7. Pole a jejich rozšíření

Definice: Komutativní okruh s nenulovou jednotkou se nazývá *pole*, pokud je má každý nenulový prvek inverzi vzhledem k násobení.

Věta: Každý konečný obor integrity je pole.

Důkaz: Nechť D je obor integrity s jednotkou 1. Nechť $a \in D$ je libovolný nenulový prvek. Potřebujeme ukázat, že a má multiplikativní inverzi. Pokud $a = 1$, je svou vlastní inverzí, takže předpokládáme $a \neq 1$. Vezměme posloupnost prvků D: $a, a^2, a^3, ...$ Vzhledem k tomu, že D je konečný, musí existovat $i, j \in \mathbb{N}, i > j$ takové, že $a^i = a^j$. Potom $a^{i-j} = 1$ z cancelation property. Protože $a \neq 1$ a víme $i - j > 1$, je a^{i-j-1} inverze k a.

Věta: Okruh celých čísel modulo p je pole pro každé prvočíslo p.

Příklad: Pole s devíti prvky:
$\mathbb{Z}(3)[i] = \{a + bi : a, b \in \mathbb{Z}(3)\} = \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$

Poznámka: Průnik všech podpolí pole je podpole a tím pádem má každé pole nejmenší podpole, kterému se říká *prime podpole* pole.

Definice: *Homeomorfismus okruhů* $\phi : R \to S$ je zobrazení zachovávající obě operace kruhu, tj.:

$$(a + b)\phi = a\phi + b\phi \text{ a } (ab)\phi = (a\phi)(b\phi) \text{ pro všechna } a, b \in R$$

Bijektivní homeomorfismus nazýváme *isomorfismus*.

Definice: Pole E je *rozšíření* pole F, pokud $F \subseteq E$.

Fundamentální věta teorie polí (Kroneckerova věta): Nechť F je pole a $f(x)$ nekonstantní polynom v $F[x]$. Potom existuje E rozšíření pole F, ve kterém má $f(x)$ nulu.

Definice: Nechť E je rozšíření pole F a nechť $a \in E$. Řekneme, že a je *algebraické* nad F, pokud je a nula nějakého polynomu v $F[x]$. Pokud a není algebraické nad F, řekneme, že je *transcendentální* nad F. Rozšíření E pole F je *algebraické rozšíření*, pokud je každý prvek E algebraický nad F. Pokud E není algebraické rozšíření nad F, je to *transcendentální rozšíření* pole F. Rozšíření pole F typu $F(a)$ je *jednoduché (simple) rozšíření* F.

Věta: Nechť E je rozšíření pole F a $a \in E$. Pokud je a transcendentální nad F, potom $F(a) \approx F(x)$. Pokud je a algebraické nad F, potom $F(a) \approx F[x]/\langle p(x)\rangle$, kde $p(x)$ je polynom v $F[x]$ minimálně takového stupně, že $p(a) = 0$. Navíc je $p(x)$ irreducibilní nad F.

Důsledek: Pokud je a algebraické nad polem F, potom existuje jedinečný monický irreducibilní polynom $p(x)$ v $F[x]$ takový, že $p(a) = 0$. Takový polynom nazýváme *minimální polynom* a nad F.

Důsledek: Nechť je a algebraické nad F a nechť $p(x)$ je minimální polynom a nad F. Pokud $f(x) \in F[x]$ a $f(a) = 0$, potom $p(x)$ dělí $f(x)$ v $F[x]$.

Definice: Nechť je E rozšíření pole F. Řekneme, že E je *rozšíření stupně n nad polem F* a píšeme $[E : F = n]$, pokud má E dimenzi n jako vektorové pole nad F. Pokud je $[E : F]$ konečné, je E *konečné rozšíření* F, jinak se jedná o *nekonečné rozšíření* F.

Příklad: Pole komplexních čísel je rozšíření 2. stupně nad polem reálných čísel, protože $\{1, i\}$ je báze. Pole komplexních čísel je nekonečné rozšíření racionálního pole.

Věta: Pokud je E konečné rozšíření F, tak je to algebraické rozšíření.

Poznámka: opačná implikace neplatí: $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ je algebraické rozšíření Q, ale není konečné

Věta: Nechť K je konečné rozšíření E a nechť E je konečné rozšíření F. Potom K je konečné rozšíření F a platí $[K : F] = [K : E][E : F]$.

Věta: Pro každé prvočíslo p a přirozené číslo n existuje, až na isomorfismy, jedinečné konečné pole řádu p^n.