Tělesa, pole. Termín ***těleso*** označuje strukturu se dvěma binárními operacemi, sčítáním a násobením, kde pro sčítání platí čtyři známé axiomy (asociativita, komutativita, existence nulového prvku a existence opačných prvků). Pro násobení platí tři axiomy (asociativita, existence jednotkového prvku a existence inverzních prvků ke všem **nenulovým** prvkům). Obě operace musí být „svázány" dvěma distributivními zákony („roznásobování závorky" zprava a zleva). Tělesa mohou být **komutativní** (přibude komutativita násobení a vynechá se jeden z distributivních zákonů, neboť je zbytečný), nebo **nekomutativní**. Komutativní tělesa se také nazývají ***pole***. V učebnici LA je úmluva 7.1, že budeme užívat kvůli stručnosti termín *těleso* pro *komutativní těleso*. Přiznávám, že jsem při psaní učebnice byl pod vlivem pražské algebraické školy (prof. V. Kořínek, proslulý značně kuriózními historkami), která termín *pole* neužívala. V posledních letech jsem již na přednáškách užíval termín pole.

Aby to nebylo tak jednoduché, vyšetřují se i *neasociativní tělesa*, v nichž násobení není asociativní (např. tzv. *oktávy*, osmisložková čísla, jisté zobecnění *kvaternionů*), tj. vynechá se příslušný axióm.

Zatím můžete víceméně pustit z hlavy neasociativní i nekomutativní tělesa. V LA potřebujeme pouze komutativní tělesa, tj. pole.

Požadavek, aby těleso mělo alespoň dva prvky, je trochu formální, příliš na něm nezáleží. Prostě nechceme, aby se jednotkový prvek rovnal nulovému. Struktura, která má jen jeden prvek, k ničemu není.

* * * * *

Okruhy. Definice okruhu obsahuje **méně** axiomů než definice tělesa, tudíž jí vyhovuje **více objektů**. Pro sčítání se axiomy okruhu a tělesa shodují, rozdíly jsou v násobení. Obvyklá definice okruhu požaduje asociativní násobení a oba distributivní zákony, které svazují operaci násobení s operací sčítání. Přidáme-li axiom komutativity pro násobení, máme *komutativní okruhy*, přidáme-li axiom jednotkového prvku, máme *okruhy s jednotkovým prvkem*, přidáme-li oba tyto axiomy, máme *komutativní okruhy s jednotkovým prvkem*. Přidáme-li ještě požadavek neexistence netriviálních dělitelů nuly, dostaneme definici *oboru integrity*. Obor integrity je tedy komutativní okruh s jednotkovým prvkem, v němž nejsou netriviální dělitelé nuly. V oboru integrity však nelze dělit, neboť v něm neexistují inverzní prvky ke všem nenulovým prvkům.

Někdy se též vyšetřují *neasociativní okruhy*, v nichž násobení není asociativní. V tomto případě je situace zdůrazněna názvem: ***neasociativní okruhy***.

Příklady. V tomto okamžiku je dobré uvést příklady:

Neasociativní a nekomutativní těleso: *oktávy* (Ty nás nemusí z hlediska LA zajímat.)

Nekomutativní těleso: *kvaterniony* (O těch asi něco málo uslyšíte v Základech ar. a alg.)

Komutativní těleso (= **pole**): *racionální čísla*; *reálná čísla*; *komplexní čísla*; všechna Z_p, kde p je prvočíslo (Pro LA nám tyto příklady bohatě stačí).

Obory integrity: všechna pole; *celá čísla*; *Gaussova celá čísla*; polynomy nad polem.

Komutativní okruhy s jednotkovým prvkem: všechna pole; všechny obory integrity; všechna Z_n, kde n je přirozené číslo.

Komutativní okruh bez jednotkového prvku: sudá celá čísla, celá čísla dělitelná třemi (nebo čtyřmi, pěti, …), značíme je obvykle 2Z, 3Z, 4Z, 5Z, …

Nekomutativní okruhy s jednotkovým prvkem: čtvercové matice téhož řádu (alespoň druhého), jejichž prvky jsou z nějakého pole.

Netriviální dělitelé nuly. *Netriviálními děliteli nuly* se rozumí **nenulové** prvky a, b, jejichž součin je nulový prvek:

$$a \bullet b = 0$$

V tělese nemohou netriviální dělitelé nuly existovat. Dokážeme to. Předpokládejme, že a, b, jsou nenulové prvky tělesa a že $a \bullet b = 0$. K nenulovému prvku a existuje v tělese inverzní prvek a^{-1}, kterým můžeme vynásobit obě strany:

Levá strana: $a^{-1} \bullet (a \bullet b) = (a^{-1} \bullet a) \bullet b = 1 \bullet b = b$

Pravá strana: $a^{-1} \bullet 0 = 0$

Pravá strana se rovná levé: $b = 0$

Prvek b však byl nenulový.

To je spor. Pro nenulové prvky a, b, tedy nemůže být $a \bullet b = 0$.

* * * * *

Parciální operace. **Okruh čtvercových matic**. Vzhledem k tomu, že nelze sčítat ani násobit **libovolné** dvě matice, hovoří se někdy o tom, že jsou tyto dvě binární operace *parciální*. Aby bylo možno sčítání matic chápat jako klasickou binární operaci (neparciální), nesmíme uvažovat **všechny** matice, ale musíme jejich „množství“ **omezit**. Omezíme-li se pouze na matice stejného typu, je na této množině sčítání normální binární operací. Omezíme-li se pouze na čtvercové matice stejného řádu, je na této množině násobení normální binární operací. Uvažujeme-li tedy množinu všech čtvercových matic stejného řádu nad komutativním tělesem (tj. polem) T, značíme ji obvykle $T^{n \times n}$, je tato množina se sčítáním a násobením *okruhem s jednotkovým prvkem* (jednotková matice E). Pokud uvažujeme matice alespoň **druhého řádu**, je tento okruh **nekomutativní**. K některým maticím (nazývají se *invertibilní*) existují inverzní matice, k jiným neexistují.

Ad příklad 4.13 (i). Prověření toho, že jedna matice je inverzní ke druhé, je snadné. Stačí ty dvě matice vynásobit. Zjistíme, že vyjde jednotková matice E.

Symetrické a antisymetrické matice. (Zdůrazněme, že se jedná pouze o čtvercové matice.) *Symetrické* matice jsou „souměrné přes hlavní diagonálu“, pro *antisymetrické* je tato symetrie „poškozená minusem“. Exaktně řečeno, matice $A = (a_{ij})$ je symetrická, je-li $a_{ij} = a_{ji}$, resp. antisymetrická, je-li $a_{ij} = -a_{ji}$. Jedná-li se o matice nad polem, které **nemá** charakteristiku 2, je nulová matice jedinou maticí, která je současně symetrická i antisymetrická. Pro matice nad polem charakteristiky 2 to **neplatí**! Například matice sestavená ze samých jedniček je současně symetrická i antisymetrická, neboť v poli charakteristiky 2 je $1 + 1 = 0$ (jednotkový prvek je opačný sám k sobě), tj. $1 = -1$.

Antisymetrické matice nad polem, **které nemá charakteristiku 2**, má na hlavní diagonále nulové prvky. Pro prvky na diagonále antisymetrické matice (mají stejný řádkový a sloupcový index) je totiž $a_{ii} = -a_{ii}$, neboli $2a_{ii} = 0$, odtud $a_{ii} = 0$. Poslední krok nelze udělat, má-li pole charakteristiku 2, neboť $2 = 0$ a a_{ii} může být jakékoli.

Bloková matice. Blokovou maticí rozumíme matici, kterou podle svého uvážení rozdělíme vodorovnými a svislými čarami na tzv. *podmatice* (*submatice*, *bloky*, *dílčí matice*). Tento pojem využijeme např. v partii o determinantech.

Hadamardův a Kroneckerův součin. V LA tyto dva součiny matic nepoužijeme. Hadamardův součin je velmi jednoduchý, násobení se provádí po složkách, násobí se matice stejného typu. Získáme tak pěkný příklad komutativního okruhu s jednotkovým prvkem (uvažujeme-li matice nad polem). Nechť A a B jsou dvě matice. Jejich Kroneckerův součin si představíme tak, že matici B vynásobíme jednotlivými prvky matice A a výsledné matice sestavíme do „velké“ matice.