Ondrej Vršanský

Materiál na štátnicu

Algebra

Verzia 1

26.IX.1997

Obsah.

2. Algebra.

2.1. Základy.

2.1.1. Základné pojmy z teórie množín.

2.1.2. Grupy a polia.

Definícia.
Usporiadanú dvojicu $(A, \oplus)$ nazývame *grupa*, ak
- $\oplus$ je binárna asociatívna operácia na A
- A je neprázdna
- $\oplus$ má neutrálny prvok e.
- $\forall x \in A\ \exists y \in A > x \oplus y = y \oplus x = e$.

Príklad.
$(Z, +)$ je grupa, $(Q^+, *)$ je grupa, $(P_{1..n}, \circ)$ je grupa.

Definícia.
Usporiadanú trojicu $(A, \oplus, \otimes)$ nazývame *okruh*, ak
- $(A, \oplus)$ je komutatívna grupa
- $\otimes$ je binárna asociatívna operácia na A
- $\otimes$ je distributívna vzhľadom na $\oplus$.

Definícia.
Neutrálny prvok operácie $\otimes$ okruhu $(A, \oplus, \otimes)$ nazývame *jednotka* okruhu $(A, \oplus, \otimes)$.

Príklad.
$(Z, +, *)$ je komutatívny okruh s jednotkou. $(2Z, +, *)$ je komutatívny okruh bez jednotky.

Definícia.
Okruh $(A, \oplus, \otimes)$ nazývame *obor integrity*, ak $\forall a,b \in A : a \neq 0 \wedge b \neq 0 \Rightarrow a \otimes b \neq 0$.

Definícia.
Obor integrity s jednotkou nazývame *teleso*.

Príklad.
$(Q, +, *)$ je teleso.

Definícia.
Teleso $(A, \oplus, \otimes)$, kde $\otimes$ je komutatívna operácia, nazývame *pole*.

Veta 2.1.2.1.
Z_n je pole práve vtedy, keď n je prvočíslo.

Dôkaz.
Stačí dokázať, že Z_n je obor integrity práve vtedy, keď n je prvočíslo. Spätná implikácia je zrejmá; ak n je prvočíslo, tak nemá iných deliteľov, než jednotku, takže $\forall x,y \neq 0 : x \otimes y \neq n$ (=0 v Z_n). Ak ale n nie je prvočíslo, tak $\exists a,b \in A : a \neq 0 \wedge b \neq 0 \wedge a \otimes b = n = 0$.

2.2. Vektorové priestory.

2.2.1. Vektorové priestory a podpriestory.

Definícia.
Usporiadanú trojicu $(V, \oplus, \varphi)$ nazývame *vektorový priestor* nad poľom F, ak
- $(V, \oplus)$ je komutatívna grupa
- $\varphi : V \times F \rightarrow V$ je taká funkcia, že $\forall \alpha,\beta \in F\ \forall x,y \in V$ platí
  - $\alpha(x \oplus y) = \alpha x \oplus \alpha y$
  - $(\alpha+\beta)x = \alpha x \oplus \beta x$
  - $\alpha(\beta(x)) = (\alpha\beta)x$

- $1.x = x$.

Lema 2.2.1.1.

$\forall \alpha \in F$: ak 0 je neutrálny prvok operácie $\oplus$ vektorového priestoru V, potom

- $\alpha.0 = 0$
- $\alpha(-x) = -(\alpha x)$

Dôkaz.

- $\alpha.0 = \alpha(0 \oplus 0) = \alpha.0 + \alpha.0 \Rightarrow 0 = \alpha.0$.
- $0 = \alpha.0 = \alpha(x \oplus (-x)) = \alpha x \oplus \alpha(-x) \Rightarrow \alpha(-x) = -(\alpha x)$.

Definícia.

Vektorový priestor $(W, \oplus, \psi)$ nazývame *podpriestor* vektorového priestoru $(V, +, \varphi)$, ak

- $W \subseteq V$
- $\forall x, y \in W : x \oplus y = x + y$
- $\forall x \in W \ \forall \alpha \in F : \psi(\alpha, x) = \varphi(\alpha, x)$.

Veta 2.2.1.1.

Neprázdna $W \subseteq V$ je podpriestor V práve vtedy, keď

- $x, y \in W : (x - y) \in W$
- $\forall x \in W \ \forall \alpha \in F : \alpha x \in W$.

Dôkaz.

Dopredná implikácia je triviálna. Obrátene nech W má požadované vlastnosti. $W \neq \emptyset$, takže $\exists x \in W$. Ale potom aj $\}x - x| \in W \Rightarrow 0 \in W$. Rovnako $(0 - x) \in W \Rightarrow -x \in W$ a teda $\forall y \in W$ aj $(x - (-y)) = (x + y) \in W$.

Veta 2.2.1.2.

Nech W, W' súpodpriestory V. Potom aj

- $W \cap W'$ je podpriestor V
- $W + W' = \{x+y;\ x \in W \text{ a } y \in W'\}$ je podpriestor V.

Dôkaz.

- $(x - y) \in W \wedge (x - y) \in W' \Rightarrow (x - y) \in W \cap W'$. Takiso αx.
- Nech $x, y \in W$ a $x', y' \in W'$. Potom $(x+x') + (y+y') = (x+y) \in W + (x'+y') \in W' \Rightarrow (x+y)+(x'+y') \in W+W'$.

2.2.2. Lineárna závislosť a nezávislosť vektorov.

Definícia.

Vektor $x \in V$ nazývame *lineárna kombinácia* vektorov $x_1..x_n \in V$, ak $\exists \alpha_1..\alpha_n : x = \alpha_1 x_1 + .. + \alpha_n x_n$.

Veta 2.2.2.1.

Ak $x_1..x_n \in V$, tak $[x_1..x_n] = \{x \in V;\ x \text{ je lineárna kombinácia } x_1..x_n\}$ je podpriestor V.

Dôkaz.

$\forall x = (\alpha_1 x_1 + .. + \alpha_n x_n),\ y = (\beta_1 x_1 + .. + \beta_n x_n) \in [x_1..x_n] : (x - y) = (\alpha_1 - \beta_1)x_1 + .. + (\alpha_n - \beta_n)x_n$. Podobne $\forall \alpha \in F : \alpha x = \alpha\alpha_1 x_1 + .. + \alpha\alpha_n x_n$.

Definícia.

$[x_1..x_n]$ nazývame *podpriestor generovaný* vektormi $x_1..x_n$.

Definícia.

Vektory $x_1..x_n$ nazývame *lineárne závislé*, ak $\exists i : x_i$ je lineárna kombinácia ostatných.

Veta 2.2.2.2.

Vektory $x_1..x_n$ sú lineárne závislé práve vtedy, keď $\exists \alpha_1..\alpha_n \neq 0 : \Sigma \alpha_i x_i = 0$.

Dôkaz.

Ak $x_1..x_n$ sú lineárne závislé, tak $\exists i : x_i$ je lineárna kombinácia ostatných. Nech je to x_n a nech $x_n = \alpha_1 x_1 + .. + \alpha_{n-1} x_{n-1}$. Potom ale pre $\alpha_n = -1$ platí $\Sigma \alpha_i x_i = x_n - x_n = 0$. Obrátene ak $\exists \alpha_1..\alpha_n \neq 0 : \Sigma \alpha_i x_i = 0$, potom $x_n = \sum_{i=1}^{n-1} \frac{\alpha_i}{\alpha_n} x_i \Rightarrow x_1..x_n$ sú lineárne závislé.

Definícia.
Vektory $x_1..x_n$ sú *lineárne* nezávislé, ak nie sú lineárne závislé.

Veta 2.2.2.3.
Vektory $x_1..x_n$ sú lineárne závislé práve vtedy, keď $\exists i : x_i$ je lineárna kombinácia predchádzajúcich.

Dôkaz.
Spätná implikácia je triviálna. Teraz ak $x_1..x_n$ sú lineárne závislé, tak vezmeme max$\{i; \alpha_i \neq 0\}$, ktoré spĺňa požiadavok zadania.

Veta 2.2.2.4.
Ak x je lineárna kombinácia $x_1..x_n$, tak $[x_1..x_n] = [x, x_1..x_n]$.

Dôkaz.
Je zrejmé, že $[x_1..x_n] \subseteq [x, x_1..x_n]$. Nech $x = \Sigma\alpha_i x_i$ a $v = \beta x + \Sigma\beta_i x_i$. Ak označíme $\gamma_i = \alpha_i + \beta_i$, potom $v = \Sigma\alpha_i x_i$ a teda $v \in [x_1..x_n]$.

Dôsledok 2.2.2.1.
Každá sústava vektorov $x_1..x_n$ obsahuje nezávislú podsústavu $x_{i1}..x_{im}$ takú, že $[x_1..x_n] = [x_{i1}..x_{im}]$.

Dôkaz.
Postupným odstraňovaním vektorov sústavy $x_1..x_n$ spôsobom popísaným vo vete 2.2.2.4 dosiahneme nezávislú podsústavu, generujúcu ten istý podpriestor.

Veta 2.2.2.5.
Nech $V = [x_1..x_n]$ a nech $y_1..y_m \in V$ sú nezávislé. Potom $n \geq m$.

Dôkaz.
$x_1..x_n$ sú generujúce $\Rightarrow$ $y_1, x_1..x_n$ sú lineárne závislé. Podľa vety 2.2.3.2 pootm existuje x_i ako lineárna kombinácia predchádzajúcich $\Rightarrow$ po jeho odstránení ostáva generujúca sústava. Ale tento postup možno postupne aplikovať na všetky y, pričom zakaždým odstránime jeden x_i (veta 2.2.3.2 nikdy nevyberie jeden z y, lebo tie sú lineárne nezávislé). Aby toto bolo možné, musí vyť $n \geq m$.

2.2.3. Báza vektorového priestoru.

Definícia.
Nezávislú sústavu vektorov $x_1..x_n \in V$ nazývame *báza* vektorového priestoru V, ak $[x_1..x_n] = V$.

Veta 2.2.3.1.
Všetky bázy vektorového priestoru V majú rovnaký počet vektorov.

Dôkaz.
Tvrdenie je triviálnym dôsledkom vety 2.2.2.5.

Definícia.
Počet vektorov báz vektorového priestoru V sa nazýva *dimenzia* V a označuje $dim(V)$.

Veta 2.2.3.2.
Ak $dim(V) = n$, tak každých $n+1$ vektorov z V je lineárne závislých.

Dôkaz.
Tvrdenie vyplýva priamo z tvrdenia 2.2.2.5.

Veta 2.2.3.3.
Každý vektor $x \in V$ možno zapísať jediným spôsobom ako lineárnu kombináciu bázy $x_1..x_n$.

Dôkaz.
Je zrejmé, že každý vektor $x \in V$ možno zapísať ako lineárnu kombináciu bázy $x_1..x_n$. Nech existujú dva rôzne zápisy $x = \Sigma\alpha_i x_i = \Sigma\beta_i x_i$ (teda $\exists i : \alpha_i \neq \beta_i$). Ale $x - x = \Sigma\alpha_i x_i - \Sigma\beta_i x_i = \Sigma(\alpha_i - \beta_i)x_i = 0$ a keďže $x_1..x_n$ sú lineárne nezávislé, $\forall i=1..n : (\alpha_i - \beta_i) = 0 \Rightarrow \alpha_i = \beta_i$.

2.2.4. Lineárne zobrazenia.

Definícia.

Funkciu $f : V \to V'$ nazveme *lineárne zobrazenie* z vektorového priestoru V do vektorového priestoru V', ak

- $\forall x,y \in V : f(x+y) = f(x) + f(y)$
- $\forall x \in V\ \forall \alpha \in F : f(\alpha x) = \alpha.f(x)$.

Veta 2.2.4.1.

f je lineárne zobrazenie práve vtedy, keď $F(0) = 0$ a $\forall x,y \in V\ \forall \alpha,\beta \in F : f(\alpha x + \beta y) = \alpha.f(x) + \beta.f(y)$.

Dôkaz.

Triviálne.

Definícia.

Lineárne zobrazenie f nazývame *izomorfizmus*, ak f je bijekcia.

Veta 2.2.4.2.

$\forall V : V$ a $F^{dim(V)}$ sú izomorfné.

Dôkaz.

Pre daný V dimenzie n skonštruujeme izomorfizmus $f : V \to F^n$. Pre $x = x_1..x_n$ položíme $f(x) = y = f(x_1) + .. + f(x_n)$. To je zobrazenie, pretože vyjadrenie všetkých $f(x_i)$ je podľa vety 2.2.3.3 jediné. Navyše $f^{-1}(y) = \Sigma f^{-1}(f(x_i)) = \Sigma x_i = x$, takže f je izomorfizmus.

Veta 2.2.4.3 (Základná veta o lineárnych zobrazeniach).

Nech $x_1..x_n$ je báza vo V a $y_1..y_n$ je báza vo W. Potom existuje jediné lineárne zobrazenie $f : V \to W$ také, že $i=1..n : f(x_i) = y_i$.

Dôkaz.

Najprv dokážeme, že také zobrazenie existuje nejviac jedno. Nech f a g sú zobrazenia s požadovanými vlastnosťami. Potom $\forall x = \alpha_1x_1..\alpha_nx_n : f(x) = f(\alpha_1x_1..\alpha_nx_n) = \Sigma f(\alpha_ix_i) = \Sigma\alpha_i.f(x_i) = \Sigma\alpha_i.g(x_i) = \Sigma g(\alpha_ix_i) = f(\alpha_1x_1..\alpha_nx_n) = f(x) \Rightarrow f = g$.

Existencia lineárneho zobrazenia s požadovanými vlastnosťami vyplýva z toho, že funkcia f, kde $\forall x = \alpha_1x_1..\alpha_nx_n : f(x) = \alpha_1y_1..\alpha_ny_n$ je lineárne zobrazenie.

Definícia.

Nech $f : V \to W$ je lineárne zobrazenie. Potom funkciu $Ker(f) = \{x \in V; f(x) = 0\}$ nazývame *jadro* (Kernel) zobrazenia f.

Veta 2.2.4.4.

Jadro každého lineárneho zobrazenia $f : V \to W$ je podpriestor V. Navyše f je injekcia práve vtedy, keď $Kef(f) = \emptyset$.

Dôkaz.

$\forall x,y \in V : f(x - y) = f(x) - f(y) = 0 - 0 = 0$. Rovnako $\forall x \in V\ \forall \alpha \in F : f(\alpha x) = \alpha.f(x) = \alpha.0 = 0$. Časť navyše je triviálna.

Definícia.

Nech $f : V \to W$ je lineárne zobrazenie. Potom funkciu $Im(f) = \{f(x) \in W; x \in V\}$ nazývame *obraz* (Image) zobrazenia f.

Veta 2.2.4.5.

Obraz každého lineárneho zobrazenia $f : V \to W$ je podpriestor W.

Dôkaz.

$\forall f(x), f(y) \in W : x,y \in V$. Ale $\forall \alpha,\beta \in F : \alpha.f(x) + \beta.f(y) = f(\alpha x + \beta y)$, pričom $\alpha x + \beta y \in V$.

2.3. Matice.

2.3.1. Pojem matice.

Definícia.

Zobrazenie $\{1..n\} \times \{1..m\} \to F$ nazývame *matica* dimenzie $n \times m$ nad poľom F.

2.3.2. Vyjadrenie lineárnych zobrazení pomocou matíc.

Definícia.

Nech $x_1..x_n$ je báza vo V, $y_1..y_m$ báza vo W a $f : V \to W$ je lineárne zobrazenie. Nech $\forall i \in 1..n : f(x_i) = \sum_{j=1}^{m} \alpha_{ij} y_j$. Potom maticu $M_f = \begin{pmatrix} \alpha_{11} & \Lambda & \alpha_{n1} \\ M & \alpha_{ij} & M \\ \alpha_{1m} & \Lambda & \alpha_{nm} \end{pmatrix}$ nazývame *maticou zobrazenia f*.

Veta 2.3.2.1.

Nech f a g sú lineárne zobrazenia. Potom aj $f+g$ je lineárne zobrazenie a $M_{f+g} = M_f + M_g$.

Dôkaz.

Triviálne.

Veta 2.3.2.2.

Nech f je lineárne zobrazenia. Potom $\forall \alpha \in F$ aj $\alpha.f$ je lineárne zobrazenie a $M_{\alpha f} = \alpha.M_f$.

Dôkaz.

Triviálne.

Veta 2.3.2.3.

Nech $f : V \to V'$ a $g : V' \to W$ sú lineárne zobrazenia. Potom aj $g \circ f$ je lineárne zobrazenie a $M_{g \circ f} = M_f \times M_g$.

Dôkaz.

$\forall \alpha,\beta \in F : g \circ f(\alpha x + \beta y) = g(f(\alpha x + \beta y)) = g(\alpha.f(x) + \beta.f(y)) = \alpha.g \circ f(x) + \beta.g \circ f(y)$. Pritom ak $M_f\ (i,j)$ označíme $\alpha_{i,j}$ a $M_g\ (i,j) = \beta_{i,j}$, tak $\forall i \in 1..n\ \forall j \in 1..m : M_{g \circ f}(i,j) = \alpha_{1i}\beta_{j1} + .. + \alpha_{ni}\beta_{jm} = g \circ f(x_i)$.

Veta 2.3.2.4.

Ak $f : V \to W$ je bijektívne lineárne zobrazenie, tak aj $f^{-1} : W \to V$ je lineárne zobrazenie.

Dôkaz.

$\forall u,v \in W\ \forall \alpha,\beta \in F : f^{-1}(\alpha u + \beta v) = f^{-1}(\alpha.id(u) + \beta.id(v)) = f^{-1}(\alpha.(f \circ f^{-1})(u) + \beta.(f \circ f^{-1})(v)) = f^{-1}(f(\alpha.f^{-1}(u)) + f(\beta.f^{-1}(v))) = f^{-1}(f(\alpha.f^{-1}(u) + \beta.f^{-1}(v))) = id(\alpha.f^{-1}(u) + \beta.f^{-1}(v)) = \alpha.f^{-1}(u) + \beta.f^{-1}(v)$.

2.3.3. Riadková ekvivalencia matíc.

Definícia.

Medzi *elementárne operácie* na maticiach patrí

- Vzájomná výmena dvoch riadkov (stĺpcov)
- Vynásobenie riadku (stĺpca) skalárnou konštantou
- Pričítanie násobku jedného riadku k inému.

Definícia.

Matica M sa nazýva *redukovaná*, ak

- Vedúci prvok každého nenulového riadku je 1
- V každom riadku je najviac jedna nenulová hodnota.

Definícia.

Matice M_1 a M_2 sú *riadkovo ekvivalentné*, ak možno upraviť jednu na druhú pomocou elementárnych riadkových úprav.

Veta 2.3.3.1.

Každá matica je riadkovo ekvivalentná s nejakou redukovanou maticou zhodnej dimenzie.

Dôkaz.

Klasický postup redukcie matice.

Definícia.

Hovoríme, že redukovaná matica A je *trojuholníková*, ak každý nenulový riadok je nad každým nulovým a postupnosť indexov vedúcich prvkov nenulových riadkov je neklesajúca.

Veta 2.3.3.2.

Každá matica je riadkovo ekvivalentná s nejakou redukovanou trojuholníkovou maticou zhodnej dimenzie.

Dôkaz.
Triviálne.

Veta 2.3.3.3.
Nenulové riadky trojuholníkovej redukovanej matice sú lineárne nezávislé.

Dôkaz.
Triviálne.

Dôsledok 2.3.3.1.
Nenulové riadky trojuholníkovej redukovanej matice tvoria bázu jej riadkového priestoru.

Dôkaz.
Tvrdenie vyplýva z vety 2.3.3.3 a faktu, že nenulové riadky trojuholníkovej redukovanej matice jej riadkový priestor generujú.

Definícia.
Hodnosť matice je dimenzia jej riadkového pristoru.

Dôsledok 2.3.3.2.
Hodnosť trojuholníkovej redukovanej matice je počet jej nenulových riadkov.

Dôkaz.
Tvrdenie vyplýva priamo z definície hodnosti a dôsledku 2.3.3.1.

Veta 2.3.3.4.
Štvorcová matica dimenzie $n\times n$ má hodnosť n práve vtedy, keď je riadkovo ekvivalentná s jednotkovou maticou rádu n.

Dôkaz.
Jediná trojuholníková redukovaná matica dimenzie $n\times n$ je jednotková matica rádu n, takže Štvorcová matica dimenzie $n\times n$ má hodnosť n práve vtedy, keď je riadkovo ekvivalentná s ňou.

Veta 2.3.3.5.
Každému podpriestoru F^n prislúcha práve jedna trojuholníková redukovaná matica dimenzie $n\times n$ nad poľom F.

Dôkaz.
Nedokazujeme.

2.3.4. Regulárne matice.

Definícia.
Matica $A_{n\times n}$ je *regulárna*, ak existuje matica $B_{n\times n}$ taká, že $A\times B = B\times A = I_n$.

Veta 2.3.4.1.
Ak $\mathbf{R}_n$ je množina regulárnych matíc rádu n, tak $(\mathbf{R}_n, \times)$ je grupa.

Dôkaz.
$\mathbf{R}_n$ je neprázdna, pretože I_n regulárna. Zároveň je I_n neutrálnym prvkom a inverzný prvok ku každej matici existuje z definície regulárnosti.

Veta 2.3.4.2.
Ak postupnosť elementárnych riadkových operácií, ktorými regulárnu maticu A upravíme na I_n, uplatníme na I_n, výsledkom bude regulárna matica $A´$ inverzná k A.

Dôkaz.
Nech E_1 .. E_k sú regulárne matice, reprezentujúce elementárne riadkové operácie. Ak $E_k\times..\times E_1\times A = I_n$, potom $E_k\times..\times E_1 = A´$.

Veta 2.3.4.3.
Matica $A_{n\times n}$ je regulárna, ak jej prislúchajúce zobrazenie je bijekcia. Naviac ak B je množina všetkých lineárnych bijekcií $f : V\to V$, tak $(B, \circ)$ je grupa.

Dôkaz.
Ak f_A je bijekcia, tak k nemu existuje inverné zobrazenie f_B a jeho matica B je inverzná k A ($A\times B = I_n$ práve tak ako $f_A\circ f_B = id$). $(B, \circ)$ je grupa, pretože $(\mathbf{R}_n, \times)$ je grupa (podľa vety 2.3.4.1).

Definícia.

Nech $x_1..x_n$ je báza vo V a $y_1..y_n$ vo V'. Nech $f : V \to V'$ je také zobrazenie, že súradnice vektora $f(x_i)$ vo V' sú $\alpha_{i1}..\alpha_{in}$. Maticu M, ktorej prvky $M(i,j) = \alpha_{ij}$, nazývame *matica zobrazenia f*. Ak $V = V'$, M je *matica prechodu* od bázy $x_1..x_n$ k báze $y_1..y_n$.

Poznámka.

Matice dimenzie $n \times m$ tvoria vektorový priestor dimenzie $m.n$, ktorého bázou sú elementárne matice E_{ij}.

2.3.5. Ekvivalentné matice.

Definícia.

Hovoríme, že matice A a B sú *ekvivalentné*, ak existujú také regulárne matice P a Q, že $B = P \times A \times Q^{-1}$.

Veta 2.3.5.1.

Ekvivalencia matíc je reláciou ekvivalencie.

Dôkaz.

- $\forall A_{m \times n} : A = I_n \times A \times I_m^{-1}$.
- $B = P \times A \times Q^{-1} \Rightarrow A = P^{-1} \times B \times Q = (P^{-1}) \times B \times (Q^{-1})^{-1}$
- $B = P \times A \times Q^{-1} \wedge C = R \times B \times T^{-1} \Rightarrow C = R \times P \times A \times Q^{-1} \times T^{-1}$

Veta 2.3.5.2.

A a B sú ekvivalentné práve vtedy, keď sú maticami rovnakého lineárneho zobrazenia vzhľadom na rôzne dvojice báz.

Dôkaz.

nech A a B sú ekvivalentné. Potom existujú regulárne P a Q aké, že $B = P \times A \times Q^{-1}$. Ak si uvedomíme, že P a Q možno chápať ako matice prechodu báz, tvrdenie je zrejmé.

Veta 2.3.5.3.

Matice A a B sú ekvivalentné práve vtedy, keď jednu možno na druhú upraviť elementárnymi riadkovými a stĺpcovými úpravami.

Dôkaz.

Spätná implikácia je triviálna a ak $B = P \times A \times Q^{-1}$, tak P a Q možno rozobrať na súčin elementárnych matíc.

2.3.6. Sústavy lineárnych rovníc.

Definícia.

$$\text{Sústavu lineárnych rovníc} \quad \begin{matrix} \alpha_{11}x_1 + & \Lambda & + \alpha_{1n}x_n = b_1 \\ \text{M} & \text{O} & \text{M} \\ \alpha_{m1}x_1 + & \Lambda & \alpha_{mn}x_n = b_m \end{matrix} \quad \text{(typ (1))}$$

reprezentujeme maticou $\begin{pmatrix} \alpha_{11} & \Lambda & \alpha_{1n} & b_1 \\ \text{M} & \text{O} & \text{M} & \text{M} \\ \alpha_{m1} & \Lambda & \alpha_{mn} & b_m \end{pmatrix}$, ktorú nazývame *rozšírená matica* sústavy.

Definícia.

$$\text{Sústava lineárnych rovníc} \quad \begin{matrix} \alpha_{11}x_1 + & \Lambda & + \alpha_{1n}x_n = b_1 \\ \text{M} & \text{O} & \text{M} \\ \alpha_{m1}x_1 + & \Lambda & \alpha_{mn}x_n = b_m \end{matrix} \quad \text{sa nazýva } \textit{homogénna}, \text{ ak } \forall i \in 1..m :$$

$b_i=0$. Pri reprezentácii homogénnej sústavy vynechávame z jej matice posledný stĺpec. Homogénna sústava, ktorej matica sa s maticou sústavy A líši iba chýbajúcim posledným stĺpcom, sa nazýva sústava *adjungovaná* k A.

Definícia.

$x_1..x_n \in F^n$ sa nazýva *koreň* sústavy lineárnych rovníc typu (1), ak $\forall j \in 1..m$: $\sum_{i=1}^{n} \alpha_{ij} x_i = b_j$. Ak dve sústavy majú rovnakú množinu riešení, hovoríme, že sú *ekvivalentné*.

Veta 2.3.6.1 (Frobien).
Sústava typu (1) má riešenie práve vtedy, keď jej matica a rozšírená matica majú rovnakú hodnosť.

Dôkaz.
Zrejmé.

Dôsledok 2.3.6.1.
Každá homogénna sústava má aspoň jeden koreň.

Dôkaz.
Triviálne.

Veta 2.3.6.2.
Množina koreňov homogénnej sústavy je podpriestor F^n.

Dôkaz.

Nech $x_1..x_n$ a $y_1..y_n$ sú korene a $\alpha,\beta\in F^n$. $\forall j\in 1..m : \sum_{i=1}^{n}\alpha_{ij}(\alpha x_i+\beta y_i)=\sum_{i=1}^{n}\alpha_{ij}\alpha x_i+\alpha_{ij}\beta y_i=\alpha\sum_{i=1}^{n}\alpha_{ij}x_i+\beta\sum_{i=1}^{n}\alpha_{ij}y_i=0+0=0.$

Definícia.
B ň ť *fundamentálny systém* tejto sústavy.

Veta 2.3.6.3.
ť r, tak dimenzia jej fundamentálneho systému je n-r a on samotný je tvorený n-rozmernými vektormi $z_{r+1}..z_n$, ktorých jediná jednotka sa postupne nachádza na pozíciách r+1 .. n.

Dôkaz.
Zrejmé.

Definícia.
ň ( ) *partikulárne riešenie*.

Veta 2.3.6.4.
ň ( ) ť fundamentálneho systému.

Dôkaz.
ľ 6 ň F^n ň ľ (ň) ntálnym systémom (pohyb v rámci ň)

2.4. Euklidovské a unitárne priestory.

2.4.1. Euklidovské priestory.

Definícia.
Zobrazenie $\psi : V\times V\to R$ nazvem *skalárny súčin* vo V, ak je symetrické, lineárne a $\forall x\in V : \psi(x, x) \geq 0$ ($\psi(x, x) = 0 \Leftrightarrow x = 0$).

Označenie.
$\psi(x, y)$ ť $\langle x, y\rangle$.

Definícia.
Ak V je vektorový priestor a ψ (V, ψ) nazvem *Euklidovský priestor*.

Definícia.
$\sqrt{\langle x,x\rangle}$ nazvem *norma* (Í) x a zapisujem $||x||$.

Veta 2.4.1.1 (Schwartz).
$\forall x,y\in V : |\langle x, y\rangle| \leq ||x||.||y||$.

Dôkaz.

Nech $x,y\in V$ a $\alpha\in F$. $0 \le \langle x+\alpha y, x+\alpha y\rangle = \|x\|^2 + \alpha\langle x, y\rangle + \alpha\langle y, x\rangle + \alpha^2\|y\|^2 = \|x\|^2 + 2\alpha\langle x, y\rangle + (\alpha\|y\|)^2 \Rightarrow D \le 0 \Rightarrow 4\alpha^2\langle x, y\rangle^2 - 4\alpha\|x\|.\|y\| \le 0 \Rightarrow |\langle x, y\rangle| \le \|x\|.\|y\|$.

Dôsledok 2.4.1.1 (Cauchyho nerovnosť).

$\forall x_1..x_n, y_1..y_n \in R : \left|\sum_{i=1}^{n} x_i y_i\right| \le \sqrt{\sum_{i=1}^{n} x_i^2} \cdot \sqrt{\sum_{i=1}^{n} y_i^2}$.

Dôkaz.

Tvrdenie vyplýva priamo z predchádzajúcej vety.

Lema 2.4.1.1.

- $\forall x\in V : \|x\| \ge 0$
- $\forall x\in V\ \forall\alpha\in F : \|\alpha x\| = |\alpha|.\|x\|$.
- $\forall x,y\in V : \|x+y\| \le \|x\| + \|y\|$ (t')

Dôkaz.

- Zrejmé z definície $\|x\|$.
-
- $\forall x,y\in V\ \forall i\in 1..n : |x_i + y_i| \le |x_i| + |y_i| \Rightarrow \|x+y\| \le \|x\| + \|y\|$.

Definícia.

x a y sú *ortogonálne* (kolmé), ak $\langle x, y\rangle = 0$. $\forall\emptyset\ne M\subseteq V$ nazývame $M^\perp = \{x\in V;\ \forall y\in M : \langle x, y\rangle = 0\}$ *ortogonálny doplnok* M vo V.

Veta 2.4.1.2.

$\forall\emptyset\ne M\subseteq V : M^\perp$ je podpriestor V.

Dôkaz.

Nech $x\in M,\ y,z\in M^\perp$, $\alpha,\beta\in F$. $\langle x, \alpha y + \beta z\rangle = \alpha\langle x, y\rangle + \beta\langle x, z\rangle = 0 + 0 = 0$.

Definícia.

Systém vektorov $x_1..x_n$ je *ortogonálny*, ak $\forall i\ne j\in 1..n : \langle x_i, x_j\rangle = 0$ a *ortonormálny*, ak navyše $\forall i\in 1..n : \|x_i\| = 1$.

Veta 2.4.1.3.

Dôkaz.

Nech $\exists\alpha_1..\alpha_n : \sum_{i=1}^{n}\alpha_i x_i = 0$. $\forall k\in 1..n : 0 = \langle 0, x_k\rangle = \left\langle\sum_{i=1}^{n}\alpha_i x_i, x_k\right\rangle = \sum_{i=1}^{n}\langle\alpha_i x_i, x_k\rangle = \sum_{i=1}^{n}\alpha_i\langle x_i, x_k\rangle = \alpha_k\langle x_k, x_k\rangle$. Ale $\langle x_k, x_k\rangle \ne 0$, takže $\alpha_k = 0$.

Dôsledok 2.4.1.2.

Každá ortonormálna sústava je lineárne nezávislá.

Dôkaz.

Zrejmé.

Veta 2.4.1.4 (Gramm-Schmidtov ortogonalizačný proces).

Nech V je Euklidovský priestor a $x_1..x_n$ je lineárne nezávislá sústava vektorov V. Potom existuje ortonormálna sústava sústava $y_1..y_n$ taká, že $\forall i\in 1..n : [x_1..x_i] = [y_1..y_i]$.

Dôkaz.

Indukciou na n.

1° $n = 1$, $x_1\ne 0$, $y_1 = x_1.\|x_1\|^{-1}$.

2° $x_1..x_{n+1}$, $y_1..y_n$, $\forall i\in 1..n : [x_1..x_i] = [y_1..y_i]$. $x_{n+1} = u + v$, kde $u\in[y_1..y_n]$, $v\notin[y_1..y_n] \Rightarrow u\perp v$. $u\in[y_1..y_n] \Rightarrow \exists\alpha_1..\alpha_n : u = \sum_{i=1}^{n}\alpha_i x_i$. Ak položíme $\alpha_i = \langle x_{n+1}, y_i\rangle$, potom $\forall i\in 1..n : \langle v, y_i\rangle = \langle x_{n+1} - \sum_{j=1}^{n}\alpha_j x_j\ , y_i\rangle = \langle x_{n+1}, y_i\rangle - \langle x_{n+1} -, y_i\rangle = \langle x_{n+1}, y_i\rangle - \langle x_{n+1}, y_i\rangle = 0$ a pre $y_{n+1} = v.\|v\|^{-1}$ platí $[x_1..x_{n+1}] = [y_1..y_{n+1}]$.

Dôsledok 2.4.1.3.

V každom konečnorozmernom euklidovskom priestore existuje ortonormálna báza.

Dôkaz.
Triviálne.

Veta 2.4.1.5.

Nech V je euklidovský priestor, $x_1..x_n$ jeho ortonormálna báza a $x = \sum_{i=1}^{n} \alpha_i x_i$,$y = \sum_{i=1}^{n} \beta_i x_i \in V$. Potom $\langle x,y\rangle = \sum_{i=1}^{n} \alpha_i \beta_i$.

Dôkaz.
$\langle x, y\rangle = \langle \sum_{i=1}^{n} \alpha_i x_i \ , \ \sum_{i=1}^{n} \beta_i x_i \ \rangle = \sum_{i=1,j=1}^{n} \alpha_i \beta_j \langle x_i , y_j \rangle = \sum_{i=1}^{n} \alpha_i \beta_i$.

Veta 2.4.1.6.

Každé dva euklidovské priestory rovnakej dimenzie sú izomorfné.

Dôkaz.
Nech V a $V´$ sú euklidovské priestory dimenzie n, $x_1..x_n$ je ortonormálna báza vo V a $y_1..y_n$ ortonormálna báza vo $V´$. Podľa základnej vety o lineárnych zobrazeniach (veta 2.2.4.3) existuje jediné lineárne zobrazenie f také, že $\forall i \in 1..n : f(x_i) = y_i$. Pritom $\forall x = \sum_{i=1}^{n} \alpha_i x_i \ , y = \sum_{i=1}^{n} \beta_i x_i \in V : \langle f(x), f(y)\rangle = \left\langle \sum_{i=1}^{n} \alpha_i f(x_i), \sum_{i=1}^{n} \beta_i f(x_i) \right\rangle =$ $\left\langle \sum_{i=1}^{n} \alpha_i y_i , \sum_{i=1}^{n} \beta_i y_i \right\rangle = \sum_{i=1}^{n} \alpha_i \beta_i$ = (podľa vety 2.4.1.5) = $\langle x, y\rangle$.

2.4.2. Ortogonálne matice.

Definícia.

Zobrazenie $f : V \to V´$ je *ortogonálne*, ak $\forall x,y \in V : \langle x, y\rangle = \langle f(x), f(y)\rangle$.

Veta 2.4.2.1.

Každé ortogonálne zobrazenie je injektívne.

Dôkaz.
$\langle x, y\rangle = \langle f(x), f(y)\rangle \Rightarrow f(x) = 0 \Leftrightarrow x = 0 \Rightarrow Ker(f) = \{0\}$.

Veta 2.4.2.2.

Ak f je ortogonálne, tak každú ortonormálnu sústavu zobrazí na ortonormálnu.

Dôkaz.
Zrejmé z definície.

Definícia.

Štvorcová matica A sa nazýva *ortogonálna*, ak jej riadky (stĺpce) tvoria ortogonálnu sústavu v R^n. Matica $A^{\perp}$ *transponovaná* k A vznikne zámenou riadky z stĺpce (a naopak).

Veta 2.4.2.3.

$A^{\perp}$ je transponovaná k A práve vtedy, keď $A \times A^{\perp} = I_n$.

Dôkaz.

Ak r_i označíme r-ty riadok A, tak $(A \times A^{\perp})(i,j) = \langle r_i, r_j\rangle = \begin{cases} 0 \leftarrow i \neq j \\ \leftarrow i = j \end{cases}$.

Veta 2.4.2.4.

O ň n tvoria spolu s operáciou násobenia matíc grupu.

Dôkaz.
$(A \times B) \times (A \times B)^{\perp} = A \times B \times B^{\perp} \times A^{\perp} = I_n$.

Definícia.

G ň n nazývame *ortogonálna grupa* ň n a zapisujeme O_n.

2.4.3. Unitárne priestory.

Označenie.

Nech $x \in C$, $x = a + bi$ Č $a - bi$ ť $\overline{x}$.

Definícia.
Nech V je vektorový priestor na C. *Skalárny súčin* vo V $\varphi : V\times V\to C$

- $\forall x,x',y\in V\ \forall\alpha,\beta\in C : \varphi(\alpha x + \beta x', y) = \alpha.\varphi(x, y) + \beta.\varphi(x', y)$
- $\forall x,y\in V : \varphi(x, y) = \overline{\varphi(y,x)}$
- $\forall x\in V : \varphi(x, x) \geq 0\ (\varphi(x, x) = 0 \Leftrightarrow x = 0)$.

Veta 2.4.3.1 (Schwartzova nerovnosť).
Ak V je unitárny priestor, tak $\forall x,y\in V : |\langle x, y\rangle| \leq \|x\|.\|y\|$.

Dôkaz.
$\forall x,y\in V : \langle x, y\rangle = |\langle x, y\rangle|(\cos\varphi + i.\sin\varphi)$. nech $t\in R$ a $x' = t.x + (\cos\varphi + i.\sin\varphi).y$.
$0 \leq \langle x', x'\rangle = \langle t.x + (\cos\varphi + i.\sin\varphi).y, t.x + (\cos\varphi + i.\sin\varphi).y\rangle = \langle tx, tx\rangle + \langle tx, (\cos\varphi + i.\sin\varphi).y\rangle + \langle(\cos\varphi + i.\sin\varphi).y, tx\rangle + \langle(\cos\varphi + i.\sin\varphi).y, (\cos\varphi + i.\sin\varphi).y\rangle = t^2\|x\|^2 + t(\cos\varphi - i.\sin\varphi)\langle x, y\rangle + t(\cos\varphi + i.\sin\varphi)\langle x, y\rangle + (\cos\varphi - i.\sin\varphi)(\cos\varphi + i.\sin\varphi)\|y\|^2 = t^2\|x\|^2 + t(\cos\varphi - i.\sin\varphi)|\langle x, y\rangle|(\cos\varphi + i.\sin\varphi) + t(\cos\varphi + i.\sin\varphi)|\langle x, y\rangle|(\cos\varphi - i.\sin\varphi) + (\cos\varphi - i.\sin\varphi)(\cos\varphi + i.\sin\varphi)\|y\|^2 = t^2\|x\|^2 + 2t|\langle x, y\rangle| + \|x\|^2$. $0 \geq D = 4t^2|\langle x, y\rangle|^2 - 4t^2\|x\|.\|y\| \Rightarrow |\langle x, y\rangle| \leq \|x\|.\|y\|$.

Lema 2.4.2.1.
Nech V je unitárny priestor. Potom
- $\forall x\in V : \|x\| \geq 0\ (\|x\| = 0 \Leftrightarrow x = 0)$
- $\forall x\in V\ \forall\alpha\in R : \|\alpha.x\| = |\alpha|.\|x\|$
- $\forall x,y\in V : \|x + y\| \leq \|x\| + \|y\|$.

Dôkaz.
- Z
- Z
- $\|x + y\|^2 = \langle x+y, x+y\rangle = \|x\|^2 + \langle x, y\rangle + \langle y, x\rangle + \|y\|^2 = (r\check{c}(x) -$ $t'\ x) = \|x\|^2 + 2.r\check{c}(\langle x, y\rangle) + \|y\|^2 \leq \|x\|^2 + 2\langle x, y\rangle + \|y\|^2 = (\|x\| + \|y\|)^2$.

Veta 2.4.3.2.
Nech V je unitárny priestor a $x_1..x_n$ je lineárne nezávislá sústava vektorov V. Potom existuje ortonormálna sústava sústava $y_1..y_n$ $\forall i\in 1..n : [x_1..x_i] = [y_1..y_i]$.

Dôkaz.
Dôkaz rovnaký ako pre euklidovské priestory (veta 2.4.1.4).

Dôsledok 2.4.3.1.
V existuje ortonormálna báza.

Dôkaz.
Zrejmé.

Veta 2.4.3.3.
Nech V je unitárny priestor, $x_1..x_n$ jeho ortonormálna báza a $x = \sum_{i=1}^{n}\alpha_i x_i$, $y = \sum_{i=1}^{n}\beta_i x_i \in V$. Potom $\langle x, y\rangle = \sum_{i=1}^{n}\alpha_i\overline{\beta_i}$.

Dôkaz.
$\langle x, y\rangle = \langle \sum_{i=1}^{n}\alpha_i x_i\ ,\ \sum_{i=1}^{n}\beta_i x_i\ \rangle = \sum_{i=1,j=1}^{n}\alpha_i\overline{\beta_j}\langle x_i, y_j\rangle = \sum_{i=1}^{n}\alpha_i\overline{\beta_i}$.

Veta 2.4.3.4.
Nech V je unitárny alebo euklidovský prietor a $x_1..x_n$ jeho ortonormálna báza. Potom
- $\forall x = \sum_{i=1}^{n}\alpha_i x_i \in V\ \forall i\in 1..n : \alpha_i = \langle x, x_i\rangle$
- $\forall x,y\in V : \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$
- $\left\|\sum_{i=1}^{n}x_i\right\| = \sum_{i=1}^{n}\|x_i\|$.

Dôkaz.

- $\langle x, x_i\rangle = \langle \sum_{j=1}^{n} \alpha_j x_j \, , x_i\rangle = \sum_{j=1}^{n} \langle \alpha_j x_j , x_i \rangle = \sum_{j=1}^{n} \alpha_j \langle x_j , x_i \rangle = \alpha_i$.
- $\|x+y\|^2 + \|x-y\|^2 = \langle x+y, x+y\rangle + \langle x-y, x-y\rangle = \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle \langle y, y\rangle + \langle x, x\rangle - \langle x, y\rangle - \langle y, x\rangle + \langle y, y\rangle = 2(\langle x, x\rangle + \langle y, y\rangle) = 2(\|x\|^2 + \|y\|^2)$.
- $\left\|\sum_{i=1}^{n} x_i\right\|^2 = \left\langle \sum_{i=1}^{n} x_i, \sum_{k=1}^{n} x_k \right\rangle = \sum_{i=1}^{n}\sum_{k=1}^{n} \langle x_i, x_k\rangle = \sum_{k=1}^{n} \langle x_k, x_k\rangle = \sum_{k=1}^{n} \|x_k\|$.

Veta 2.4.3.5.

Nech V je unitárny alebo euklidovský priestor, $x_1..x_n$ ortogonálna sústava vektorov z V a $x \in V$. Ak $\forall i \in 1..n$: $\alpha_i = \langle x, x_i\rangle$, potom

- $\sum_{j=1}^{n} |\alpha_j|^2 \le \|x\|^2$ (*Besselova nerovnosť*)
- Ak $x_1..x_n$ je báza vo V, tak $\sum_{j=1}^{n} |\alpha_j|^2 = \|x\|^2$ (*Parsevalova rovnosť*).

Dôkaz.

Doplníme $x_1..x_n$ na bázu $x_1..x_m$. Podľa vety 2.4.3.3 $\|x\|^2 = \sum_{j=1}^{m} |\alpha_j|^2 \ge \sum_{j=1}^{m} |\alpha_j|^2$.

2.5. Grupy.

2.5.1. Pologrupy.

Lema 2.5.1.1.

Nech G je grupa a nech $ax = ay$ ($xa = ya$). Potom $x = y$.

Dôkaz.

$ax = ay \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow x = y$.

Definícia.

Usporiadanú dvojicu $(G, \bullet)$ nazývame *pologrupa*, ak G je neprázdna množina a $\bullet$ je binárna asociatívna operácia na G.

Lema 2.5.1.2.

Nech $(G, \bullet)$ je pologrupa s vlastnosťami

1. $\exists e \in G\ \forall x \in G : e \bullet x = x$
2. $\forall x \in G\ \exists y \in G : y \bullet x = e$. Potom G je grupa.

Dôkaz.

Nech $y \bullet x = e$ a $z \bullet y = e$. Potom $x \bullet y = e \bullet x \bullet y = () = z \bullet y \bullet x \bullet y = z \bullet (y \bullet x) \bullet y = z \bullet e \bullet y = z \bullet y = e$ a $x \bullet e = x \bullet y \bullet x = e \bullet x = x$.

Lema 2.5.1.3.

Pologrupa $(G, \bullet)$ je grupa práve vtedy, keď $\forall a,b \in G\ \exists x,y \in G : x \bullet a = b \wedge a \bullet y = b$.

Dôkaz.

Dopredná implikácia je triviálna. Obrátene nech $\forall a,b \in G\ \exists x,y \in G : x \bullet a = b \wedge a \bullet y = b$. Označme e koreň rovnice $x \bullet a = a$. Potom $\forall b \in G : e \bullet b = e \bullet (a \bullet y) = (e \bullet a) \bullet y = a \bullet y = b \Rightarrow e$ je ľavá jednotka G a preto podľa lemy 2.5.1.2 je G grupa.

Veta 2.5.1.1.

Ak v konečnej pologrupe G platia pravidlá o krátení, tak G je grupa.

Dôkaz.

Položme $\forall a \in G : \varphi_a : G \to G$ také, že $\forall a \in G : \varphi_a(x) = a \bullet x$ a $\psi_a : G \to G$ také, že $\forall x \in G : \psi_a(x) = x \bullet a$. Obe tieto zobrazenia sú injektívne ($\varphi_a(x) = \varphi_a(y) \Rightarrow a \bullet x = a \bullet y \Rightarrow x = y$ a rovnako $\psi_a(x) = \psi_a(y) \Rightarrow x \bullet a = y \bullet a \Rightarrow x = y$) a keďže G je konečná, sú ja surjektívne a teda bijektívne. Ale potom $\forall a,b \in G\ \exists x,y \in G : \varphi_a(x) = a \bullet x = b \wedge \psi_a(y) = y \bullet a = b$ a teda podľa lemy 2.5.1.3 je G grupa.

2.5.2. Izomorfizmus na grupách.

Veta 2.5.2.1.

Nech A je množina. Potom usporiadaná dvojica $(\mathbf{P}(A), \circ)$ je grupa.

Dôkaz.

Triviálne.

Definícia.

$(\mathbf{P}(A), \circ)$ je *permutačná grupa* na A (alebo grupa permutácií). Pre $A = \{1..n\}$ ju nazývame *symetrická grupa rádu n* a označujeme S_n.

Definícia.

Nech $(G, *)$ a $(H, \bullet)$ sú grupy. Bijekciu $f : G \to H$ s predpisom $\forall x,y \in G : f(x*y) = f(x) \bullet f(y)$ nazývame *izomorfizmus*. V takom prípade hovoríme, že A a B sú *izomorfné*.

Veta 2.5.2.2.

Nech $f : A \to B$ je bijekcia. Potom $(\mathbf{P}(A), \circ)$ a $(\mathbf{P}(B), \circ)$ sú izomorfné.

Dôkaz.

Nech $\varphi,\psi \in \mathbf{P}(A)$. Položme $\Phi : \mathbf{P}(A) \to \mathbf{P}(B)$ také, že $\Phi(\varphi) = f \circ \varphi \circ f^{-1}$. Potom $f(\varphi \circ \psi) = f \circ \varphi \circ \psi \circ f^{-1} = f \circ \varphi \circ f^{-1} \circ f \circ \psi \circ f^{-1} = (f \circ \varphi \circ f^{-1}) \circ (f \circ \psi \circ f^{-1}) = \Phi(\varphi) \circ \Phi(\psi)$ a Φ je izomorfizmus.

Veta 2.5.2.3.

Nech $f : (G, *) \to (H, \bullet)$ je izomorfizmus. Potom aj f^{-1} je izomorfizmus.

Dôkaz.

$$\forall u,v \in H : f^{-1}(u \bullet v) = f^{-1}((f \circ f^{-1})(u) \bullet (f \circ f^{-1})(v)) = f^{-1}(f(f^{-1}(u)) \bullet f(f^{-1}(v))) = f^{-1}(f(f^{-1}(u) * f^{-1}(v))) = f^{-1}(u) * f^{-1}(v).$$

2.5.3. Podgrupy.

Definícia.

Nech $(G, *)$ a $(H, \bullet)$ sú grupy. Hovoríme, že H je *podgrupa* G a píšeme $H \subseteq G$, ak H je podmnožina G a $\forall x,y \in H : x*y = x \bullet y$.

Veta 2.5.3.1.

Neprázdna podmnožina H grupy $(G, \bullet)$ je jej podgrupa práve vtedy, keď

- $e \in H$
- $\forall x \in H : x^{-1} \in H$
- $\forall x,y \in H : x \bullet y \in H$.

Dôkaz.

Dopredná implikácia je triviálna. Obrátene nech platia uvedené podmienky. Potom $(H, \bullet)$ spĺňa podmienky grupy a keďže $H \subseteq G$, H je podgrupa G.

Veta 2.5.3.2.

Neprázdna podmnožina H grupy $(G, \bullet)$ je jej podgrupa práve vtedy, keď $\forall x,y \in H : x \bullet y^{-1} \in H$.

Dôkaz.

Dopredná implikácia je triviálna. Obrátene nech $\forall x,y \in H : x \bullet y^{-1} \in H$. Potom $\forall x \in H : x \bullet x^{-1} = e \in H$. Zároveň $\forall x \in H : e \bullet x^{-1} = x^{-1} \in H$, takže H je podľa vety 2.5.3.1 podgrupa G.

Veta 2.5.3.3.

Nech $\{H_i\}_{i \in 1..n}$ je systém podgrúp G. Potom aj $\bigcap_{i=1}^{n} H_i$ je podgrupa G.

Dôkaz.

Triviálne.

Veta 2.5.3.4.

Nech M je neprázdna podmnožina grupy G. Potom existuje jediná jej podgrupa $[M]$ taká, že

1. $[M] \supseteq M$
2. $\forall H < G : H \supseteq M \Rightarrow H \supseteq [M]$.

Dôkaz.

Nech $\{H_i\}_{i\in 1..n}$ je systém podgrúp G takých, že $\forall i\in 1..n : H_i\supseteq M$. Potom aj $[M] = \bigcap_{i=1}^{n} H_i$ je podgrupa G a $[M]\supseteq M$. Pritom z vlastnosti 2. vyplýva, že každé dve takéto podgrupy sú zhodné, takže $[M]$ je jediná.

Definícia.

$[M]$ nazývame *minimálna podgrupa* G, obsahujúca M.

Veta 2.5.3.5.

$[M] = \left\{x_1^{e_1}..x_n^{e_n}; \forall i\in 1..n: x_i\in M \wedge e_i\in\{-1,1\}\right\}$.

Dôkaz.

$M\notin\emptyset \Rightarrow \exists x\in M \Rightarrow x\bullet x^{-1}=e\in[M]$. Zároveň $\forall x=x_1^{e_1}..x_n^{e_n}, y=y_1^{d_1}..y_m^{d_m}\in M : x\bullet y = x_1^{e_1}..x_n^{e_n}y_1^{d_1}..y_m^{d_m}\in[M]$ a $x^{-1} = x_1^{-e_1}..x_n^{-e_n}\in[M]$, že $[M]$ je podgrupa G. Zároveň $[M]\supseteq$ minimálnej podgrupy G, obashujúcej M eďže j o rá ene žd $x = x_1^{e_1}..x_n^{e_n}; \forall i\in 1..n\ x_i\in M\wedge e_i\in\{-1\ 1\}\in$ do minimálnej podgrupy, $[M]$ je minimálna podgrupa.

Definícia.

Nech $(G, \bullet)$ je grupa, $a\in G$. n-tou *mocninou* a rozumieme $a^n = \begin{cases} a^{n-1}\bullet a \leftarrow n>1 \\ a \leftarrow n=1 \\ e \leftarrow n=0 \\ \left(a^{-1}\right)^{-n} \leftarrow n<0 \end{cases} \in G$.

Lema 2.5.3.1.

Nech $(G, \bullet)$ je pologrupa, $a, b_1..b_n\in G$, ričo $\forall i\in 1..n : a\bullet b_i = b_i\bullet a$. Potom $a\bullet(b_1\bullet..\bullet b_n) = (b_1\bullet..\bullet b_n)\bullet a$.

Dôkaz.

Triviálne.

Veta 2.5.3.6.

Nech $a,b\in G$. Potom $\forall m,n\in Z$:

1. $a^m\bullet a^n = a^{m+n}$
2. $(a^m)^n = a^{m.n}$
3. $a\bullet b = b\bullet a \Rightarrow (a\bullet b)^n = a^n\bullet b^n$.

Dôkaz.

1. Indukciou na n. $a^m\bullet a^1 = a^{m+1}$ z definície. $a^m\bullet a^{n+1} = a^m\bullet a^n\bullet a = a^{m+n}\bullet a = a^{m+n+1}$
2. Indukciou na n. $(a^m)^1 = a^m$. $(a^m)^{n+1} = (a^m)^n\bullet a^m = a^{m.n}\bullet a^m = a^{m.(n+1)}$.
3. Indukciou na n. $(a\bullet b)^1 = a\bullet b = a^1\bullet b^1$. $(a\bullet b)^{n+1} = (a\bullet b)^n\bullet a\bullet b = a^n\bullet b^n\bullet a\bullet b = a^{n+1}\bullet b^{n+1}$.

(Dôkaz bol vykonaný pre $n > 1$; pre záporné n je dôkaz symetrický).

2.5.4. Cyklické grupy.

Definícia.

Grupa G sa nazýva *cyklická*, ak $\exists a\in G : G = [a]$. Prvok a nazývame *generátor* grupy G. Ak $\forall m,n\in N : a^m\neq a^n$, tak G je ne onečná, in $\exists n\in N : a^n = a$) je G cyklická grupa rádu n.

Veta 2.5.4.1.

K ždá od r li ej r je li á.

Dôkaz.

Nech H je netriviálna podgrupa $G = [a]$ a nech $p = \min\{n\in N; a^n\in H\}$. Je zrej , že $[a^p]\subseteq H$. Ale $\forall s\in N\ \exists q,r\in N : a^s = (a^p)^q\bullet a^r = a^{p.q+r}$, kde $r\leq p$. Ale $a^s\in H \Rightarrow a^r\in H$ (lebo $a^{pq}\in H$) $\Rightarrow r\geq p \vee r = 0 \Rightarrow r = 0 \Rightarrow a^s\in[a^p] \Rightarrow [a^p]\supseteq H \Rightarrow H = [a^p] \Rightarrow H$ je cyklická.

Veta 2.5.4.2.

K žd dve li r rovn o rád s izo orfn .

Dôkaz.

Nech $[a]$ a $[b]$ sú rovnakého rádu. Potom hľadaným izomorfizmom je zobrazenie $a^n\rightarrow b^n$.

2.5.5. Homomorfizmy grúp.

Definícia.

Nech $(G, *)$ a $(H, \bullet)$ sú grupy. Zobrazenie $f : G \to H$ nazývame *izomorfizmus*, ak $\forall x,y \in G : f(x*y) = f(x) \bullet f(y)$.

Veta 2.5.5.1.

Nech $f : (G, \bullet) \to (H, *)$ a $g : (H, *) \to (K, \oplus)$ sú homomorfizmy. Potom aj $g \circ f$ je homomorfizmus.

Dôkaz.

$\forall x,y \in G : g \circ f(x+y) = g(f(x+y)) = g(f(x) * f(y)) = g(f(x)) \oplus g(f(y)) = g \circ f(x) \oplus g \circ f(y)$.

Veta 2.5.5.2.

Nech $f : (G, \bullet) \to (H, *)$ je homomorfizmus. Potom

1. Ak e_G je jednotka v G a e_H v H, tak $f(e_G) = e_H$
2. $\forall x \in G : f(x^{-1}) = (f(x))^{-1}$
3. $\forall x \in G \ \forall n \in Z : f(x^n) = (f(x))^n$.

Dôkaz.

1. $e_H * f(e_G) = f(e_G) = f(e_G \bullet e_G) = f(e_G) * f(e_G) \Rightarrow f(e_G) = e_H$.
2. $\forall x \in G : e_H = f(e_G) = f(x \bullet x^{-1}) = f(x) * f(x^{-1}) \Rightarrow f(x^{-1}) = (f(x))^{-1}$.
3. $\forall x \in G \ \forall n \in N : f(x^1) = f(x)^1$ a $f(x^{n+1}) = f(x^n \bullet x) = f(x^n) * f(x) = f(x)^n * f(x) = f(x)^{n+1}$. Ak $n < 0$, $f(x^n) = f((x^{-1})^{-n}) = f(x^{-1})^{-n} = (f(x)^{-1})^{-n} = (f(x))^n$.

Veta 2.5.5.3.

Nech $f : (G, \bullet) \to (H, *)$ je homomorfizmus. Potom $Ker(f) \subseteq G$ a $Im(f) \subseteq H$.

Dôkaz.

$Ker(f$ je ne rázdne, le o odľ ve . . . odse 1. $e_G \in Ker(f$. Zároveň $\forall x,y \in Ker(f) : f(x \bullet y) = f(x) * f(y) = e_H * e_H = e_H$ odľ ve . . . odse . $f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H$, čiže $Ker(f)$ je podgrupa G. podobne je neprázdne aj $Im(f)$ (z rovnakého dôvodu ako $Ker(f)$), $\forall x,y \in Im(f) \ \exists u,v \in G : f(u) = x$ a $f(v) = y$. Potom $x * y^{-1} = f(u) * f(v)^{-1} = f(u) * f(v^{-1}) = f(u \bullet v^{-1}) \in Im(f)$, čiže $Im(f)$ je podgrupa H.

Veta 2.5.5.4.

Nech $f : [a] \to (G, \bullet)$ je surjektívny homomorfizmus. Potom G je cyklická grupa.

Dôkaz.

f je surjektívne $\Rightarrow \forall x \in G \ \exists \ n \in N : f(a^n) = x \Rightarrow f(a)^n = x \Rightarrow G = [f(a)]$.

Veta 2.5.5.5.

Nech $f : (G, \bullet) \to (H, *)$ je homomorfizmus. Potom f je inje i s rje i ráve v ed , eď $Ker(f) = \{e\}$ $(Im(f) = H)$.

Dôkaz.

Dopredné implikácie sú triviálne. Obrátene nech $Ker(f) = \{e\}$. Potom $\forall x,y \in G : f(x) = f(y) \Rightarrow e_H = f(x) * f(y)^{-1} = f(x) * f(y^{-1}) = f(x \bullet y^{-1}) \Rightarrow x \bullet y^{-1} = e_G \Rightarrow x = y$. Obrátená implikácia pre $Im(f)$ je triviálna.

2.5.6. Permutačné grupy.

Definícia.

Nech $(G, \bullet)$ je grupa. $\forall a \in G$ nazývame zobrazenie $f_a : G \to G$, kde $\forall x \in G : f_a(x) = a \bullet x$ $(x \bullet a$, ľ vá (pravá) *translácia a*.

Lema 2.5.6.1.

Nech $(G, \bullet)$ je grupa. Potom $\forall a \in G$ je ľ vá i r vá r nslá i a bijektívna.

Dôkaz.

Dô z v oná e re ľ v r nslá i . Dô z re r v r nslá i je s e ri . $\forall x,y \in G : f_a(x) = f_a(y) \Leftrightarrow a \bullet x = a \bullet y \Leftrightarrow x = y \Rightarrow f_a$ je injekcia. Zároveň $\forall x \in G : f_a(a^{-1} \bullet x) = a \bullet a^{-1} \bullet x = x \Rightarrow f_a$ je surjekcia $\Rightarrow f_a$ je bijekcia.

Dôsledok 2.5.6.1.

Nech $(G, \bullet)$ je grupa a f_a je ľ vá r vá r nslá i rv $a \in G$. Potom $f_a \in \mathbf{P}(G)$.

Dôkaz.
Tvrdenie vyplýva priamo z lemy 2.5.6.1 a definície **P**(*G*).

Veta 2.5.6.1 (Cayley).
K ždej r e $G, \bullet$ exis je izo orfná od r er čnej r **P**(*G*).

Dôkaz.
S č áz ť, že re $H = \{f_a; a \in G, f_a$ je ľ vá r vá r nslá i $a\}$ je $(H, \circ)$ podgrupa *G*. Ale $\forall a,b,x \in G$: $f_a \circ f_b(x) = f_a(f_b(x)) = f_a(b \bullet x) = a \bullet b \bullet x = f_{a \bullet b}(x$, že vrdenie platí.

Definícia.
Permutácia $\varphi \in S_n$ sa nazýva *cyklus*, ak $\exists i_1 < .. < i_m \in 1..n \ \forall k \in 1..m : \varphi(i_k) = i_{k+1} \wedge \varphi(i_m) = i_1$. Č slo *m* nazývame *dĺžka* cyklu φ. C l s dĺž s n z v *transpozícia*.

Definícia.
Č slo $r = \min\{n \in N; \varphi^n = id\}$ sa nazýva *rád* cyklu φ.

Veta 2.5.6.2.
Rád žd o l je rovn je o dĺž e.

Dôkaz.
Triviálne.

Veta 2.5.6.3.
Nech $\varphi, \psi \in S_n$ sú disjunktné. Potom $\varphi \circ \psi = \psi \circ \varphi$.

Dôkaz.
Triviálne.

Dôsledok 2.5.6.2.
Ak $\varphi, \psi \in S_n$ sú disjunktné, tak $\forall n \in N : (\varphi \circ \psi)^n = \varphi^n \circ \psi^n$.

Dôkaz.
Tvrdenie vyplýva priamo z predchádzajúcej vety.

Veta 2.5.6.4.
K ždá er á i $\varphi \neq id$ s dá ž n or die zá vorie jedin s ôso o z s ť v v re s čin disj n n lov dĺž s oň .

Dôkaz.
Triviálne.

Veta 2.5.6.5.
K ždá $\varphi \in S_n$ s dá n s ť o s čin r ns oz i .

Dôkaz.
odľ ve . .6. s ždá $\varphi \neq id$ dá napísať ako súčin disjunktných cyklov. Zároveň cyklus $(i_1, .. , i_n)$, kde $n >$, s dá rozložiť n r ns oz ie $i_1, i_2) \circ .. \circ (i_{n-1}, i_n)$. *id* vyjadrím ako $(i_1, i_2) \circ (i_1, i_2)$.

Veta 2.5.6.6.
Všetky vyjadrenia φ o s čin r ns oz i j rovn ritu.

Dôkaz.
Triviálne.

Definícia.
$\varphi \in S_n$ je *párna*, je v j dri eľná o s čin árne o oč r ns oz i . φ je *nepárna*, ak nie je párna.

Dôsledok 2.5.6.3.
1. S čin dvo er i rovn ej ri je árn .
2. Inverzná permutácia k párnej (nepárnej) je párna (napárna).
3. Párne permutácie tvoria spolu s operáciou skladania zobrazení podgrupu S_n.

Dôkaz.
1. Vyplýva priamo z predchádzajúcej vety.
2. Vyplýva priamo z predchádzajúcej vety.

3. Vyplýva z 1. a 2.

Definícia.

Grupu párnych permutácií z S_n nazývame *alternujúca podgrupa* S_n.

2.5.7. Rozklady na grupách.

Definícia.

Systém $\{A_i\}_{i\in 1..n}$ od ož n A je *rozklad* A, ak $\forall i\neq j\in 1..n : A_i\cap A_j=\emptyset$.

Definícia.

Nech $(H, *)$ je podgrupa $(G, *)$. $\forall g\in G$ defin je e nožin $H_g = \{g*h;\ h\in H)$ a $H^g = \{h*g;\ h\in H\}$. Ď lej ozn č e $G|_H = \{H_g;\ g\in G\}$ a $G|^H = \{H^g;\ g\in G\}$.

Veta 2.5.7.1.

Nech $(H, *)$ je podgrupa $(G, *)$. Potom $G|_H$ a $G|^H$ sú rozklady grupy G.

Dôkaz.

Tvrdenie do áže e re $G|_H$. Dôkaz pre $G|^H$ je symetrický. Nech $\exists g,g´\in G : H_g\cap H_g\neq\emptyset$. Potom $\exists x\in G : x\in H_g \wedge x\in H_{g´} \Rightarrow \exists h,h´\in H : x = g*h = g´*h´ \Rightarrow g = g´*h´*h\in H_{g´} \wedge g´ = g*h*h´\in H_g \Rightarrow H_g = H_{g´}$.

Veta 2.5.7.2.

Nech $(H, *)$ je podgrupa $(G, *)$. Potom $\forall g\in G : H_g = H$.

Dôkaz.

$f : H\to H_g$ s predpisom $f(x) = g*x$ je zjavne bijekcia.

Veta 2.5.7.3 (Lagrange).

Nech $(H, *)$ rádu p je od r onečnej $G, *)$ rádu n. Potom n je deli eľn p.

Dôkaz.

odľ ve . .7. $\forall\ g\in G : H_g = H \Rightarrow |H_g| = |H| = p$. eďže $G|_H$ je rozklad G s onečn oč o komponentov (lebo g je onečná , $G| = n$ je deli eľn $H| = p$.

Dôsledok 2.5.7.1.

Nech G je onečná r rád n. Potom $\forall g\in G$: rád g delí n.

Dôkaz.

Rád g je rádom $[g]$, že vrdenie v l v ri o z L r n eovej ve .

Dôsledok 2.5.7.2.

K ždá r rvoč seln o rád je li á.

Dôkaz.

Nech G je rádu n a n je rvoč slo. o o $\forall g\in G : g\neq e \Rightarrow [g]$ je rádu n, lebo n ne á in deli eľov.

2.5.8. Invariantné podgrupy.

Definícia.

Podgrupa H grupy G sa nazýva *invariantná* alebo *normálna*, ak $\forall g\in G : H_g = H^g$. Zapisujeme $H<G$.

Lema 2.5.8.1.

Podgrupa H grupy G je inv ri n ná ráve v ed , eď $\forall g\in G : H_g{}^{g´} = \{g*h*g^{-1};\ h\in H\} \approx H$.

Dôkaz.

$H<G \Rightarrow \forall g\in G : H_g = H^g \Rightarrow \forall g\in G\ \exists h\in H_g\ \exists h´\in H^g : h*g = g*h´ \Rightarrow g = h*g*h´$ eďže odľ ve 2.5.7.2 $H_g = H^g = H$, $H_g{}^{g´} = \{g*h*g^{-1};\ h\in H\} = H$. Obrátene $\forall g\in G\ \forall v\in H_g\ \exists h\in H : x*h = x*h*x^{-1}*x = (h*x^{-1}*x = h´) = h´*x\in H^g \Rightarrow H_g\subseteq H^g$. čná in l zi odo ne.

Dôsledok 2.5.8.1.

Podgrupa H grupy G je inv ri n ná ráve v ed , eď $\forall g\in G : \forall h\in H : g*h*g^{-1}\in H$.

Dôkaz.

Tvrdenie vyplýva priamo z predchádzajúcej vety.

Veta 2.5.8.2.

Ak $f : G \to H$ je homomorfizmus, tak $Ker(f) < G$.

Dôkaz.

$\forall g \in G, x \in Ker(f) : f(g*x*g^{-1}) = f(g) * f(x) * f(g^{-1}) = f(g) * f(g^{-1}) = f(g*g^{-1}) = f(e) = e \Rightarrow g*x*g^{-1} \in Ker(f)$.

Definícia.

Nech G je r . nožin $Z(G)=\{g \in G; \forall x \in G : x*g = g*x\}$ nazývame *centrum* grupy G.

Veta 2.5.8.3.

Cen r ždej r je jej inv ri n no od r o .

Dôkaz.

$\forall g \in G, x \in Z(G)\ \forall h \in G : g*x*g^{-1}*h = x*g*g^{-1}*h = x*e*h = x*h = h*x = h*x*g*g^{-1} = h*g*x*g^{-1} \Rightarrow Z(G) < G$.

Definícia.

Nech G je r . nožin $K(G) = \{g*h*g^{-1}*h^{-1}; g,h \in G\}$ nazývame *komutant* grupy G. Prvok $g*h*g^{-1}*h^{-1}$ ozn č je e $[g, h]$.

Veta 2.5.8.4.

Ko n ždej r je jej inv ri n ná od r .

Dôkaz.

$\forall g \in G,\ k=a*b*a^{-1}*b^{-1} \in K(G) : g*k*g^{-1} = g*a*b*a^{-1}*b^{-1}*g^{-1} = g*a*g^{-1}*g*b*g^{-1}*g*\ a^{-1}*g^{-1}*g*b^{-1}*g^{-1} = [g*a*g^{-1}, g*b*g^{-1}] \in K(G)$.

Definícia.

Nech G je grupa. Homomorfizmus $f : G \to G$ nazývame *automorfizmus*. nožin všetkých automorfizmov na G ozn č e $A(G)$.

Veta 2.5.8.5.

Nech G je grupa. Potom $(A(G), \circ)$ je grupa.

Dôkaz.

id je jednotka v $A(G)$, $\forall f \in A(G) : f^{-1} \in A(G$, le o žd automorfizmus je bijekcia, a $\forall f,g \in A(G) : f \circ g \in A(G)$, lebo automorfizmus je aj homomorfizmus.

Definícia.

Nech G je grupa. Grupa $(A(G), \circ)$ sa nazýva *alternujúca* grupa na G.

Veta 2.5.8.6.

Nech G je grupa. Potom $\forall g \in G$ je zobrazenie $\varphi_g : G \to G$ s predpisom $\varphi_g(x) = g*x*g^{-1}$ automorfizmus.

Dôkaz.

Triviálne.

Definícia.

Nech G je grupa. Potom $\forall g \in G$ automorfizmus $\varphi_g : G \to G$ s predpisom $\varphi_g(x) = g*x*g^{-1}$ nazývame *vnútorný* o orfiz s, rčen rv o g. nožin vn orn o orfiz ov, rčen rv i G, ozn č je e $I(G)$.

Veta 2.5.8.7.

Nech G je grupa. Potom $(I(G), \circ)$ je grupa.

Dôkaz.

$\varphi_g \circ \varphi_h(x) = \varphi_g(\varphi_h(x)) = \varphi_g(h*x*h^{-1}) = g*h*x*h^{-1}*g^{-1} = \varphi_{g \circ h}(x$. s n vl s nos i z r č je veta 2.5.8.5.

Veta 2.5.8.8.

Nech G je grupa. Potom $I(G) < A(G)$.

Dôkaz.

$\forall f \in A(G)\ \forall \varphi_g \in I(G)\ \forall x \in G : \varphi_{f(g)}(x) = f(g) * x * f(g)^{-1} = f(g) * f(\ f^{-1}(x)\ ) * f(g)^{-1} = f(g * f^{-1}(x) * g^{-1}) = f(\varphi_g(f^{-1}(x))) = f \circ \varphi_g \circ f^{-1}(x) \in I(G)$.

2.5.9. Faktorové grupy.

Veta 2.5.9.1.

Nech $(H, \bullet)<(G, \bullet)$. Potom existuje jediná binárna operácia $*$ á, že $G|_H, *)$ je grupa a zobrazenie $f : G\to G|_H$ s predpisom $f(g) = H_g$ homomorfizmus.

Dôkaz.

Definujme operáciu $*$ predpisom $H_g*H_h = H_{g\bullet h}$. Táto operácia je korektná iba ak je nezávislá od výberu reprezentantov tried H_g a H_h. nech teda $H_g = H_{g´}$ a $H_h = H_{h´}$. Potom ale $H_{g\bullet h} = H_{g´\bullet h´}$, čiže nezávislosť je z r čená. so i vnosť $*$ iež, le o $\forall x,y,z\in G : (H_x * H_y) * H_z = H_{x\bullet y} * H_z = H_{(x\bullet y)\bullet z} = H_{x\bullet(y\bullet z)} = H_x * H_{y\bullet z} = H_x * (H_y * H_z)$. Inverzný prvok je zrejmý a takisto f je homomorfizmus, lebo $\forall g,h\in G : f(x\bullet y) = H_{x\bullet y} = H_x * H_y = f(x) * f(y)$.

Definícia.

Nech $H<G$, $*$ taká binárna operácia, že $(G|_H, *)$ je grupa a zobrazenie $f : G\to G|_H$ s predpisom $f(g) = H_g$ homomorfizmus. Potom $(G|_H, *)$ je *faktorová grupa* G odľ H.

Veta 2.5.9.2.

Nech $f : G\to H$ je surjektívny homomorfizmus. Potom $Ker(f)<G$ a $G|_{Ker(f)} \approx H$.

Dôkaz.

Homomorfizmus f vyplýva priamo z vety 2.5.8.2. Definujme $g : G|_{Ker(f)}\to H$ predpisom $\forall x\in G : g(Ker(f)_x) = f(x)$. $\forall x,y\in G : Ker(f)_x = Ker(f)_y \Rightarrow x\bullet y^{-1}\in Ker(f) \Rightarrow f(x\bullet y) = e_H \Rightarrow f(x) = f(y) \Rightarrow g$ je injektívne lineárne zobrazenie. Naviac g je o o orfiz s, re ože f je o o orfiz s. eďže f je surjekcia, g je izomorfizmus.

Dôkaz.

Dôsledok 2.5.9.1.

Nech G je grupa. Potom $G|_{Z(G)} \approx I(G)$.

Dôkaz.

Nedokazujeme.

2.6. Determinanty.

2.6.1. Determinant matice.

Definícia.

Nech A je štvorcová matic s ň n. Č slo $A| = \sum_{\tau\in S_n}\left(\operatorname{sgn}\tau.\prod_{i=1}^{n} a_{i,\tau(i)}\right)$, kde $\operatorname{sgn}\tau = 1$, ak τ je párna a -1, ak τ je nepárna, nazývame *determinant* matice A.

2.6.2. Vlastnosti determinantov.

Veta 2.6.2.1.

Nech A je š vor ová i s ň n. Potom $|A| = |A^{\perp}|$.

Dôkaz.

$|A^{\perp}| = \sum_{\tau\in S_n}\left(\operatorname{sgn}\tau.\prod_{i=1}^{n} a^{\perp}_{i,\tau(i)}\right) = \sum_{\tau\in S_n}\left(\operatorname{sgn}\tau.\prod_{i=1}^{n} a_{\tau(i),i}\right) = \sum_{\tau\in S_n}\left(\operatorname{sgn}\tau.\prod_{i=1}^{n} a_{i,\tau(i)}\right)$, lebo inverzná permutácia má rovnakú paritu.

Veta 2.6.2.2.

Nech A je štvorcová matica stupňa n. Nech $c\in F$ a nech $A´$ vznikne z A vynásobením niektorého riadku c. Potom $|A´| = c.|A|$.

Dôkaz.

Triviálne.

Veta 2.6.2.3.

Nech A je štvorcová matica stupňa n a nech $A´$ vznikne z A výmenou dvoch riadkov. Potom $|A´| = -|A|$.

Dôkaz.

Výmenou dvoch riadkov porušíme paritu každej permutácie.

Dôsledok 2.6.2.1.

Nech A je štvorcová matica stupňa n. Ak A má dva rovnaké riadky, tak $|A| = 0$.

Dôkaz.

Zrejmé z predchádzajúceho tvrdenia.

Definícia.

Ak vo vzorci pre výpočet determinantu vyberiem pred zátvorku $a_{i,j}$ zo všetkých členov, v ktorých sa nachádza, potom číslo v zátvorke nazývame *algebraický doplnok* k $a_{i,j}$.

Lema 2.6.2.1(Laplace).

Nech A je štvorcová matica stupňa n. Potom $\forall i \in 1..n : |A| = \sum_{j=1}^{n} a_{i,j} A_{i,j}$.

Dôkaz.

Triviálne.

Lema 2.6.2.2.

Nech A je štvorcová matica stupňa n. Potom $\forall i,k \in 1..n : \sum_{j=1}^{n} a_{i,j} A_{k,j} = 0$.

Dôkaz.

Pre* $i \neq k$ $\sum_{j=1}^{n} a_{i,j} A_{k,j} = 0$, lebo do i-teho riadku sme dali k-ty, čím vznikli dva rovnaké riadky.

Označenie.

Nech A je štvorcová matica stupňa n, nech $i,j \in 1..n$. Determinant matice, ktorá v znikne z A odobratím i-teho riadku a j-teho stĺpca, označíme $M_{i,j}$.

Lema 2.6.2.3.

Nech A je štvorcová matica stupňa n, nech $i,j \in 1..n$. Potom $A_{i,j} = (-1)^{i+j} M_{i,j}$.

Dôkaz.

Zrejme $A_{1,1} = M_{1,1} = (-1)^2 M_{1,1}$. Ale $a_{i,j}$ presunieme i-1+j-1 výmenami riadkov a stĺpcov na pozíciu 1,1 a keďže každá s týchto operácií obracia znamienko determinantu a $(-1)^{i-1+j-1} = (-1)^{i+j}$, platí $A_{i,j} = (-1)^{i+j} M_{i,j}$.

Veta 2.6.2.5.

Nech A je štvorcová matica stupňa n. Nech $c \in F$ a nech A' vznikne z A pripočítaním c-násobku nejakého riadku A k inému riadku A. Potom $|A'| = |A|$.

Dôkaz.

Nech A' vznikne pripočítaním c-násobku i-teho riadku ku k-temu. Potom $|A'| = \sum_{j=1}^{n} a'_{k,j} A'_{k,j} = \sum_{j=1}^{n} a_{k,j} A_{k,j} + \sum_{j=1}^{n} c.a_{k,j} A_{i,j} = \sum_{j=1}^{n} a_{k,j} A_{k,j} + c.\sum_{j=1}^{n} a_{k,j} A_{i,j} = \sum_{j=1}^{n} a_{k,j} A_{k,j} + c.0 = \sum_{j=1}^{n} a_{k,j} A_{k,j} = |A|$.

Definícia.

Nech A je štvorcová matica stupňa n. Maticu $A_a = \begin{pmatrix} A_{1,1} & \Lambda & A_{1,n} \\ \mathrm{M} & \mathrm{O} & \mathrm{M} \\ A_{n,1} & \Lambda & A_{n,n} \end{pmatrix}$, v ktorej stĺpcoch sú algebraické doplnky riadkov matice A, nazývame matica *adjungovaná* k A.

Veta 2.6.2.6

Nech A je štvorcová matica stupňa n a A_a je jej adjungovaná matica. Potom $A \times A_a = \begin{pmatrix} |A| & 0 & 0 \\ 0 & |A| & 0 \\ 0 & 0 & |A| \end{pmatrix}$.

Dôkaz.

Tvrdenie vyplýva priamo z Laplaceovej vety (veta 2.6.2.4) a jej dôkazu.

Dôsledok 2.6.2.2.

Nech A je štvorcová matica stupňa n. Ak $|A|\neq 0$, tak A je regulárna a $A^{-1} = A_a \times |A|^{-1}$.

Dôkaz.

Tvrdenie vyplýva priamo z predchádzajúcej vety.

2.6.3. Matice elementárnych úprav.

Označenie.

Nech $c \in F$. Maticu , ktorá vznikne z jednotkovej vynásobením i-teho riadku c, označím $E_i(c)$. Maticu , ktorá vznikne z jednotkovej výmeno i-teho a j-teho riadku, označím $E_{i,j}$. Maticu , ktorá vznikne z jednotkovej pripočítaním c-násobku i-teho riadku k j-temu, označím $E_{i,j}(c)$.

Lema 2.6.3.1.

$|E_i(c)| = c$, $|E_{i,j}| = -1$ a $|E_{i,j}(c)| = 1$.

Dôkaz.

Všetky tri tvrdenie vyplývajú z definície determinantu a možno si ich ľahko overiť.

Veta 2.6.3.1.

Determinant regulárnej matice je nenulový.

Dôkaz.

Ak A je regulárna, tak podľa vety 2.3.4.2 ju možno vyjadriť v podobe súčinu elementárnych matíc. Ľahko sa možno presvedčiť, že determinant súčinu elementárnych matíc je rovný súčinu ich determinantov a keďže determinanty elementárnych matíc sú nenulové, je nenulový aj $|A|$.

Veta 2.6.3.2.

Nech A a B sú štvorcové matice stupňa n. Potom $|A \times B| = |A|.|B|$.

Dôkaz.

Ak A aj B sú regulárne, tak podľa vety 2.3.4.2 ich možno vyjadriť v podobe súčinu elementárnych matíc. Determinant súčinu týchto postupností je podľa vety 2.6.3.1 rovný súčinu determinantov týchto postupností, čiže $|A \times B| = |A|.|B|$. Ak aspoň jedna z matíc A, B nie je regulárna, tak $|A \times B| = |A| = 0$.

Veta 2.6.3.3.

Nech A je štvorcová matica stupňa n. Nech $c \in F$ a nech A' vznikne z A vynásobením niektorého riadku c. Potom $|A'| = |E_i(c) \times A| = |E_i(c)|.|A| = c.|A|$.

Dôkaz.

Podľa vety 2.6.2.2 $|A'| = c.|A|$. Posledná rovnosť platí podľa lemy 2.6.2.1. Prostredná rovnosť vyplýva z vety 2.6.3.2.

Dôsledok 2.6.3.1.

$E_i(c)$ je elementárna matica, reprezentujúca vynásobenie i-teho riadku matice skalárom c.

Dôkaz.

Tvrdenie vyplýva z prvej rovnosti predchádzajúcej vety.

Veta 2.6.3.4.

Nech A je štvorcová matica stupňa n a nech A' vznikne z A výmenou i-teho riadku za j-ty. Potom $|A'| = |E_{i,j} \times A| = |E_{i,j}|.|A| = -|A|$.

Dôkaz.

Podľa vety 2.6.2.3 $|A'| = -|A|$. Posledná rovnosť platí podľa lemy 2.6.2. . Prostredná rovnosť vyplýva z vety 2.6.3.2.

Dôsledok 2.6.3.2.

$E_{i,j}$ je elementárna matica, reprezentujúca výmenu riadkov i a j.

Dôkaz.

Tvrdenie vyplýva z prvej rovnosti predchádzajúcej vety.

Veta 2.6.3.5.

Nech A je štvorcová matica stupňa n. Nech $c \in F$ a nech A' vznikne z A pripočítaním c-násobku i-teho riadku k j-temu. Potom $|A'| = |E_{i,j}(c) \times A| = |E_{i,j}(c)|.|A| = |A|$.

Dôkaz.

Podľa vety 2.6.2.5 $|A'| = |A|$. Posledná rovnosť platí podľa lemy 2.6.2.1. Prostredná rovnosť vyplýva vety 2.6.3.2.

Dôsledok 2.6.3.3.

$E_{i,j}$ je elementárna matica, reprezentujúca pripočítanie c-násobku i-teho riadku k j-temu.

Dôkaz.

Tvrdenie vyplýva z prvej rovnosti predchádzajúcej vety.

2.6.4. Grupa regulárnych matíc.

Veta 2.6.4.1.

Zobrazenie $Det : \mathbf{R}_n \to R$ s predpisom $Det(A) = |A|$ je homomorfizmus.

Dôkaz.

$Det(A \times B) = |A \times B| =$ podľa vety 2.6.3.2 $= |A|.|B| = Det(A).Det(B)$.

Dôsledok 2.6.4.1.

$\mathbf{R}_n|_{Ker(Det)} \approx R$.

Dôkaz.

Tvrdenie vyplýva z vety 2.5.9.2.

2.6.5. Cramerovo pravidlo.

Veta 2.6.5.1 (Cramerovo pravidlo).

Nech A je regulárna matica, adjungovaná k sústave $S = \begin{matrix} a_{1,1}x_1 & \Lambda & a_{1,n}x_n & = b_1 \\ \mathrm{M} & \mathrm{O} & \mathrm{M} & \mathrm{M} \\ a_{n,1}x_1 & \Lambda & a_{n,n}x_n & = b_n \end{matrix}$. Potom S má jediný koreň $(y_1, .. , y_n)$, kde $\forall i \in 1..n : y_i = |D_i|.|A|^{-1}$, pričom D_i vznikne z A nahradením i-teho stĺpca pravou stranou sústavy.

Dôkaz.

$$\forall i \in 1..n \quad : \quad \sum_{j=1}^{n} \frac{a_{i,j}|D_j|}{|A|} = \sum_{j=1}^{n} \frac{a_{i,j}\sum_{k=1}^{n} b_k A_{k,j}}{|A|} = \frac{1}{|A|}\sum_{j=1}^{n} a_{i,j}\sum_{k=1}^{n} b_k A_{k,j} = \frac{1}{|A|}\sum_{j=1}^{n}\sum_{k=1}^{n} b_k a_{i,j} A_{k,j} =$$

$$\frac{1}{|A|}\sum_{k=1}^{n}\sum_{j=1}^{n} b_k a_{i,j} A_{k,j} = \frac{1}{|A|}\sum_{k=1}^{n} b_k \sum_{j=1}^{n} a_{i,j} A_{k,j} = \frac{1}{|A|}\sum_{k=1}^{n} b_k |A| = b_i.$$

2.7. Okruhy.

2.7.1. Základné vlastnosti.

Veta 2.7.1.1.

Nech $(A, \oplus, \otimes)$ je okruh. Potom

- $\forall x \in A : x \otimes 0 = 0 \otimes x = 0$
- $\forall x,y \in A : x \otimes (-y) = (-x) \otimes y = -(x \otimes y)$.

Dôkaz.

- $\forall x \in A : x \otimes 0 = x \otimes (0 \oplus 0) = x \otimes 0 \oplus x \otimes 0 \Rightarrow 0 = x \otimes 0$. $0 \oplus x$ podobne.
- $\forall x,y \in A : 0 = x \otimes 0 = x \otimes (y\text{-}y) = x \otimes y \oplus x \otimes (-y) \Rightarrow x \otimes (-y) = -(x \otimes y)$. $(-x) \otimes y$ podobne.

Veta 2.7.1.2.

Nech $(A, \oplus, \otimes)$ je okruh a $a_1..a_n$, $a \in A$. Potom $a \otimes (a_1 \oplus .. \oplus a_n) = a \otimes a_1 \oplus .. \oplus a \otimes a_n$.

Dôkaz.

Triviálne.

Označenie.
Nech $(A, \oplus, \otimes)$ je okruh, $a \in A$ a $n \in N$. Výraz $\underbrace{a \oplus \ldots \oplus a}_{n}$ budeme zapisovať skrátene $n.a$.

Veta 2.7.1.3.
Nech $(A, \oplus, \otimes)$ je okruh, $x,y \in A$ a $n \in N$. Potom $x \otimes (n.y) = n.(x \otimes y)$.

Dôkaz.
Tvrdenie je priamym dôsledkom vety 2.7.1.2.

2.7.2. Obory integrity.

Definícia.
Nech $(A, \oplus, \otimes)$ je okruh. Prvok $a \in A$ nazývame ľavý (ravý) *deliteľ nuly*, ak $\exists b \in A : b \neq 0 \wedge a \otimes b = 0$ ($b \otimes a = 0$). Ak $a \neq 0$, a je *netriviálny* deliteľ nuly.

Poznámka.
Obor integrity je okruh s aspoň dvoma prvkami, neobsahujúci netriviálne delitele nuly.

Veta 2.7.2.1.
Nech $(A, \oplus, \otimes)$ je obor integrity. Potom v A platia obmedzené pravidlá o krátení ($\forall a,x,y \in A : a \otimes x = a \otimes y \Rightarrow x = y$ a $x \otimes a = y \otimes a \Rightarrow x = y$).

Dôkaz.
$\forall a,x,y \in A : a \otimes x = a \otimes y \Rightarrow a \otimes x \oplus -(a \otimes y) = 0 \Rightarrow a \otimes x \oplus a \otimes (-y) = 0 \Rightarrow a \otimes (x \oplus (-y)) = 0 \Rightarrow x \oplus (-y) = 0 \Rightarrow x = y$. Obrátené pravidlo podobne.

Veta 2.7.2.2.
Nech $(A, \oplus, \otimes)$ je okruh s aspoň dvoma prvkami, v ktorom platia obmedzené pravidlá o krátení. Potom A je obor integrity.

Dôkaz.
$\forall x,y \in A : x \otimes y = 0 \Rightarrow x \otimes y = x \otimes 0 \Rightarrow y = 0$.

Veta 2.7.2.3.
Každé teleso je obor integrity.

Dôkaz.
$\forall x,y \in A \; \exists x' \in A : x \otimes y = 0 \Rightarrow x' \otimes x \otimes y = x' \otimes 0 \Rightarrow y = 0$.

2.7.3. Podokruhy.

Definícia.
Okruh $(B, \oplus, \otimes)$ je *podokruh* okruhu $(A, +, *)$, ak $(B, \oplus)$ je podgrupa $(A, +)$ a $\forall x,y \in B : x \otimes y = x * y$.

Veta 2.7.3.1.
Okruh $(B, \oplus, \otimes)$ je podokruh okruhu $(A, +, *)$ práve vtedy, keď $\forall x,y \in B : x \oplus (-y) \in B \wedge x \otimes y \in B$.

Dôkaz.
Obdobne ako pre podgrupy.

Veta 2.7.3.2.
Nech $\{B_i\}_{i \in 1..n}$ je systém podokruhov A. Potom aj $\bigcap_{i=1}^{n} B_i$ je podokruh A.

Dôkaz.
Triviálne.

Veta 2.7.3.3.
Nech A je okruh a $M \subseteq A$. Potom existuje jediný podokruh $[[M]]$ okruhu A taký, že $M \subseteq [[M]]$ a $\forall B \subseteq A : B$ je podokruh $A \Rightarrow B \subseteq [[M]]$.

Dôkaz.
$[[M]]$ je prienik všetkých podokruhov A, obsahujúcich M. Z vlastnosti $\forall B \subseteq A : B$ je podokruh $A \Rightarrow B \subseteq [[M]]$ vyplýva, že $[[M]]$ je jediný.

Definícia.

Nech A je okruh a $M \subseteq A$. Okruh $[[M]]$, ktorého existenciu zabezpečuje veta 2.7.3.3, nazývame podokruh *generovaný* množinou M. Prvky M sú *generátory* okruhu $[[M]]$.

Veta 2.7.3.4.

Nech A je okruh a nech $M \subseteq A$ obsahuje jednotku. Ak $\exists a \in A\ \forall x \in A : a \otimes x = x \otimes a$, tak okruh $[[M \cup \{a\}]]$, ktorého existenciu zabezpečuje veta 2.7.3.3, má tvar $\{x_0 \otimes a^0 \oplus \ldots \oplus x_n \otimes a^n;\ \forall i \in 1..n: x_i \in A\}$ a označujeme ho $M[a]$.

Dôkaz.

$M[a] \supseteq M$, lebo $\forall x \in M : x = x \otimes a^0 = x \otimes e$. $\forall x = x_0 \otimes a^0 \oplus \ldots \oplus x_n \otimes a^n,\ y = y_0 \otimes a^0 \oplus \ldots \oplus y_n \otimes a^n \in M[a] : (x - y) = (x_0 - y_n) \otimes a^0 \oplus \ldots \oplus (x_n - y_n) \otimes a^n \in M[a]$. Podobne možno odvodiť, že $(x \otimes y) \in M[a]$, takže $M[a]$ je podokruh A. A napokon aj $M[a] \subseteq [[M]]$, lebo minimálny podokruh musí všetky prvky tvaru prvkov z $M[a]$ obsahovať.

Definícia.

Nech A je okruh a nech $M \subseteq A$. Okruh $M[a]$, ktorého existenciu zabezpečuje veta 2.7.3.4, nazývame *okruh polynómov* v premennej a pod M.

2.7.4. Homomorfizmy a ideály okruhov.

Definícia.

Nech $(A, \oplus, \otimes)$ je okruh. Zobrazenie $f : A \to A$ nazveme *homomorfizmus okruhov* (krátene homomorfizmus), ak je homomorfizmom vzhľadom na obe operácie $\oplus$ a $\otimes$.

Veta 2.7.4.1.

Nech A,B a C sú okruhy a zobrazenia $f : A \to B$ a $g : B \to C$ homomorfizmy. Potom aj $g \circ f : A \to C$ je homomorfizmus.

Dôkaz.

Tvrdenie vyplýva priamo z vety o zloženom homomorfizme grúp.

Definícia.

Nech $(A, \oplus, \otimes)$ je okruh. $\emptyset \neq I \subseteq A$ je *ideál*, ak

1. $\forall x, y \in I : (x - y) \in I$
2. $\forall x \in I\ \forall r \in A : x \otimes r \in I \wedge r \otimes x \in I$.

Veta 2.7.4.2.

Nech A a B sú okruhy a zobrazenie $f : A \to B$ homomorfizmus. Potom $Ker(f)$ je ideál A.

Dôkaz.

$\forall x, y \in Ker(f) : f(x - y) = f(x) - f(y) = 0 + 0 = 0 \in Ker(f)$. Zároveň $\forall r \in A : f(x \otimes r) = f(x) * f(r) = 0 * f(r) = 0$. Obdobne $f(r \otimes x)$.

Veta 2.7.4.3.

Nech A' je podokruh A a B' podokruh B. Ak $f : A \to B$ je homomorfizmus, tak $f(A') = \{f(x) \in B;\ x \in A'\}$ je podokruh B a $f^{-1}(B') = \{x \in A;\ f(x) \in B'\}$ je podokruh A.

Dôkaz.

$\forall f(x), f(y) \in f(A') : f(x) * f(y) = f(x \otimes y) \in f(A')$, lebo A' je okruh. Podobne $\forall x, y \in f^{-1}(B') : f(x \otimes y) = f(x) * f(y) \in B'$, lebo B' je okruh.

Veta 2.7.4.4.

Nech A,B sú okruhy a I je ideál B. Ak $f : A \to B$ je homomorfizmus, tak $f^{-1}(I) = \{x \in A;\ f(x) \in I\}$ je ideál A.

Dôkaz.

Podľa vety 2.7.4.3 je $f^{-1}(I)$ podokruh A. Navyše $\forall x \in f^{-1}(I)\ \forall r \in A : f(r \otimes x) = f(r) * f(x) \in I$, lebo I je ideál.

Veta 2.7.4.5.

Nech $\{I_i\}_{i \in 1..n}$ je systém ideálov A. Potom aj $\bigcap_{i=1}^{n} I_i$ je ideál A.

Dôkaz.

Triviálne.

Veta 2.7.4.6.

Nech A je okruh a $I \subseteq A$. Potom existuje jediný ideál (I) okruhu A taký, že $I \subseteq (I)$ a $\forall J \subseteq A : J$ je ideál $A \Rightarrow J \subseteq (I)$.

Dôkaz.

Obdobne ako pre okruhy.

Definícia.

Nech A je okruh a $I \subseteq A$. Okruh (I), ktorého existenciu zabezpečuje veta 2.7.3.3, nazývame ideál *generovaný* množinou I. Prvky I sú *generátory* okruhu (I).

Veta 2.7.4.7.

Nech A je komutatívny okruh, $a \in A$. Potom $(a) = \{r \otimes a \oplus n.a;\ r \in A, n \in Z\}$. Ak $1 \in A$, tak $(a) = \{r \otimes a;\ r \in A\}$.

Dôkaz.

$\forall x = p \otimes a \oplus m.a,\ y = r \otimes a \oplus n.a \in (a) : x - y = (p-r) \otimes a \oplus (m-n).a$ a $\forall s \in A : r \otimes x = r \otimes (p \otimes a \oplus m.a) = (p \otimes s) \otimes a \oplus (n.s).a \in (a)$, takže (a) je ideál A. Navyše $a \in (a)$ a každý ideál A, obsahujúci a musí obsahovať všetky prvky A tvaru prvkov (a), takže (a) je minimálny.

2.7.5. Faktorové okruhy.

Veta 2.7.5.1.

Nech I je ideál A. Potom existujú jediné operácie $\oplus$, $\otimes$ také, že $(A|_I, \oplus, \otimes)$ je okruh a zobrazenie $f : A \to A|_I$ s predpisom $f(a) = a+I$ komutatívny homomorfizmus.

Dôkaz.

Definujme operáciu $\oplus$ predpisom $\forall x,y \in A : (x+I) \oplus (y+I) = (x \oplus y)+I$ a operáciu $\otimes$ predpisom $\forall x,y \in A : (x+I) \otimes (y+I) = (x \otimes y)+I$ (kde $+$, $*$ sú operácie okruhu A). $(A, +)$ je komutatívna grupa, I je jej invariantná podgrupa a teda aj $(A|_I, \oplus)$ je komutatívna grupa a f homomorfizmus. Navyše $\forall x,y,z \in A : (x+I) \otimes ((y+I) \otimes (z+I)) = (x+I) \otimes (y \otimes z+I) = (x \otimes y \otimes z+I) = (x \otimes y+I) \otimes (z+I) = ((x+I) \otimes (y+I)) \otimes (z+I)$ a $(x+I) \otimes ((y+I) \oplus (z+I)) = (x+I) \otimes ((y \oplus z)+I) = (x \otimes (y \oplus z)+I) = ((x \otimes y) \oplus (x \otimes z)+I) = ((x \otimes y)+I) \oplus ((x \otimes z)+I)$, takže $(A|_I, \oplus, \otimes)$ je okruh.

Veta 2.7.5.2.

nech $f : A \to B$ je surjektívny homomorfizmus. Potom existuje jediný izomorfizmus $g : A|_{Ker(f)} \to B$ taký, že $f = g \circ p$, kde p je projekcia zaručená vetou 2.7.5. .

Dôkaz.

Dôkaz podobný ako pre vetu 2.5.9.2.

2.8. Polia.

2.8.1. Podpole.

Veta 2.8.1.1.

Nech F je pole. Potom $\emptyset \neq F' \subseteq F$ je podpole F práve vtedy, keď

1. $1 \in F'$
2. $\forall x,y \in F' : (x-y) \in F'$
3. $\forall x,y \in F' : x * y^{-1} \in F'$.

Dôkaz.

Dopredná implikácia je triviálna. Z vlastnosti 2. vyplýva, že $(F', +)$ je podgrupa $(F, +)$. Podobne z vlastností 1. a 3. vyplýva, že $(F', *)$ je pologrupa. Spolu teda $(F', +, *)$ je okruh a z vlastnosti 3. vyplýva, že je to aj pole.

Definícia.

Ideál I okruhu A sa nazýva *maximálny*, ak $I \subset A$ a $\forall$ ideál $J : J \supset I \Rightarrow J = A$.

Veta 2.8.1.2.

Nech A je komutatívny okruh s jednotkou, I je ideál A. Potom $A|_I$ je pole práve vtedy, keď I je maximálny.

Dôkaz.

Nech $A|_I$ je pole. Potom má aspoň 2 prvky. I je nula v $A|_I$ a $1+I$ jednotka. $1 = 1 - 0 \notin I \Rightarrow I \neq A$. Nech teraz $\exists$ideál $J \supset I$, $J \neq A$. Potom $\exists x \in J : x \notin I$. Položme $K = \{i + r.x;\ i \in I,\ r \in A\}$. Ľahko možno odvodiť, že K je ideál v A. Ale každý prvok tavru prvkov K musí byť v minimálnom ideáli, generovanom $I \cup \{x\}$, takže $K = (I \cup \{x\})$ a $J \supseteq K$. Ale $1 = 1 + 0.\ x \in K$, takže $K = A$ a teda aj $J = A$, čo znamená, že I bol maximálny.

Obrátene nech I je maximálny. Potom $A|_I$ má aspoň 2 prvky. $\forall x \notin I : (I \cup \{x\}) = A \Rightarrow 1 \in (I \cup \{x\})$. Keďže sme ukázali, že $(I \cup \{x\}) = \{i + r.x;\ i \in I,\ r \in A\}$, $\exists i \in I\ \exists r \in A : 1 = i + r.\ x$. Potom ale trieda $1+I = (i + r.\ x)+I = (i+I) + (r.\ x)+I = (\forall i \in I : (i+I) = I) = (r+I) * (x+I) \Rightarrow *$ má inverzný prvok. Ostatné vlastnosti poľa sú zaručené zo zadania, čiže $A|_I$ je pole.

2.8.2. Podielové pole.

Veta 2.8.2.1.

Nech A je komutatívny obor integrity. Potom existuje pole $Q(A)$ a injektívny homomorfizmus $j : A \to Q(A)$ tak, že

1. $\forall x \in Q(A)\ \exists a,b \in A : b \neq 0 \wedge x = j(a) * j(b)^{-1}$
2. $\forall$injektívny homomorfizmus $f : A \to F$, kde F je pole, existuje jediný homomorfizmus $g : Q(A) \to F$ tak, že $f = g \circ j$.

Dôkaz.

Položme $B = A \times A^*$, kde $A^* = A - \{0\}$. Na B definujme reláciu $\sim$ predpisom $(a, b) \sim (c, d) \Leftrightarrow a*d = b*c$, kde $*$ je násobenie v okruhu A. $\sim$ je zjavne symetrická a reflexívna. Navyše $(a, b) \sim (c, d) \wedge (c, d) \sim (x, y) \Leftrightarrow a*d = b*c \wedge c*y = d*x \Leftrightarrow a*d*y = b*c*y \wedge b*c*y = b*d*x \Leftrightarrow a*d*y = b*d*x \Leftrightarrow a*y = b*x \Leftrightarrow (a, b) \sim (x, y)$, takže $\sim$ je aj tranzitívna a teda je to relácia ekvivalencie. Definujme $Q(A) = B|_\sim$. Triedu ekvivalencie, do ktorej patrí (a, b), označím $\frac{a}{b}$. Ďalej definujme operácie $\oplus$ a $\otimes$ predpismi $\frac{a}{b} \oplus \frac{c}{d} = \frac{a*d + b*c}{b*d}$ a $\frac{a}{b} \otimes \frac{c}{d} = \frac{a*c}{b*d}$. Ukážeme, že $(Q(A), \oplus, \otimes)$ je pole.

I. <u>Nezávislosť označenia tried ekvivalencie od výberu reprezentantov.</u> $\frac{a}{b} \sim \frac{a'}{b'}$ a $\frac{c}{d} \sim \frac{c'}{d'} \Leftrightarrow a*b' = a'*b \wedge c*d' = c'*d \Leftrightarrow a*b'*d*d' = a'*b*d*d' \wedge c*d'*b*b' = c'*d*b*b' \Leftrightarrow a*b'*d*d' + c*d'*b*b' = a'*b*d*d' + c'*d*b*b' \Leftrightarrow a*d*b'*d' + b*c*b'*d' = a'*d'*b*d + b'*c'*b*d \Leftrightarrow (a*d + b*c)*b'*d' = (a'*d' + b'*c')*b*d \Leftrightarrow \frac{a*d + b*c}{b*d} = \frac{a'*d' + b'*c'}{b'*d'} \Leftrightarrow \frac{a}{b} \oplus \frac{c}{d} = \frac{a'}{b'} \oplus \frac{c'}{d'}$. Podobne $\frac{a}{b} \sim \frac{a'}{b'}$ a $\frac{c}{d} \sim \frac{c'}{d'} \Leftrightarrow a*b' = a'*b \wedge c*d' = c'*d \Leftrightarrow a*b'*c*d' = a'*b*c'*d \Leftrightarrow a*c*b'*d' = a'*c'*b*d \Leftrightarrow \frac{a*c}{b*d} = \frac{a'*c'}{b'*d'} \Leftrightarrow \frac{a}{b} \otimes \frac{c}{d} = \frac{a'}{b'} \otimes \frac{c'}{d'}$.

II. <u>Komutatívnosť $\oplus$</u>. $\frac{a}{b} \oplus \frac{c}{d} = \frac{a*d + b*c}{b*d} = \frac{c*b + d*a}{d*b} = \frac{c}{d} \oplus \frac{a}{b}$.

III. <u>Neutrálny prvok $\oplus$</u> (nula). Nulou v $Q(A)$ je trieda $\frac{0}{x}$, $x \neq 0$. $\frac{a}{b} \oplus \frac{0}{x} = \frac{0*b + x*a}{x*b} = \frac{a}{b}$.

IV. <u>Inverzný prvok $\oplus$</u>. Položme $-\left(\frac{a}{b}\right) = \frac{-a}{b}$. Potom $\frac{a}{b} \oplus \frac{-a}{b} = \frac{a*b - b*a}{b*b} = \frac{0}{b*b}$.

V. <u>Komutatívnosť $\otimes$</u>. $\frac{a}{b} \otimes \frac{c}{d} = \frac{a*c}{b*d} = \frac{c*a}{d*b} = \frac{c}{d} \otimes \frac{a}{b}$.

VI. <u>Neutrálny prvok $\otimes$</u> (jednotka). Jednotkou v $Q(A)$ je trieda $\frac{x}{x}$, $x \neq 0$. $\frac{a}{b} \otimes \frac{x}{x} = \frac{a*x}{b*x} = \frac{a}{b}$.

VII. <u>Inverzný prvok $\otimes$</u>. Položme $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. Potom $\frac{a}{b} \otimes \left(\frac{a}{b}\right)^{-1} = \frac{a}{b} \otimes \frac{b}{a} = \frac{a*b}{b*a} = (a*b = x) = \frac{x}{x}$.

VIII. Distributívnosť $\otimes$ vzhľadom na $\oplus$. $\frac{x}{y} \otimes \left(\frac{a}{b} + \frac{c}{d}\right) = \frac{x}{y} \otimes \frac{a*d+b*c}{b*d} = \frac{x*(a*d+b*c)}{x*b*d} = \frac{x*a*d+x*b*c}{x*b*d} = \frac{x*a*d}{x*b*d} \oplus \frac{x*b*c}{x*b*d} = \frac{a}{b} \oplus \frac{c}{d}$.

Tým sme dokázali, že $Q(A)$ je pole. Teraz zvoľme pevné $\neq x \in A$ a definujme $j : A \to Q(A)$ predpisom $j(a) = \frac{a*x}{x}$. $j(a+b) = \frac{(a+b)*x}{x} = \frac{a*x+b*x}{x} = \frac{a*x}{x} \oplus \frac{b*x}{x} = j(a) \oplus j(b)$ a rovnako $j(a*b) = \frac{a*b*x}{x} = \frac{a*x*b*x}{x*x} = \frac{a*x}{x} \otimes \frac{b*x}{x} = j(a) \otimes j(b)$, takže j je homomorfizmus. Navyše $j(a)=j(b) \Rightarrow \frac{a*x}{x} = \frac{b*x}{x} \Rightarrow a*x*x = b*x*x \Rightarrow a = b$, takže j je injekcia.

Majme teraz pole F a injektívny homomorfizmus $f : A \to F$. Pre f definujme zobrazenie $g : Q(A) \to F$ predpisom $g\left(\frac{a}{b}\right) = f(a).f(b)^{-1}$, kde . je násobenie v poli F. $\frac{a}{b} \sim \frac{a'}{b'} \Rightarrow a*b' = a'*b \Rightarrow f(a*b') = f(a'*b) \Rightarrow f(a).f(b') = f(a').f(b) \Rightarrow f(a).f(b)^{-1} = f(a').f(b')^{-1} \Rightarrow g\left(\frac{a}{b}\right) = g\left(\frac{a'}{b'}\right)$, takže g je nezávislé od výberu reprezentantov. Navyše $g\left(\frac{a}{b} \oplus \frac{c}{d}\right) = g\left(\frac{a*d+b*c}{b*d}\right) = f(a*d + b*c).f(b*d)^{-1} = f(a*d).f(b*d)^{-1} + (b*c).f(b*d)^{-1} = f(a).f(d).f(b)^{-1}.f(d)^{-1} + f(b).f(c).f(b)^{-1}.f(d)^{-1} = f(a).f(b)^{-1} + f(c).f(d)^{-1} = g\left(\frac{a}{b}\right) + g\left(\frac{c}{d}\right)$ a $g\left(\frac{a}{b} \otimes \frac{c}{d}\right) = g\left(\frac{a*c}{b*d}\right) = f(a*c).f(b*d)^{-1} = f(a).f(c).f(b)^{-1}.f(d)^{-1} = f(a).f(b)^{-1}.f(c).f(d)^{-1} = g\left(\frac{a}{b}\right).g\left(\frac{c}{d}\right)$, takže g je homomorfizmus. Pritom $g \circ j(a) = g(j(a)) = g\left(\frac{a*x}{x}\right) = f(a*x).f(x)^{-1} = f(a).f(x).f(x)^{-1} = f(a)$, takže $g \circ j = f$.

Jednoznačnosť g. Nech $g_1 \circ j = f \wedge g_2 \circ j = f$. Potom $g_1\left(\frac{a*x}{x}\right) = f(a) \wedge g_2\left(\frac{a*x}{x}\right) = f(a) \Rightarrow g_1\left(\frac{a*x}{x}\right) = g_2\left(\frac{a*x}{x}\right)$ a teda $g_1 = g_2$.

Veta 2.8.2.2.

Nech A_1, A_2 sú izomorfné komutatívne obory integrity. Potom aj $Q(A_1)$ a $Q(A_2)$ sú izomorfné.

Dôkaz.

Majme izomorfizmus $f : A_1 \to A_2$ a injektívne homomorfizmy $j_1 : A_1 \to Q(A_1)$ a $j_1 : A_2 \to Q(A_2)$. Potom podľa vety 2.8.1.1 existuje jediný homomorfizmus $g_1 : Q(A_1) \to Q(A_2)$ taký, že $g_1 \circ j_1 = j_2 \circ f$, ktorý je navyše injektívny, lebo aj j_1, j_2 aj f sú injektívne. Podobne existuje a je injektívny aj homomorfizmus $g_2 \circ j_2 : Q(A_2) \to Q(A_1) = j_1 \circ f^{-1}$. Potom ale $g_1 \circ g_2$ aj $g_2 \circ g_1$ sú bijektívne automorfizmy, z čoho vyplýva, že $Q(A_1)$ a $Q(A_2)$ sú izomorfné.

2.9. Okruhy polynómov.

2.9.1. Konštrukcia polynómov.

Definícia.

Nech $A \subset B$, $x \in B$. Množinu $A[x] = \{\sum_{k=0}^{n} a_k x^k ; \forall i \in 0..n : a_i \in A\}$ nazývame *okruh polynómov* v premennej x s koeficientami v A.

Definícia.

Nech $A \subset B$, $x \in B$ Ak každý polynóm v x s koeficientami va A je nulový len vtedy, keď všetky jeho koeficienty sú nulové, tak x nazývame *transcendentný* prvok nad A. Inak je x *algebraický*.

Veta 2.9.1.1 (Dosadzovacie pravidlo).

Nech $A \subset B$ a $A' \subset B'$ sú okruhy a nech $x \in B$ je transcendentný nad A. Ak $\forall a \in A : ax = xa$ a $\exists y \in B' \ \forall v \in B'$: $by = yb$, potom ku každému homomorfizmu $f : A \to A'$ existuje jediný homomorfizmus $\varphi : A[x] \to B'$ taký, že $\forall a \in A : \varphi(a) = f(a)$ a $\varphi(x) = y$.

Dôkaz.

$A[x] = \{ \sum_{k=0}^{n} a_k x^k \ ; \ \forall i \in 0..n \ : \ a_i \in A \}$. Definujme φ predpisom $\varphi\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} f(a_k) y^k$. Ľahko možno nahliadnuť, že φ je práve hľadaný homomorfizmus.

Definícia.

Polynóm $\sum_{k=0}^{n} a_k x^k$ je *invertovateľný*, ak $\exists a : aa_0 = a_0 a = 1$.

Označenie.

Stupeň polynómu f označíme Δf.

Veta 2.9.1.2 (O delení so zvyškom).

Nech A je komutatívny okruh s jednotkou, x je transcendentný nad A a nech $f(x) = \sum_{k=0}^{n} a_k x^k$ a $g(x) = \sum_{k=0}^{m} b_k x^k \in A[x]$, pričom g je invertovateľný. Potom existuje jediná usporiadaná dvojica polynómov $q(x)$, $r(x) \in A[x]$ taká, že $f(x) = g(x)q(x) + r(x)$, kde $0 \le n < m$ ($\Delta r(x) = n$ a $\Delta g(x) = m$).

Dôkaz.

Ak $m > n$, tak $f = 0.g + f$. Nech teraz $n \ge m$. Položme $f_1(x) = f(x) - \frac{a_0}{b_0} x^{n-m} . g(x)$. Je zrejmé, že $f_1(x)$ je menšieho stupňa, než $f(x)$ a preto podľa indukčného prepokladu $\exists q', r' : f_1 = q'.g + r'$. Ale potom $f(x) = \left(q'(x) + \frac{a_0}{b_0} x^{n-m} \right) g(x) + r(x)$, kde $r(x) = r'(x)$ + zvyšné členy z $f_1(x)$. jednoznačnosť je zjavná, lebo ak $f(x) = q(x).g(x) + r(x) = q'(x).g(x) + r'(x)$, tak $r(x) - r'(x) = \left(q(x) - q'(x)\right).g(x)$. Ale ľavá strana je stupňa menšieho ako m a pravá stupňa aspoň m, takže obe sú nulové a teda $q(x) = q'(x)$ a $r(x) = r'(x)$.

Definícia.

Hovoríme, že polynóm f *delí* polynóm g a zapisujeme f/g, ak existuje polynóm h taký, že $g = f.h$.

Lema 2.9.1.1.

Nech f/g a g/h. Potom f/h.

Dôkaz.

Triviálne.

Lema 2.9.1.2.

Nech f/g a f/h. Potom $f/(g+h)$.

Dôkaz.

Triviálne.

Definícia.

Hovoríme, že polynóm h je *najväčší spoločný deliteľ* polynómov f a g a zapisujeme $h = (f,g)$, ak h/f, h/g a $\forall h' : h'/f \wedge h'/g \Rightarrow h/h'$. Ak f/g a g/f, hovoríme, že f a g sú *asociované*.

Lema 2.9.1.3.

Nech $f = q.g + r$. Potom $(f,g) = (g,r)$.

Dôkaz.

Nech $h/f \wedge h/g$. Potom ale h/r, lebo $r = f - q.g$. Obrátene nech $k/g \wedge k/r$. Potom k/f, lebo $f = q.g + r$. Takže každý spoločný deliteľ f a g je aj spoločným deliteľom g a r a naopak, z čoho vyplýva dokazované tvrdenie.

Veta 2.9.1.3 (Euklidov algoritmus).

Ak $F[x]$ je pole, tak $\forall f,g \in F[x] \ \exists (f,g)$.

Dôkaz.
Tvrdenie induktívne vyplýva z lemy 2.9.1.3.

Veta 2.9.1.4.
Ak $F[x]$ je pole, tak každý ideál $F[x]$ je hlavný.

Dôkaz.
Nech I je ideál v $F[x]$. Prípady $I = \{0\} = (0)$ a $I = F[x] = (1)$ sú triviálne. Preto nech $\{0\} \subset I \subset F[x]$. Položme $\Delta = \min\{\Delta f(x); f(x) \in I\}$. Nech $f \in I$ je stupňa Δ. Je zjavné, že $I \supseteq (f(x))$. Obrátene nech $I \ni k(x) = q(x).g(x) + r(x)$. Ale Δr nemôže byť nenulová a menšia ako Δf, takže $r(x) = 0$ a $k(x) = q(x).g(x) \in (f(x))$.

2.9.2. Okruhy hlavných ideálov.

Definícia.
Komutatívny obor integrity, v ktorom je každý ideál hlavný, nazývame *okruh hlavných ideálov* a označujeme skratkou *OHI*.

Veta 2.9.2.1.
Nech A je *OHI* a $I_0 \subseteq .. \subseteq I_n \subseteq ..$ je postupnosť ideálov A. Potom $\exists n \in N\ \forall m > n : I_m = I_n$.

Dôkaz.
Stačí ukázať, že $J = \bigcup_{I \in A} I$ je ideál v A. Ale $\forall a,b \in J\ \exists n,m \in N : a \in I_n \wedge b \in I_m$. BUNV nech $n \geq m$. Potom $a,b \in I_n \Rightarrow a\text{-}b \in I_n \Rightarrow a\text{-}b \in J$. Podobne $\forall r \in A\ \forall a \in J\ \exists n \in N : a \in I_n \Rightarrow ar \in I_n \Rightarrow ar \in J$, takže J je ideál v $A \Rightarrow \exists n \in N : I_n = J$ a $\forall m \geq n : I_m \supseteq I_n \Rightarrow I_m = J$.

Definícia.
Nech A je okruh, $a,b \in A$. Hovoríme, že a *delí* b v A a zapisujeme a/b, ak $\exists c \in A : b = c.a$.

Lema 2.9.2.1.
Nech A je *OHI*, $a,b,c \in A$. Potom $a/b \wedge b/c \Rightarrow a/c$.

Dôkaz.
Triviálne.

Lema 2.9.2.2.
Nech A je *OHI*, $a,b,c \in A$. Potom $a/b \wedge a/c \Rightarrow a/bc$.

Dôkaz.
$b = d_1 a \wedge c = d_2 a \Rightarrow bc = d_1 a d_2 a = (d_1 d_2 a)a$.

Definícia.
Nech A je *OHI*, $a,b \in A$. Ak a/b a b/a, hovoríme, že a a b sú *asociované* a píšeme $a \sim b$.

Lema 2.9.2.3.
Nech A je *OHI*, $a,b \neq 0 \in A$, $a \sim b$. Potom existuje deliteľ jednotky c taký, že $b = ca$.

Dôkaz.
$a = d_1 b = d_1 d_2 a \Rightarrow d_1 d_2 = 1 \Rightarrow d_1$ aj d_2 sú delitele jednotky.

Definícia.
Nech A je *OHI*, $a \in A$. Ak a je deliteľný iba deliteľmi jednotky a prvkami s ním asociovanými, tak hovoríme, že a je *ireducibilný*.

Veta 2.9.2.2.
Nech A je *OHI*, $a,b \in A$. Potom $\exists (a,b)$.

Dôkaz.
Položme $I = \{pa + qb; p,q \in A\}$. I je zjavne ideál v A a keďže A je *OHI*, $\exists c \in A : I = (a)$. Ale potom $\exists p,q \in A : c = pa + qb$ a teda $c = (a,b)$.

Lema 2.9.2.4.
Nech A je *OHI*, $a,b,c \in A$. Ak $(a,b) = 1$ a a/bc, tak a/c.

Dôkaz.
Triviálne.

Dôsledok 2.9.2.1.

Nech A je *OHI*, $a,b,c \in A$. Ak a je ireducibilný a a/bc, tak $a/b \vee a/c$.

Dôkaz.

Triviálne.

Veta 2.9.2.3 (Rozklad na prvočísla).

Nech A je *OHI* a $0 \neq a \in A$ nie je deliteľ jednotky. Potom a možno až na poradie členov jednoznačne vyjadriť ako súčin ireducibilných $p_1..p_n \in A$.

Dôkaz.

Triviálnou štrukturálnou indukciou dostaneme rozklad a na ireducibilné prvky. Jednoznačnosť rozkladu vyplýva z dôsledku 2.9.2.1.

Dôsledok 2.9.2.2.

Nech A je *OHI* a $0 \neq a \in A$ nie je deliteľ jednotky. Potom a možno jednoznačne vyjadriť ako $\prod_{p \in \{q \in A;\, q \text{ je ireducibilný}\}} p^{\alpha_p}$, kde $\alpha_p \geq 0$.

Dôkaz.

Triviálne.

Veta 2.9.2.4.

Nech A je *OHI*, $a = \prod_{p \in A} p^{\alpha_p}, b = \prod_{p \in A} p^{\beta_p} \in A$. Potom $(a,b) = c = \prod_{p \in A} p^{\min\{\alpha_p, \beta_p\}}$.

Dôkaz.

c je zjavne spoločný deliteľ a a b. Navyše ak $d = \prod_{p \in A} p^{\gamma_p}$ je spoločný deliteľ a a b, tak $\forall p \in A$ ireducibilné platí $\gamma_p \geq \min\{\alpha_p, \beta_p\}$, takžd c/d.

Definícia.

Nech A je *OHI*, $a,b \in A$. Číslo $[a,b]$ nazývame *najmenším spoločným násobkom* a a b, ak $a/[a,b]$, $b/[a,b]$ a $\forall c \in A : a/c,\ b/c \Rightarrow [a,b]/c$.

Veta 2.9.2.5.

Nech A je *OHI*, $a = \prod_{p \in A} p^{\alpha_p}, b = \prod_{p \in A} p^{\beta_p} \in A$. Potom $[a,b] = c = \prod_{p \in A} p^{\max\{\alpha_p, \beta_p\}}$.

Dôkaz.

c je zjavne spoločný násobok a a b. Navyše ak $d = \prod_{p \in A} p^{\gamma_p}$ je spoločný násobok a a b, tak $\forall p \in A$ ireducibilné platí $\gamma_p \leq \max\{\alpha_p, \beta_p\}$, takžd d/c.

2.9.3. Korene polynómov.

Definícia.

Nech F je pole, x je transcendentný nad F a $f(x) = \sum_{k=0}^{n} a_k x^k \in F[x]$. Polynóm $Df(x) = f'(x) = \sum_{k=0}^{n} (k \times a_k) x^{k-1}$ nazývame *derivácia* polynómu $f(x)$.

Veta 2.9.3.1.

Nech F je pole, x je transcendentný nad F a $f(x), g(x) \in F[x]$. Potom $(f(x) + g(x))' = f'(x) + g'(x)$.

Dôkaz.

Nech $f(x) = \sum_{k=0}^{n} a_k x^k$ a $g(x) = \sum_{k=0}^{n} b_k x^k$. $(f+g)(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$, $(f+g)'(x) = \sum_{k=0}^{n} k \times (a_k + b_k) x^{k-1}$ $= \sum_{k=0}^{n} (k \times a_k) x^{k-1} + (k \times b_k) x^{k-1} = \sum_{k=0}^{n} (k \times a_k) x^{k-1} + \sum_{k=0}^{n} (k \times b_k) x^{k-1} = f'(x) + g'(x)$.

Veta 2.9.3.2.

Nech F je pole, x je transcendentný nad F a $f(x), g(x) \in F[x]$. Potom $fg'(x) = f'(x)\, g(x) + f(x) g'(x)$.

Dôkaz.

Nech $f(x) = \sum_{i=0}^{n} a_i x^i$ a $g(x) = \sum_{j=0}^{n} b_j x^j$. Potom $fg(x) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j x^{i+j}$ a $fg'(x) = \sum_{i=0}^{n}\sum_{j=0}^{n}(i+j)a_i b_j x^{i+j-1} = \sum_{i=0}^{n}\left(i.a_i x^{i-1}\sum_{j=0}^{n} b_j x^j + a_i x^i \sum_{j=0}^{n} b_j x^{j-1}\right) = \sum_{i=0}^{n}\left(i.a_i x^{i-1}\sum_{j=0}^{n} b_j x^j\right) + \sum_{i=0}^{n}\left(a_i x^i \sum_{j=0}^{n} b_j x^{j-1}\right) = \sum_{i=0}^{n} i.a_i x^{i-1}.\sum_{j=0}^{n} b_j x^j + \sum_{i=0}^{n} a_i x^i.\sum_{j=0}^{n} b_j x^{j-1} = f'(x).g(x) + f(x).g'(x).$

Definícia.

Nech F je pole, F' je nadpole F, $x \in F'$ je transcendentný nad F a $f(x) \in F[x]$ r m $\Delta f \geq 1$ H r m $c \in F'$ je *koreň* polynómu $f(x)$, ak $(x-c)/f(x)$ v $F[x]$.

Veta 2.9.3.3.

Nech F je pole, F' je nadpole F, $x \in F'$ je transcendentný nad F a $f(x) \in F[x]$ r m $\Delta f \geq 1$. $c \in F'$ r ň $f(x)$ r y ď $f(c) = 0$.

Dôkaz.

$f(x) = (x-c)q(x) + r(x)$. Ak c r ň $f(x)$, tak $r(x) = 0$ a $f(c) = (c-c)q(c) = 0$. Obrátene tak isto.

Veta 2.9.3.4.

Ak $f(x) \in C[x]$ je ireducibilný, tak $\Delta f \leq 1$.

Dôkaz.

V $C[x]$ m y óm u ň n práve n r ň

Lema 2.9.3.1.

$f(x) \in R[x]$ m r y m g r ych r ň

Dôkaz.

Nech $a + bi = c \in C$ r ň $f(x)$. Potom $f(c) = 0$. Ale $R(a+bi)^k = R(a-bi)^k$ (z binomickej vety) a $I(a+bi)^k = -I(a-bi)^k$ $f(\bar{c}) = 0$ a $f(x) = (x-c)(x-\bar{c})q(x)$.

Veta 2.9.3.5.

Ak $f(x) \in R[x]$ je ireducibilný, tak $\Delta f \leq 2$.

Dôkaz.

Ak $f(x)$ m r y r ň c, tak $f(x) = (x-c)q(x)$ A m m ň m g r r c a $\bar{c}$ a $f(x) = (x-c)(x-\bar{c})q(x) = ((x-a)^2 + b^2)q(x)$.

Veta 2.9.3.6.

Nech $f(x) \in F[x]$ u ň 2 3 P m $f(x)$ r uc r y ď m r y r ň

Dôkaz.

Dopredná implikácia je triviálna. Obrátene nech $f(x)$ m r y r ň P m m ň m g r r N yš y u ň 3 mu y ľ my 2 9 3 1 yť h r m x r ň r y r f u ň r r ú m h ch m g r ych r ň r uc

Definícia.

H r m c je *viacnásobný* (k-) r ň $f(x)$, ak $(x-c)^k / f(x)$ v $F[x]$.

Definícia.

Pole F sa nazýva *úplné* (uzavreté), ak $\forall f(x) \in F[x] : \Delta f(x) \geq 1 \Rightarrow f(x)$ má v $F[x]$ r ň

Veta 2.9.3.7.

Nech F' je úplné nadpole F. Polynóm $f(x) \in F[x]$ má v F' ň r ň r y ď $\Delta(f(x), Df(x)) \geq 1$.

Dôkaz.

Nech $f(x)$ má v F' dvojnásobný k r ň c. Potom $f(x) = (x-c)^2 g(x)$. $Df(x) = (x-c)^2 Dg(x) + 2(x-c)g(x) \Rightarrow (x-c)/(f(x), Df(x)) \Rightarrow \Delta(f(x), Df(x)) \geq 1$. Obrátene nech $\Delta(f(x), Df(x)) \geq 1$. Potom $\exists d(x)$ u ň ň 1 r $(f(x), Df(x))$ K ď F' je úplné, $d(x)$ m r ň c. Aj $(x-c)/(f(x), Df(x))$. Nech $f(x) = (x-c)f_1(x)$ P ľ y 2 9 3 2 $Df(x) = f_1(x) + (x-c)Df_1(x) \Rightarrow (x-c)/f_1(x)$. Nech $f_1(x) = (x-c)f_2(x)$. Potom ale $f(x) = (x-c)^2 f_2(x)$ a teda $f(x)$ má v F' r ň

2.9.4. Algebraické rozšírenia polí.

Definícia.

Nadpole F' ľ F nazývame *rozšírenie* ľ F R š r ľ F je *algebraické*, ak všetky jeho prvky sú algebraické nad F.

Veta 2.9.4.1.

Nech F je pole, x je transcendentný nad F a $f(x) \in F[x]$ je ireducibilný. Potom existuje nadpole F' ľ F, v ktorom má $f(x)$ r ň

Dôkaz.

P m $I = (f(x))$. $\forall g(x) \in F[x]\text{-}(f(x)) : (f(x), g(x)) = 1 \Rightarrow \exists u(x), v(x) \in F[x] : u(x).f(x) + v(x).g(x) = 1$. Ale $u(x).f(x)$ aj $v(x).g(x) \in I$ $1 \in I \Rightarrow I$ je maximálny $\Rightarrow F' = F[x]|_I$ je pole. Definujme $\varphi : F \to F'$ predpisom $\forall a \in F : \varphi(a) = a + I$ Ľ h m h uť φ y h m m rf mu F je podpole F' (F je izomorfné s $\varphi(F) = \{a + I;\ a \in F\}$ a $\varphi(F)$ je podpole F'). Navyše $f(x + I) = \sum_{k=0}^{n} (a_k + I)(x + I)^k = \sum_{k=0}^{n} (a_k + I)(x^k + I) = \sum_{k=0}^{n} (a_k x^k + I) = \left(\sum_{k=0}^{n} a_k x^k\right) + I = f(x) + I = I$ (lebo $f(x) \in I$) $= 0$ $x + I$ r ň f v F'.

Definícia.

K r m r r r r ľ m F nazývame *konečné rozšírenie* ľ F. Jeho dimenziu nazývame *stupeň rozšírenia* u m $[F':F]$.

Veta 2.9.4.2.

K é é r š r ľ F je aj jeho algebraickým rozšírením.

Dôkaz.

Nech F' é r š r F, $[F':F] = k$ a $c \in F'$. Vektory $1, c, .., c^k$ ú r é $\exists \alpha_0..\alpha_k \in F : \sum_{k=1}^{n} \alpha_k c^k = 0$. Ale potom polynóm f, definovaný predpisom $f(x) = \sum_{k=1}^{n} \alpha_k c^k$ má v F' r ň

2.9.5. Konečné polia.

Definícia.

Charakteristika ľ F $char(F) = \min\{k \in N;\ k.1 = 0\}$.

Veta 2.9.5.1.

Nech F é ch r r y p. Potom $\exists n \in N : |F| = p^n$.

Dôkaz.

M $\{e^k\}_{k=0..p-1}$ je podpole F izomorfné so Z_p. F é r š r Z_p. Nech $[F : Z_p] = n$ a nech $\alpha_1..\alpha_n$ je báza v F. Potom ale zobrazenie $f : F \to Z_p^n$, definované predpisom $\forall x \in F : x = \sum_{k=1}^{n} \alpha_k c^k \Rightarrow f(x) = (\alpha_1, .., \alpha_n)$ je bijekcia a $|F| = |Z_p|^n = p^n$.

Veta 2.9.5.2.

Ak $(F, \oplus, \otimes)$ é $(F^*, \otimes)$ je cyklická grupa.

Dôkaz.

P ľ y 2 5 7 3 m hu ť gru y F^* m hu ť r éh r u F^* (rovný rádu podgrupy F^* generovanej jej prvkom) delí $q - 1$ K r F^* r ň m r c $x^{q-1} = 1$. Ak sa m r ť r c, ktorého rád je práve $q - 1$, budú mocniny c g r ť c ú F^* a F^* bude cyklická. Napíšme $q - 1$ ú r $q - 1 = \prod_{k=1}^{r} p_k^{e_k}$ K ď $\forall k \in 1..r : p_k^{e_k} \mid q-1$, všetky korene rovnice $x^{p_k^{e_k}} = 1$ r ňm r c $x^{q-1} = 1$ a patria do F Z r ň š $((x^q - 1), (x^q - 1)') = 1$ (lebo $(x^q - 1)' = q.x^{q-1} - 1 = -1$), š y r y ómu $x^{q-1} = 1$ (a teda aj $x^{p_k^{e_k}} = 1$) je rôznych. Spomedzi nich práve $p_k^{e_k - 1}$ r ň m rovnice $x^{p_k^{e_k - 1}} = 1$ x u r ň c_k rovnice $x^{p_k^{e_k}} = 1$ r r ň m r c $x^{p_k^{e_k - 1}} = 1$ Ľ h m h uť ú $c = \prod_{k=1}^{r} c_k$ hľ m r m r u $q - 1$.

Veta 2.9.5.3.

K é é r m m r ú m rf é

Dôkaz.

Nech $|F| = q = p^n$. Nenulové prvky F tvoria multiplikatívnu grupu F^* rádu $q - 1$. V dôkaze vety 2.9.5.2 m u r F^* r ň m r c $x^{q-1} = 1$ r $a_1 .. a_q$ ľ F (teda aj nula) r ň m r c $x^q - x = 0$ Z h y y óm $(x - a_1)..(x - a_q)$ ľ m y ómu $x^q - x$, lebo $\forall(x - a_i)$ sú ireducibilné a delia $x^q - x$ A y ómy ú rm é u ň q a teda $x^q - x = \prod_{k=1}^{q}(x - a_k)$ K é é m hu q yh u r m rf é F.

Veta 2.9.5.4.

Nech $F´$ é r š r F a $F´´$ é r š r $F´$. Potom $F´´$ é r š r F a $[F´´ : F] = [F´ : F][F´´ : F´]$.

Dôkaz.

Konštrukciou bázy $F´´$ nad F pomocou báz $F´´$ nad $F´$ a $F´$ nad F y r r u m

Veta 2.9.5.5 (Nedelbrunn).

K é é

Dôkaz.

Nedokazujeme.

2.10. Bilineárne a kvadratické formy.

2.10.1. Bilineárne formy.

Definícia.

Nech U, V, W ú r m r é r é r ry ľ m F. Zobrazenie $f : U \times V \to W$ nazývame *bilineárnym*, ak

1. $\forall x_1..x_n \in U\ \forall y \in V\ \forall \alpha_1..\alpha_n \in F : f\left(\sum_{k=1}^{n} \alpha_k x_k, y\right) = \sum_{k=1}^{n} f(\alpha_k x_k, y)$
2. $\forall x \in U\ \forall y_1..y_n \in V\ \forall \alpha_1..\alpha_n \in F : f\left(x, \sum_{k=1}^{n} \alpha_k y_k\right) = \sum_{k=1}^{n} f(x, \alpha_k y_k)$.

Ak $W = F$ h r m f je *bilineárna forma*.

Definícia.

Nech U a V ú r m r é r é r ry ľ m F a nech f je bilineárna forma $U \times V \to F$. Nech $\alpha_1..\alpha_n \in F$ je báza v U a $\beta_1..\beta_m \in F$ báza vo V. Maticu $A_{n \times m}$, definovanú predpisom $A(i,j) = f(\alpha_i, \beta_j)$, nazývame *matica bilineárnej formy* hľ m cu $\alpha_1..\alpha_n$ a $\beta_1..\beta_m$.

2.10.2. Charakteristické vektory a hodnoty matíc (bi)lineárnych zobrazení.

Definícia.

Nech V, W ú r m r é r é r ry ľ m F a $f : V \to W$ je lineárne r $c \in F$ nazývame *charakteristickou* (*vlastnou*) *hodnotou* zobrazenia f, ak $\exists \alpha \neq 0 \in F : f(\alpha) = c.\alpha$. Vektor α nazývame *charakteristický* (*vlastný*) *vektor* zobrazenia f.

Veta 2.10.2.1.

Nech V, W ú r m r é r é r ry ľ m F a $f : V \to W$ je lineárne zobrazenie. M astných vektorov zobrazenia f, prislúchajúcich jeho charakteristickej hodnote c, je podpriestor V.

Dôkaz.

Nech M m ch r f, prislúchajúcich jeho charakteristickej hodnote c. $\forall x,y \in M$ $\forall \alpha,\beta \in F : f(\alpha x + \beta y) = \alpha f(x) + \beta f(y) = \alpha cx + \beta cy = c(\alpha x + \beta y) \in M$.

Definícia.

Nech A š rc m c ľ m F. $c \in F$ je *charakteristický prvok* matice A, ak $\exists x_1..x_n \in F : (A - cI_n)\begin{pmatrix} x_1 \\ \text{M} \\ x_n \end{pmatrix} = 0$.

Lema 2.10.2.1.

Nech A š rc m c ľ m F. $c \in F$ je charakteristický prvok matice A, ak $\begin{vmatrix} a_{1,1}-c & \Lambda & a_{1,n} \\ M & a_{k,k}-c & M \\ a_{n,1}-c & \Lambda & a_{n,n}-c \end{vmatrix} = 0.$

Dôkaz.

Tvrdenie vyplýva priamo z definície charakteristického prvku matice.

Dôsledok 2.10.2.1.

Štvorcová matica rádu n má najviac n charakteristických prvkov.

Dôkaz.

Ch r r c ch r mô yť c h ť m c

2.10.3. Podobnosť matíc.

Definícia.

H r m š rc é m c A,B rádu n sú *podobné*, ak existuje regulárna štvorcová matica P rádu n $B = P \times A \times P^{-1}$.

Veta 2.10.3.1.

Nech A,B sú regulárne štvorcové matice rádu n. Nech X m ch h ô matice A a Y m ch h ô m c B. Ak A a B sú podobné, potom $X = Y$.

Dôkaz.

Nech c je vlastná hodnota matice A. Potom $|A - cI_n| = 0$. Nech B je podobná s A. Potom $\exists P$ r gu r $B = P \times A \times P^{-1}$. Ale $|B - cI_n| = |P \times A \times P^{-1} - cI_n| = |P \times A \times P^{-1} - cP \times I_n \times P^{-1}|$ = (operácia násobenia matíc konštantou je komutatívna) $= |P \times A \times P^{-1} - P \times cI_n \times P^{-1}| = |P \times (A - cI_n) \times P^{-1}|$ = (A aj P sú regulárne) $= |P||A - cI_n||P^{-1}| = 0$, lebo $|A - cI_n| = 0$ c é B.

2.10.4. Kvadratické formy.

Definícia.

Nech V je vektorový r r ľ m F H r m r $f : V \to F$ je *kvadratická forma*, ak existuje bilineárna forma $g : V \times V \to F$ $\forall x \in V : f(x) = g(x,x)$. Ak $\forall x,y \in V : g(x,y) = g(y,x)$ h r m r f rm g je *symetrická*.

Veta 2.10.4.1.

Nech F je pole, $char(F) \neq 2$, V je vektorový priestor nad F a f je kvadratická forma na V. Potom na V existuje jediná symetrická bilineárna forma g $\forall x \in V : f(x) = g(x,x)$.

Dôkaz.

Nech h je bilineárna forma, ktorej existencia vyplýva definície kvadratickej formy. Definujme g predpisom $g(x,y) = ½(h(x,y) + h(y,x))$. Zrejme $g(x,y) = g(y,x)$ ď $g(x,x) = h(x,x) = f(x)$, g hľ bilineárna forma. Navyše $g(x,y) = ½(g(x+y,\ x+y) - g(x,x) - g(y,y)) = ½(f(x+y) - f(x) - f(y))$ m ur ť g.

Definícia.

Nech V je vektorový priestor dimenzie n ľ m F. Nech g je kvadratická forma na V, definovaná bilineárnou formou f a nech $\alpha_1..\alpha_n$ je báza vo V. Maticu $A_{n \times n}$, definovanú predpisom $A(i,j) = f(\alpha_i,\alpha_j)$, nazývame *matica kvadratickej formy* g hľ m u $\alpha_1..\alpha_n$. A je *symetrická*, ak je f symetrická.

2.10.5. Kongruencia matíc.

Definícia.

Štvorcové matice A,B rádu n sú *kongruentné*, ak $\exists$ regulárna štvorcová matica P rádu n $B = P \times A \times P^{T}$. Kongruenciu matíc A a B u m $A \cong B$.

Veta 2.10.5.1.
Štvorcové matice A,B rádu n ú gru é r y ď ú m c m r f rmy hľ m rô y

Dôkaz.
P reprezentuje maticu prechodu medzi bázami.

Veta 2.10.5.2.
Nech A,B sú štvorcové matice rádu n. Ak A je symetrická a $A\cong B$, tak aj B je symetrická.

Dôkaz.
Zrejmé.

Veta 2.10.5.3.
Relácia kongruencie je reláciou ekvivalencie.

Dôkaz.
Triviálne.

Veta 2.10.5.4.
K ym r c m c gru m c u ru $\begin{pmatrix} d_1 & 0 & \Lambda & 0 \\ 0 & O & 0 & M \\ M & 0 & d_k & 0 \\ 0 & \Lambda & 0 & 0 \end{pmatrix}$, kde $\forall i\in 1..k : d_i\neq 0$.

Dôkaz.
K ď m c mu m y ť r r é r é Í c é r c mô m h uť g y u

Dôsledok 2.10.5.1.
1. Pr ú r u f rmu f existuje báza, pri ktorej má $f(x,y)$ tvar $\sum_{i=1}^{k} d_i x_i y_i$.
2. Pr ú r c ú f rmu g existuje báza, pri ktorej má $g(x)$ tvar $\sum_{i=1}^{k} d_i x_i^2$.

Dôkaz.
Tvrdenia vyplývajú priamo z predchádzajúcej vety.

2.10.6. Reálne kvadratické formy.

Veta 2.10.6.1 (Sylvester).
Nech f je reálne kvadratická forma nad R^n a nech $x = x_1..x_n\in R^n$. Potom existuje báza, pri ktorej má $f(x)$ tvar $\sum_{k=1}^{m} \pm x_k$, kde $m \leq n$.

Dôkaz.
P ľ y 2 10 5 4 r c f rm gru m c u ru $\begin{pmatrix} d_1 & 0 & \Lambda & 0 \\ 0 & O & 0 & M \\ M & 0 & d_k & 0 \\ 0 & \Lambda & 0 & 0 \end{pmatrix}$. Pre reálne d_i yš x u m c y éh r u Í c m c u $|d_i|$ dostávame na diagonále ± 1.

Definícia.
Nech f je reálne kvadratická forma nad R^n, nech $x = x_1..x_n\in R^n$ a nech A je matica f hľ m u r x c u ru u 2 10 6 1 A A m u r (Í c) (r) m u m r (Í c) úc m r m 1 (r) m r m (Í c m) úc m r m –1 h r m A je v *kanonickom tvare*.

Veta 2.10.6.2 (Sylvestrov zákon zotrvačnosti).

Nech f je reálne kvadratická forma nad R^n, nech $x = x_1..x_n \in R^n$ a nech A je matica f hľ m u r x c u ru u 2 10.6.1. Nech A je v kanonickom tvare s r nenulovými riadkami, z ktorých má k vedúci prvok 1. Potom k a r ú ur é f rm u f (a teda nezávislé od bázy).

Dôkaz.

P u ch r ur h ť u r c f rmy ch r existujú dve matice A a B formy f c m r r m A má k riadkov s vedúcim prvkom 1 a B l a $k < l$. U u m m y r : S_1 nech sú vektory s nulovými súradnicami k+1..n a S_2 vektory s nulovými súradnicami 1..l. S_1 aj S_2 sú podpriestory R^n ď $k < l$, $\dim(S_1) + \dim(S_2) > n \Rightarrow S_1 \cap S_2 \neq \emptyset$. Tento prienik sú práve vektory s nenulovými súradnicami $k..l$ A ľ m c A je hodnota kvadratickej formy v týchto r ch ľ B r r

Definícia.

Nech f je reálne kvadratická forma nad R^n a nech A je jej matica v kanonickom tvare. H r m A je *kladne*(*záporne*) (*semi*)*definitná* ú g r y ä š (m š ä š r é m š r é) u

Veta 2.10.6.3.

Nech V je euklidovský priestor dimenzie n a f je kvadratická forma na V. Potom na V existuje r rm $\forall x = x_1..x_n \in V : f(x) = \sum_{k=1}^{n} d_k x_k^2$, kde d_k ú é f rmy f.

Dôkaz.

Nech $\alpha_1..\alpha_n$ je ortonormálna báza vo V a A je symetrická matica formy f hľ m u $\alpha_1..\alpha_n$. Z vety 2 10 5 4 y x u r g m c P $P \times A \times P^T$ g A ď P je ortogonálna, tak $P \times A \times P^T = P \times A \times P^{-1}$ a ak maticu P chápeme ako maticu prechodu od $\alpha_1..\alpha_n$ k nejakej báze $\beta_1..\beta_n$, tak aj $\beta_1..\beta_n$ je ortonormálna. Na diagonále matice $P \times A \times P^{-1}$ ú r é f rmy f.

Dôsledok 2.10.6.1.

Všetky charakteristické vektory reálnej symetrickej matice sú reálne.

Dôkaz.

Tvrdenie vyplýva priamo z predchádzajúcej vety.