2 Grupy, tělesa a aritmetika modulo p

2.1 Grupy a tělesa

Řada algebraických objektů má podobu množiny s nějakou dodatečnou strukturou. Například vektorový prostor je množina vektorů, ty však nejsou 'jeden jako druhý': jeden z nich hraje význačnou roli nulového vektoru, pro každé dva vektory je dán jejich součet, je definována operace násobení vektoru skalárem atd. Právě tuto dodatečnou informaci, která vektorový prostor odlišuje od pouhé množiny vektorů, máme na mysli, když mluvíme o 'struktuře'. Často se i samotné tyto objekty označují pojmem *algebraické struktury*.

Dva význačné příklady takových struktur zavedeme v tomto oddílu: jsou jimi grupa a těleso. Jsou definovány jako množina s jednou resp. dvěma operacemi, které mají (v porovnání s většinou ostatních algebraických struktur) poměrně silné vlastnosti. Příkladů grup i těles je přesto podivuhodná řada, a to v nejrůznějších oblastech matematiky.

Pojem tělesa ostatně čtenář obeznámený s vektorovými prostory možná zná. Každý vektorový prostor totiž existuje nad určitým tělesem, jehož prvky jsou právě ony skaláry, jimiž můžeme vektory násobit. Vektorové prostory nad tělesem reálných čísel (probírané v přednášce z lineární algebry) jsou tak jen jedním speciálním případem.

Nechť M je množina. Zobrazení $\star$ z $M \times M$ do M se nazývá *(binární) operace na množině M*. Taková operace může mít různé vlastnosti. Řekneme, že $\star$ je *komutativní* operace, pokud pro každé $x, y \in M$ je $x \star y = y \star x$ (tedy pokud výsledek nezáleží na pořadí operandů). Operace $\star$ je *asociativní*, pokud pro $x, y, z \in M$ je $x \star (y \star z) = (x \star y) \star z$ (výsledek nezáleží na uzávorkování).

Příklad asociativní operace jsme již viděli u relací. Uvážíme-li množinu všech relací na dané množině X a definujeme-li operaci $\circ$ jako složení dvou relací, bude tato binární operace asociativní, ale nikoli komutativní.

Prvky množiny M mohou mít vzhledem k operaci $\star$ speciální vlastnosti. Prvek $n \in M$ je *neutrálním prvkem (vzhledem k operaci $\star$)*, pokud pro každé $x \in M$ je $x \star n = x$ a rovněž $n \star x = x$. Všimněme si, že z definice triviálně plyne, že takový prvek je nejvýše jeden. Jsou-li totiž n, n' neutrální prvky, pak na jednu stranu $n \star n' = n'$ (protože n je neutrální), ale na druhou stranu $n \star n' = n$ (protože n' je neutrální), takže $n = n'$.

Nechť n je neutrální prvek vzhledem k operaci $\star$. *Prvek inverzní k prvku $x \in M$* je takový prvek y, pro nějž platí, že $x \star y = y \star x = n$. V případě, že $\star$ je asociativní operace, je opačný prvek k libovolnému prvku $x \in M$ nejvýše jeden. Jsou-li totiž y, y' dva takové prvky, uvažme výraz $y \star x \star y'$. Obě jeho uzávorkování dají stejný výsledek. Přitom $(y \star x) \star y' = n \star y' = y'$, ale $y \star (x \star y') = y \star n = y$, takže $y = y'$.

Nyní již můžeme definovat pojem grupy. *Grupa* je množina M spolu s asociativní binární operací $\star$, ve které existuje neutrální prvek a ke každému prvku existuje prvek inverzní. Pokud je operace $\star$ navíc komutativní, mluvíme o *komu-*

tativní nebo *abelovské grupě*.

Standardními příklady grup jsou třeba množina všech reálných (celých, komplexních, racionálních) čísel s operací sčítání. Přirozená čísla se sčítáním grupu netvoří (0 je neutrální, ale neexistuje skoro žádný inverzní prvek), a třeba celá čísla s násobením rovněž ne (1 je neutrální, ale inverzní prvky rovněž neexistují). Ani v množině racionálních čísel neexistuje inverzní prvek k číslu 0 vzhledem k operaci násobení (pro žádné racionální y není $0 \cdot y = 1$). Oproti tomu množina všech *nenulových* racionálních čísel již tvoří grupu vzhledem k operaci násobení.

Množina všech matic daných rozměrů je grupou vzhledem ke sčítání. Grupou je rovněž množina všech regulárních čtvercových matic řádu n s operací násobení. Požadavek regularity je podstatný, protože k žádné singulární matici by neexistoval inverzní prvek. Spojité reálné funkce tvoří grupu vzhledem ke sčítání, permutace dané množiny vzhledem ke skládání, atd. Relace na dané množině spolu s operací skládání grupu netvoří.

Pojem tělesa zachycuje dvě grupy, definované na téže základní množině. Jeho prototypem je množina všech reálných čísel $\mathbf{R}$ s operacemi $+$ a $\cdot$. Dvojice $(\mathbf{R}, +)$ je komutativní grupa s neutrálním prvkem 0, dvojice $(\mathbf{R}, \cdot)$ ale grupa není (stejně jako u racionálních čísel chybí inverzní prvek k číslu 0). Z tohoto důvodu v následující definici tělesa přistupujeme k neutrálnímu prvku první operace s jistou opatrností.

Nechť množina M spolu s operací $\oplus$ tvoří komutativní grupu s neutrálním prvkem (dejme tomu) 0, a nechť na množině $M \setminus \{0\}$ je určena další binární operace $\otimes$. Potom $(M, \oplus, \otimes)$ je *těleso*, pokud $(M \setminus \{0\}, \otimes)$ je rovněž komutativní grupa a navíc platí *distributivní zákon*:

$$x \otimes (y \oplus z) = (x \oplus y) \otimes (x \oplus z) \tag{1}$$

pro každé $x, y, z \in M$.

Mezi tělesa patří množiny všech racionálních, reálných a komplexních čísel, vždy se standardními operacemi sčítání a násobení. V následujícím oddílu budeme hovořit o tělesech, která sestávají jen z konečného počtu prvků.

Všimněme si ještě, že pojem vektorového prostoru není příliš vzdálen od pojmu abelovské grupy. Dá se říci, že vektorový prostor je abelovská grupa (s operací sčítání vektorů), na které je navíc definováno násobení vektorů prvky daného tělesa.

2.2 Aritmetika modulo p

Připomeňme si, že ekvivalence $\sim$ na množině X je relace na X, která je reflexívní, symetrická a tranzitivní. Jsou-li na množině X definovány nějaké operace, může být přirozený požadavek, aby ekvivalence $\sim$ navíc zachovávala tyto dodatečné operace. Takovým ekvivalencím se pak říká kongruence. My se zaměříme na jeden konkrétní příklad: kongruence modulo p.

Nechť $p \geq 1$ je přirozené číslo. Definujme na množině všech celých čísel relaci $\equiv$ (*kongruenci modulo* p) předpisem

$$x \equiv y, \text{ pokud } p \text{ dělí rozdíl } x - y.$$

Je-li potřeba zdůraznit hodnotu čísla p, píšeme $x \equiv y \pmod p$.

Fakt, že se jedná o ekvivalenci, není ani třeba dokazovat. Každá z p tříd této ekvivalence je tvořena všemi čísly, které při dělení číslem p dávají tentýž zbytek. Proto se označují jako *zbytkové třídy modulo* p. Třídu obsahující číslo x budeme značit jako $[x]_p$ (jindy se používá značení $\mathcal{Z}_p(x)$) a o prvku x budeme mluvit jako o reprezentantu této třídy. Je-li číslo p zřejmé z kontextu, píšeme místo $[x]_p$ prostě $[x]$. Množina všech zbytkových tříd modulo p se značí $\mathbf{Z}/p$. Třídy $[0]_p$ a $[1]_p$, které mají svým způsobem význačné postavení, budeme značit prostě 0 resp. 1.

Jak je naznačeno v úvodu tohoto oddílu, kongruence modulo p se chová ‘slušně’ k operacím sčítání a násobení na celých číslech:

Tvrzení 2.1 *Nechť $x \equiv x'$ a $y \equiv y'$ jsou celá čísla. Potom*

$$x + y \equiv x' + y' \quad a \quad xy \equiv x'y'.$$

Důkaz. Z faktu $x \equiv x'$ plyne $x' - x = pm$, kde m je celé. Podobně $y' - y = pn$, n celé. Potom $(x'+y') - (x+y) = pm + pn = p(m+n)$, takže $x + y \equiv x' + y'$. Stejně tak $x'y' - xy = (x + pm)(y + pn) - xy = p(xn + ym + pmn)$, proto $x'y' \equiv xy$. □

Hlavním důvodem, proč je tento fakt důležitý, je, že umožňuje přenést aritmetické operace z celých čísel na zbytkové třídy, kde tak dostaneme tzv. *aritmetické operace modulo* p. Nechť číslo p je pevně dáno, takže jej nemusíme explicitně uvádět. Pro třídy $[x]$ a $[y]$, zadané pomocí svých reprezentantů, definujeme jejich součet $\oplus$ a součin $\otimes$ předpisy

$$\begin{aligned} [x] \oplus [y] &= [x + y]\,, \\ [x] \otimes [y] &= [xy]\,. \end{aligned}$$

U podobné definice je však třeba ověřit její *korektnost*: nedostaneme při jiné volbě reprezentantů tříd $[x]$ a $[y]$ jiné výsledky? Kdyby ano, jednalo by se o špatnou definici.

Proto předpokládejme, že $[x] = [x']$ a $[y] = [y']$. To samozřejmě znamená, že $x \equiv x'$ a $y \equiv y'$. Podle Tvrzení 2.1 tedy $x + x' \equiv y + y'$. Pak ovšem musí být $[x + y] = [x' + y']$, takže hodnota přiřazená součtu $[x] \oplus [y]$ je na volbě reprezentantů nezávislá. Podobně je tomu u operace $\otimes$.

Podívejme se pro konkrétnost na případ $p = 7$, třeba na třídy $[2]_7$ a $[6]_7$. Z definice je

$$\begin{aligned} [2]_7 &= \{\ldots, -5, 2, 9, 16, \ldots\}, \\ [6]_7 &= \{\ldots, -1, 6, 13, 20, \ldots\}. \end{aligned}$$

Všechny možné součty prvku z třídy $[2]_7$ a prvku z třídy $[6]_7$ tvoří množinu

$$\{\dots, -6, 1, 8, 15, 22, \dots\},$$

což je právě třída $[8]_7$, takže je přirozené, že jsme položili $[2]_7 \oplus [6]_7 = [8]_7$. Podobně množina všech součinů prvku ze třídy $[2]_7$ a prvku ze třídy $[6]_7$ tvoří přesně třídu $[12]_7$.

Množina $\mathbf{Z}_7$ má 7 prvků, které lze psát například jako $[0]_7$, $[1]_7$, $\dots$, $[6]_7$. Při počítání modulo p můžeme v praxi vynechat symboly pro třídy a pracovat pouze s čísly $0, 1, \dots, p-1$ (s tzv. *úplnou soustavou zbytků modulo* p), s tím, že výsledek každé operace nahradíme příslušným zbytkem. Například při počítání modulo 5 bychom tak mohli psát třeba $3 \oplus 4 = 2$ nebo $4 \otimes 3 = 2$. Úplnou informaci o aritmetice modulo 5 podává tabulka 1.

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabulka 1: Aritmetika nad $\mathbf{Z}_5$.

Cvičení 2.2 Napište podobné tabulky pro aritmetiku modulo 2.

Věta 2.3 *Pro libovolné* $p \geq 1$*:*

(a) dvojice ($\mathbf{Z}_p$,$\oplus$) *je komutativní grupa,*

(b) operace $\otimes$ *na* $\mathbf{Z}_p \setminus \{0\}$ *je komutativní, asociativní a má neutrální prvek,*

(c) operace $\oplus$ *na* $\mathbf{Z}_p$ *je distributivní vzhledem k operaci* $\otimes$*, tj.*

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

pro libovolné $a, b, c \in \mathbf{Z}_p$.

Důkaz. Věta snadno plyne z vlastností aritmetických operací na celých číslech. V části (a) je například operace $\oplus$ komutativní, protože

$$[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a] .$$

Podobně dostaneme asociativitu. Třída [0] je zjevně neutrální vzhledem ke sčítání. Inverzní prvek ke třídě $[a]$ je třída $[-a]$.

Část (b) se dokazuje zcela podobně. Část (c) je opět důsledkem distributivity na celých číslech, protože platí

$$\begin{aligned}[a] \otimes \Big([b] \oplus [c]\Big) &= [a] \otimes [b+c] = [a(b+c)] = [ab+ac] = [ab] \oplus [ac] \\ &= \Big([a] \otimes [b]\Big) \oplus \Big([a] \otimes [c]\Big).\end{aligned}$$

□

Je $\mathbf{Z}_p$ spolu s operacemi $\oplus$ a $\otimes$ tělesem? Podle Věty 2.3 k tomu mnoho nechybí: vlastně pouze to, aby ke každé nenulové třídě existoval inverzní prvek vzhledem k násobení. Pak by totiž i $(\mathbf{Z}_p, \otimes)$ byla abelovská grupa. Ptáme se tedy, kdy ke třídě $[x] \in \mathbf{Z}_p$ existuje inverzní prvek vzhledem k násobení. Asi tomu tak nebude vždy; například pro $p = 4$ nenajdeme inverzní prvek ke třídě $[2]_4$. Máme totiž $[2] \otimes [1] = [2]$, $[2] \otimes [2] = [0]$ a $[2] \otimes [3] = [2]$. Na druhou stranu například $\mathbf{Z}_5$ tělesem je, jak se lze přesvědčit z výše uvedené tabulky operace $\otimes$. Úplnou odpověď na naši otázku nabízí následující tvrzení.

Tvrzení 2.4 *Ke třídě $[r] \in \mathbf{Z}_p$ existuje inverzní prvek vzhledem k násobení, právě když r a p jsou nesoudělná čísla.*

Důkaz. Implikaci zleva doprava dokážeme sporem. Dejme tomu, že r i p jsou dělitelná číslem $d > 1$, a nechť $[s]$ je inverzní k $[r]$, to jest $[r] \otimes [s] = [1]$. Z definice je $[rs] = [1]$, takže rozdíl $rs - 1$ je dělitelný číslem p, řekněme $rs - 1 = pn$, kde n je celé. Pak ale

$$rs - pn = 1,$$

přičemž levá strana je dělitelná číslem d (které dělí jak r, tak p). Proto musí číslo d dělit i jedničku na pravé straně, takže $d = 1$. Spor.

K důkazu opačné implikace předpokládejme, že čísla r a p jsou nesoudělná. Uvažme p součinů $1 \cdot r$, $2 \cdot r$, …, $p \cdot r$. Tvrdíme, že žádné dva z těchto součinů nejsou kongruentní modulo p, tedy že $ir \not\equiv jr$ pro různé i, j. Představme si, že $ir \equiv jr$ pro nějaké $i \neq j$. Pak p dělí $r(i - j)$, a protože s r je nesoudělné, musí p dělit rozdíl $i - j$. (Tento fakt plyne například z jednoznačnosti rozkladu na prvočísla.) Ovšem rozdíl $i - j$ je v absolutní hodnotě menší než p, takže jedinou možností je $i = j$, což je spor s předpokladem.

V každé zbytkové třídě modulo p tím pádem leží nejvýše jeden součin $i \cdot r$, kde $i = 1, \ldots, p$. Tříd je ale (stejně jako součinů) přesně p, takže dokonce v každé třídě leží právě jeden tento součin. Speciálně pro nějaké i je $ir \in [1]$. Pak ale $[i] \otimes [r] = [ir] = [1]$, čili $[i]$ je hledaný inverzní prvek ke třídě $[r]$. □

Z této věty již snadno plyne charakterizace čísel p, pro něž je $\mathbf{Z}_p$ tělesem. Každé prvočíslo p je nesoudělné s libovolným číslem, které není násobkem p. Na druhou stranu, pokud p není prvočíslo, pak se dá psát jako $p = a \cdot b$ (kde $1 < a, b < p$), a potom a, p jsou soudělná čísla. Shrnuto:

Důsledek 2.5 *Množina $\mathbf{Z}_p$ s operacemi $\oplus$ a $\otimes$ je tělesem, právě když p je prvočíslo.*

Nabízí se ještě další otázka. Víme, že $\mathbf{Z}_p$ je těleso pouze pro prvočíselná p. Existuje těleso o neprvočíselném počtu prvků, řekněme čtyřprvkové?

Cvičení 2.6 Ověřte, že množina $\{0, 1, 2, 3\}$ spolu s operacemi $\star$ a $\circ$, zadanými pomocí následujících tabulek, je tělesem. Ukažte, že tyto operace se liší od sčítání a násobení na množině $\mathbf{Z}_4$.

$\star$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\circ$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Obecně platí věta, kterou nebudeme dokazovat, že n-prvkové těleso existuje právě tehdy, když n je mocnina prvočísla.

Nechť p je prvočíslo. Víme-li, že $\mathbf{Z}_p$ je těleso, nic nám nebrání uvažovat o vektorových prostorech nad tímto tělesem. Podobně jako jedním ze základních příkladů vektorového prostoru nad reálnými čísly je prostor $\mathbf{R}^n$, tvořený n-ticemi reálných čísel, zde jeho roli hraje vektorový prostor

$$\mathbf{Z}_p^n = \{ (a_1 \dots a_n) \mid a_i \in \mathbf{Z}_p \text{ pro každé } i \},$$

přičemž sčítání $+$ a násobení skalárem $\cdot$ jsou definovány 'po složkách':

$$\begin{aligned} (a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 \oplus b_1, \dots, a_n \oplus b_n), \\ c \cdot (a_1, \dots, a_n) &= (c \otimes a_1, \dots, c \otimes a_n), \end{aligned}$$

kde $c \in \mathbf{Z}_p$. Všimněme si, že protože jednotlivé složky vektorů jsou prvky $\mathbf{Z}_p$, sčítáme je pomocí operace $\oplus$ a násobíme pomocí operace $\otimes$.

V dalších částech přednášky se budeme často setkávat se speciálním případem této kontrukce, vektorovým prostorem $\mathbf{Z}_2^n$ nad $\mathbf{Z}_2$, jehož prvky jsou n-tice nul a jedniček.

Cvičení 2.7 Nechť $a, b \in \mathbf{Z}_2^n$. Kdy bude i-tá složka součtu $a + b$ nulová?

Ve vektorových prostorech nad konečnými tělesy lze provádět všechny obvyklé operace jako v reálných vektorových prostorech, například řešit soustavy rovnic. Jako příklad řešme soustavu

$$\begin{aligned} x + 2y + 3z + 4t &= 1 \\ x + y + 2z &= 0 \end{aligned}$$

o 4 neznámých nad tělesem $\mathbf{Z}_5$ (viz tabulka 1). Pro přehlednost vynecháváme třídové závorky a aritmetické operace zapisujeme jako $+$, $\cdot$ (a nikoli $\oplus, \otimes$).

Standardním postupem vytvoříme matici a převedeme ji do kanonického tvaru:

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 1 & 1 & 2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 0 & 4 & 4 & 1 & 4 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 0 & 1 & 1 & 4 & 1 \end{array}\right)$$
$$\sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 4 \\ 0 & 1 & 1 & 4 & 1 \end{array}\right),$$

přičemž provedené úpravy jsou (po řadě): přičtení čtyřnásobku prvního řádku k druhému, vynásobení druhého řádku 'číslem' 4, a přičtení trojnásobku druhého řádku k prvnímu. Zjišťujeme, že řešení této soustavy mají tvar

$$\{\, (4 + 4z + 4w, 1 + 4z + w, z, w) \mid z, w \in \mathbf{Z}_5 \,\}.$$

Cvičení 2.8 Kolik těchto řešení je?