} = q_1 \dots q_{m-1} q_{m+1} \dots q_l$$

Použijeme dále indukci vzhledem ke k. □

2.7 Kořeny polynomů

Definice 2.46

Nechť je R okruh, $c \in R$, $f \in R[x]$, $f = f_n x^n + \dots + f_1 x + f_0$. c se nazývá kořenem polynomu f, platí-li

$$f(c) := f_n c^n + \dots + f_1 c + f_0 = 0.$$

Lemma 2.47

Nechť R je komutativní okruh, $c \in R$, $f, g \in R[x]$. Pak platí:

1. $(f + g)(c) = f(c) + g(c)$
2. $(fg)(c) = f(c) \cdot g(c)$

Věta 2.48

Nechť R je komutativní okruh, $c \in R$, $f \in R[x]$. Pak c je kořen f právě tehdy, když platí $(x - c)|f$.

Definice 2.49

Nechť R je komutativní okruh, $c \in R$, $f \in R[x]$, $k \geq 1$. c je k-násobný kořen f, platí-li $(x - c)^k | f$, a zároveň $(x - c)^{k+1} \not| f$.

Věta 2.50

Nechť R je těleso, f nenulový polynom nad R, pak f má nejvýše $n = st(f)$ kořenů, počítáme-li každý tolikrát, co jeho násobnost.

Poznámka 2.51

Větu je možno zobecnit až na okruh integrity.

Definice 2.52

Nechť R je okruh, $f \in R[x]$, definujme $\varphi(f) : R \to R, a \mapsto f(a)$

Věta 2.53

Nechť R je nekonečný obor integrity. Pak $f = g$ právě tehdy, když $\varphi(f) = \varphi(g)$.

Definice 2.54

Nechť $f = a_n x^n + \dots + a_1 x + a_0$ Definujeme $f' = n a_n x^{x-1} + \dots + a_1$ a nazýváme derivace f.

Lemma 2.55

Platí $(f + g)' = f' + g'$, $(f \cdot g)' = f' \cdot g + f \cdot g'$.

Věta 2.56
Nechť R je těleso charakteristiky 0, $f \in R[x]$, $c \in R$. Jestliže c je k-násobný kořen f, $k \geq 2$, pak c je (k-1)-násobný kořen f'. Jestliže c je jednoduchý kořen (násobnosti jedna) f, pak c není kořen f'.

Definice 2.57
Těleso R se nazývá algebraicky uzavřené, má-li každý nekonstantní polynom nad R v R kořen.

Věta 2.58
Žádné konečné těleso není algebraicky uzavřené.

Příklad 2.6
pro $R = \{a_1, \ldots a_n\}$ polynom $f = (x - a_1) \ldots (x - a_n) + 1$ nemá v R kořen.

Věta 2.59
Těleso R je algebraicky uzavřené $\Leftrightarrow$ ireducibilní polynomy jsou právě lineární polynomy.

2.8 Polynomy nad C, R, Q

Věta 2.60 Základní věta algebry
Těleso $\mathbf{C}$ je algebraicky uzavřené.

Lemma 2.61
Nechť $c \in \mathbf{C}$ je kořen $f \in \mathbf{R}[x]$. Pak $\overline{x}$ je kořen f.

Věta 2.62
Nad $\mathbf{R}$ jsou ireducibilní polynomy právě lineární polynomy a kvadratické polynomy se záporným diskriminantem.

Věta 2.63
Nechť $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$. $\frac{p}{q}$ je kořen f, $p \in \mathbf{Z}$, $q \in \mathbf{Z} \setminus \{0\}$, $(p, q) = 1$. Pak $p|a_0$, $q|a_n$. Pro $r \in \mathbf{Z}$ platí $(p - rq)|f(r)$.

Věta 2.64
Polynom $f \in \mathbf{Z}[x]$ je ireducibilní $\Leftrightarrow$ je ireducibilní nad $\mathbf{Q}$.

Věta 2.65 Eisensteinovo kriterium
Nechť máme polynom $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$. Jestliže existuje prvočíslo p tak, že $p|a_0, \ldots p|a_{n-1}, p$nedělí$a_n, p^2$nedělí$a_0$ potom f je ireducibilní nad $\mathbf{Q}$.

Příklad 2.7
$x^n + 2$ je ireducibilní nad $\mathbf{Q}$ (pro prvočíslo p=2).