Algebra Abstrakcyjna - Definicje i Twierdzenia

Przepisał: Ricko

Rok 2014/2015

Spis treści

Rozdział 1

Wykłady

1.1 Wykład 1 - 07.10.14

1.1.1 Grupy

Def.: Grupą nazywamy zbiór niepusty G z określonym w nim działaniem dwuargumentowym

$\cdot : G \times G \to G$ - funkcja

$(a, b) \mapsto a \cdot b$

o własnościach

1) $\cdot$ jest działaniem łącznym

$\forall_{a,b,c \in G}\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

2) $\cdot$ ma element neutralny

$\exists_{e \in G}\ \forall_{a \in G}\ a \cdot e = e \cdot a = a$

3) Każdy element $a \in G$ ma element odwrotny

$\forall_{a \in G}\ \exists_{a' \in G}\ a \cdot a' = a' \cdot a = e$

Jeśli dodatkowo działanie $\cdot$ jest przemienne ($\forall_{a,b \in G}\ a \cdot b = b \cdot a$) to grupę G nazywamy **abelową**

Uwaga

Element neutralny działania i element odwrotny do a są określone jednoznacznie

Umowa

Przyjmujemy:

$e = 1$

$a' = a^{-1}$

1.1.2 Podgrupy i warstwy

Def.: **Podgrupą** H grupy G nazywamy podzbiór $\emptyset \neq H \subset G$, który sam jest grupą z działaniem z grupy G

Równoważnie:

1) $\forall_{a,b \in H}\ a \cdot b \in H$

2) $\forall_{a \in H}\ a^{-1} \in H$

Tw: Podzbiór $\emptyset \neq H \subset G$ jest podgrupa $G \iff \forall_{a,b \in H}\ ab^{-1} \in H$

Def: **Warstwą lewostroną** podgrupy H w grupie G (o reprezentancie a) nazywamy zbiór $a \cdot H = \{a \cdot h | h \in H\}$

Def: **Warstwą prawostroną** podgrupy H w grupie G (o reprezentancie a) nazywamy zbiór $H \cdot a = \{h \cdot a | h \in H\}$

Uwaga: W przestrzeniach wektorowych są ona zwykle te same, u nas jednak najczęściej nie będzie tak: $a \cdot H \neq H \cdot a$

Tw: Niech H będzie podgrupą grupy G ($H < G$)

1) Dwie warstwy lewostronne podgrupy G sa równe albo rozłączne
2) $G = \bigcup_{a \in G} aH$
3) Moc każdej warstwy lewostronnej jest równa mocy H ($|a \cdot H| = |H|, a \in G$)

Def: Liczbę warstw lewostronnych podgrupy H w grupie G (równą liczbie warstw prawostronnych) nazywamy **indeksem** podgrupy H w grupie G i oznaczamy $[G : H]$

1.2 Wykład 2 - 14.10.14

1.2.1 Rząd grupy

Def.: Rzędem grupy G nazywamy moc zbioru G i oznaczamy $|G|$

Przyp.: $H < G \quad G = \bigcup_{a \in G} aH \quad |aH| = |H| \quad aH \cap bH \neq \emptyset \Rightarrow aH = bH$

Dowodząc w ten sam sposób co przypomniane powyżej twierdzenie można udowodnić jego wersję dla

warstw prawostronnych:

$H < G \quad G = \bigcup_{a \in G} Ha \quad |Ha| = |H| \quad Ha \cap Hb \neq \emptyset \Rightarrow Ha = Hb$

Wn.: $|G| = |H|\cdot$ (ilość warstw prawostronnych) $= |H|\cdot$ (ilość warstw lewostronnych)

(ilość warstw lewostronnych) = (ilość warstw prawostronnych) $= [G : H]$

Tw. Lagrange'a: $|G| = |H| \cdot [G : H]$ (nawet jeśli rzedy są nieskończone)

Wn.: $|G| < \infty \Rightarrow |H| \Big| |G|$

Rząd podgrupy dzieli rząd grupy dla grup skończonych

1.2.2 Rząd elementów grupy

Def.: Rzędem elementu $a \in G$ nazywamy liczbę

$r(a) = \min\{k \in \mathbb{N}\backslash\{0\} \mid a^k = 1 \text{ (element neutralny) } \}$

Jeśli takie k nie istnieje to mówimy, że a ma rząd nieskończony (piszemy $r(a) = \infty$)

Wn.: $|G| < \infty \wedge a \in G \Rightarrow r(a) \mid |G|$

1.2.3 Zbiór generatorów grupy. Grupy skończenie generowane i grupy cykliczne

$\emptyset \neq A \subseteq G$

$\langle A \rangle = \bigcap_{A \subseteq H < G} H$

Tw.: $\langle A \rangle$ jest najmniejszą podgrupą grupy G zawierającą zbiór A

Uwaga $\langle A \rangle = \{a_1^{\varepsilon_1} \cdot ... \cdot a_k^{\varepsilon_k} \mid a_i \in A, \varepsilon_i \in \{-1, 1\}$

" $\supseteq$ " elementy A i ich odwrotne + skończone iloczyny

" $\subseteq$ " najmniejsza podgrupa $\subseteq$ podgrupa G

Def.:

(1) Jeśli $\langle A \rangle = G$ to mówimy, że A jest zbiorem generatorów grupy G

$\underbrace{G = \langle G \rangle}_{\text{zawsze}} = \underbrace{\langle A \rangle \quad A \not\subseteq G}_{\text{może tak być}}$

(2) Jeśli $G = \langle A \rangle$ dla pewnego skończonego zbioru A to mówimy, że grupa G jest skończenie generowaną

(3) Jeśli $G = \langle \{a\} \rangle := \langle a \rangle$ dla pewnego $a \in G$ to mówimy, że G jest grupą cykliczną

Wn.: Grupa G jest cykliczna, jeśli zawiera element, którego rząd jest równy rzędowi grupy

Stw.: Każda grupa cykliczna jest abelowa

Tw.: Podgrupa grupy cyklicznej jest cykliczna

1.3 Wykład 3 - 21.10.14

1.3.1 Homomorfizmy grup. Jądro i obraz

Def.: Niech G, G' będa grupami. Funkcję $\varphi : G \to G'$ nazywamy **homomorfizmem grup** jeśli $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ dla dowolnych $a, b \in G$ (pierwsze działanie jest w G, drugie w G')

Def.: Homomorfizm $\varphi : G \to G'$ nazywamy:

- **Monomorfizmem** jeśli φ jest funkcją różnowartościową (iniekcją)
- **Epimorfizmem** jeśli φ jest funkcją 'na' (suriekcja)
- **Izomorfizmem** jeśli φ jest funkcją różnowartościową i 'na' (bijekcja)

Własności homomorfizmu $\varphi : G \to G'$

1) $\varphi(1) = 1$ ponieważ $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) \Rightarrow \underbrace{\varphi(1)^{-1} \cdot \varphi(1)}_{1} = \underbrace{\varphi(1)^{-1} \cdot \varphi(1)}_{1} \cdot \varphi(1) \Rightarrow 1 = \varphi(1)$

2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$ ponieważ $\varphi(1) = \varphi(a^{-1} \cdot a) = \varphi(a^{-1}) \cdot \varphi(a) \Rightarrow (\varphi(a))^{-1} = \varphi(a^{-1})$

Def.: Jądrem homomorfizmu $\varphi : G \to G'$ nazywamy zbiór

$Ker\ \varphi = \{a \in G \mid \varphi(a) = 1\}$

Def.: Obrazem homomorfizmu $\varphi : G \to G'$ nazywamy zbiór

$Im\ \varphi = \{\varphi(a) \mid a \in G\} = \varphi(G)$

Tw.: $\varphi : G \to G'$ - homomorfizm grup

1) $Ker\ \varphi < G$

2) $Im\ \varphi < G'$

1.3.2 Podgrupy normalne

Def.: Podgrupę H grupy G nazywamy **podgrupą normalną** jeśli $aH = Ha$ dla dowolnego $a \in G$

Oznaczamy $(H \triangleleft G)$

Uwaga: W grupie abelowej każda podgrupa jest normalna

Tw.: Podgrupa H grupy G jest podgrupą normalną $\iff \forall_{a \in G}\ \forall_{h \in H}\ aha^{-1} \in H$

Tw.: $\varphi : G \to G'$ - homomorfizm grup

$Ker\ \varphi \triangleleft G$

1.3.3 Centrum i komutant grupy

Def.: Centrum grupy G nazywamy zbiór $Z(G) = \{a \in G \big|\ \forall_{b \in G}\ ab = ba\}$

Tw.: $Z(G) \triangleleft G$

Uwaga: G-abelowa to $Z(G) = G$

Def.: Komutatorem grupy G nazywamy element $[a, b] = aba^{-1}b^{-1}$, ponadto $[a, b]^{-1} = [bab^{-1}a^{-1}] = [b, a]$

Def.: Komutantem grupy G nazywamy podgrupę generowaną przez wszystkie komutatory i oznaczamy $[G, G]$

$[G, G] = \{f_1^{\varepsilon_1} \cdot ... \cdot f_n^{\varepsilon_n} \ \big|\ n \in \mathbb{N}\}$ gdzie f_i - komutator, $\varepsilon_i \in \{-1, 1\}$

Uwaga: W grupie abelowej $[G, G] = \{1\}$

Tw.: $[G, G] \triangleleft G$

1.3.4 Grupy proste

Def.: Grupę G nazywamy **prostą** jeśli jej jedynymi podgrupami normalnymi są G i $\{1\}$

Stw.: Jeśli $|G|$ jest liczba pierwszą to G jest grupą prostą

Tw.: Dla $m \geqslant 5$ grupa A_n jest prosta (wykorzystuje się ten fakt w dowodzie faktu, ze nie ma wzorów na pierwiastki stopni $\geqslant 5$)

1.4 Wykład 4 - 28.10.14 (prowadzony przez Prof. Sładka)

Lemat: Przy założeniu $H \triangleleft G$ oraz $aH = a'H,\ bH = b'H \Rightarrow abH = a'b'H$

Niech $H \triangleleft G$ oraz niech G/H będzie zbiorem warstw grupy G względem H

W G/H określamy działanie

$(aH)(bH) \stackrel{def}{=} (ab)H$

Z lematu wynika poprawność definicji

Tw.: Zbiór G/H z wyróżnionym elementem $1 \cdot H = H$ oraz powyższym działaniem jest grupą natomiast odwzorowanie $\kappa : G \to G/H \quad \kappa(a) = aH$ jest epimorfizmem grup oraz $Ker\ \kappa = H$

Tw.: Podgrupa H grupy G jest normalna witw, gdy istnieje homomorfizm φ określony na G taki, że $H = Ker\ \varphi$

Tw.(o homomorfizmie grup):

Jeśli $\varphi : G \to G'$ jest homomorfizmem grup to istnieje dokładnie jeden homomorfizm $\psi : G/Ker\ \varphi \to G'$ taki, że $\varphi = \psi \circ \kappa$

Tw.(o izomorfizmie grup)

Jeśli $\varphi : G \to G'$ jest homomorfizmem grup to $G/Ker\ \varphi$ jest grupą izomorficzną z $Im\ \varphi$ $(G/Ker\ \varphi \cong Im\ \varphi)$

Tw.(o izomorfizmie grup)

Niech $H < G,\ K \triangleleft G$

Wtedy:

1. $HK = \{h \cdot k : h \in H, k \in K\} \triangleleft G$
2. $H \cap K \triangleleft G$
3. $HK/_K \cong H/_{H \cap K}$

Tw.(o izomorfizmie grup)

Niech $H \triangleleft G,\ K \triangleleft G$ oraz $H \subset K$

Wtedy:

1. $K/_H \triangleleft G/_H$
2. $G/H\big/_{K/H} \cong G/K$

Tw.(o izomorfizmie grup)

Niech $H \triangleleft G$ oraz X niech będzie zbiorem podgrup G zawierających H, a Y zbiorem podgrup grupy G/H

Wtedy istnieje odwzorowanie wzajemnie jednoznaczne $\phi : X \to Y$

Przypomnienie

$[G,G] =< \{[a,b] : a,b \in G, [a,b] = aba^{-1}b^{-1}\}$

Uwaga: G-abelowa $\Leftrightarrow [G,G] = \{1\}$

Tw.: Niech $H < G$. Wtedy $H \triangleleft G$ i G/H - abelowa $\Leftrightarrow$ gdy $[G,G] \in H$

Def.: Grupę G nazywamy **rozwiązalną**, jeśli istnieje ciąg podgrup $\{1\} = G_0 \triangleleft G_1 \triangleleft ... \triangleleft G_n = G$ taki, że G_{i+1}/G_i jest podgrupą abelową dla $i = 0...n-1$

Uwaga: Warunek G_{i+1}/G_i - grupa abelowa jest równoważny warunkowi $[G_{i+1}, G_{i+1}] \subset G_i$

1.5 Wykład 5 - 04.11.14

1.5.1 Skończenie generowane grupy abelowe

$G = \langle a_1, ..., a_n \rangle = \{a_1^{k_1} \cdot ... \cdot a_n^{k_n} \mid k_i \in \mathbb{Z}\}$

Przykłady: $\{1\}, \mathbb{Z}, \mathbb{Z}_n = \langle 1 \rangle$

Tw.: Każda grupa cykliczna rzędu n jest izomorficzna $\mathbb{Z}_n$

Tw.: Produkt grup skończenie generowanych jest grupą skończenie generowaną

Wn.: $G_1...G_n$ - grupy skończenie generowane $\Rightarrow G_1 \times ... \times G_n$ jest grupą skończenie generowaną

$\mathbb{Z}^k = \underbrace{\mathbb{Z} \times ... \times \mathbb{Z}}_{k}$

$\mathbb{Z}^k \times \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_s}$

Tw. (strukturalne dla skończenie generowanych grup abelowych)

Każda skończenie generowana grupa abelowa jest izomorficzna z grupą $\mathbb{Z}^k \times \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_s}$, gdzie

1) $k \geqslant 0$

2)$n_i \geqslant 2 \qquad n_i \big| n_{i+1}$ dla $i = 1...s-1$

1.5.2 Pierścienie i podpierścienie

Def.: Pierścieniem nazywamy zbiór niepusty z działaniami:

$+ : P \times P \to P$ (dodawanie)

$\cdot : P \times P \to P$ (mnożenie)

o własnościach

1) $(P, +)$ jest grupą abelową (z elementem neutralnym 0)

2) mnożenie jest łączne

3) mnożenie jest rozdzielne względem dodawania

$a, b, c \in P$

$(a+b) \cdot c = ac + bc \ \wedge \ c(a+b) = ca + cb$

Jeśli $\cdot$ jest przemienne to pierścień nazywamy przemiennym

Jeśli $\cdot$ ma element neutralny to mówimy, że P jest pierścieniem z 1

Jeśli P jest pierścieniem z 1 i dla każdego $a \in P^*$ istnieje $a' \in P$, taki $a \cdot a' = a' \cdot a = 1$ to mówimy, że P jest pierścieniem z dzieleniem

$$P^* = P \setminus \underbrace{\{0\}}_{el.\ neutralny}$$

Przemienny pierścień z dzieleniem nazywamy **ciałem**

UMOWA

Pierścień - przemienny z 1

1.6 Wykład 6 - 18.11.14

1.6.1 Elementy odwracalne i dzielniki zera w pierścieniu

Def.: Element $a \in P \setminus \{0\}$ nazywamy **dzielnikiem zera** jeśli istnieje $b \in P \setminus \{0\}$ taki, że $a \cdot b = 0$

Def.: Element $a \in P$ nazywamy **elementem odwracalnym** jeśli istnieje $b \in P$ taki, że $a \cdot b = 1$

Def.: Pierścień, który nie posiada dzielników zera nazywamy **pierścieniem całkowitym**

Oznaczenia:

$D(P)$ - zbiór dzielników zera pierścienia P

$U(P)$ - zbiór elementów odwracalnych pierścienia P

Stw. Przypuśćmy, że $0 \neq a \in P \backslash D(P)$

$ab = ac \Rightarrow b = c$

Tw.: $D(P) \cap U(P) = \emptyset \longleftarrow$ Zadanie domowe

Tw.: $|P| < \infty \Rightarrow P = \{0\} \cup D(P) \cup U(P)$

Wn.: Skończony pierścień całkowity jest ciałem (każdy element niezerowy jest odwracalny)

1.6.2 Podpierścienie i ideały

Def.: Podzbiór $\emptyset \neq R \subset P$ nazywamy **podpierścieniem**, jeśli

1) $\forall_{a,b \in R} \quad a - b \in R$

2) $\forall_{a,b \in R} \quad a \cdot b \in R$

Def.: Podpierścień I pierścienia P nazywamy **ideałem** jeśli

$\forall_{a \in I} \ \forall_{x \in P} \quad ax \in I \qquad I \lhd P$

Tw.: $(A) \lhd P \longleftarrow$ zadanie domowe

Def.: Ideał (A) nazywamy ideałem generowanym przez zbiór A. Jeśli $A = \{a_1, ..., a_n\}$ to piszemy $(A) = (a_1, ..., a_n)$ i mówimy, że jest skończenie generowany

Ideał (a) nazywamy ideałem głównym

Lem.: Niech $I \lhd P$. Jeśli $I \cap U(P) \neq \emptyset \Leftrightarrow I = P$

Tw.: P jest ciałem $\Longleftrightarrow$ P ma dokładnie dwa ideały

1.6.3 Pierścień ilorazowy

Niech I będzie ideałem pierścienia P $I \triangleleft P$

$x + I = \{x + a \mid a \in I\}$ - warstwa pierścienia P względem ideału I

$P/_I$ - zbiór warstw

Stw.: $x + I = y + I \Leftrightarrow x - y \in I$

Działania na zbiorze warstw:

$(a + I) + (b + I) = (a + b) + I$

$(a + I) \cdot (b + I) = (a \cdot b) + I$

Tw.: $P/_I$ jest pierścieniem przemiennym z 1

$0 + I = I$

$1 + I = 1$

1.6.4 Homomorfizmy pierścieni

Def.: Odwzorowanie $\varphi : P \to R$ nazywamy **homomorfizmem pierscieni**, jeśli

$\varphi(a + b) = \varphi(a) + \varphi(b)$

$\varphi(ab) = \varphi(a)\varphi(b)$ dla $a, b \in P$

Monomorfizm - homomorfizm różnowartościowy (iniekcja)

Epimorfizm - homomorfizm 'na' (suriekcja)

Izomorfizm - homomorfizm różnowartościowy i 'na' (bijekcja)

Def.: Jądrem homomorfizmu $\varphi : P \to R$ nazywamy zbiór $Ker\ \varphi = \{a \in P \mid \varphi(a) = 0\}$

Def.: Obrazem homomorfizmu φ nazywamy zbiór $Im\ \varphi = \{\varphi(a) \mid a \in P\}$

1.7 Wykład 7 - 25.11.14

Zadanie Domowe:

Tw.: Niech $\varphi : P \to R$ będzie homomorfizmem pierścieni

1. $Ker\ \varphi \triangleleft P$
2. $Im\ \varphi < R$

Wn.: I jest ideałem pierścienia P witw, gdy I jest jądrem pewnego homomorfizmu pierścienia P

1.7.1 Twierdzenia o izomorfizmie pierścieni

Tw.: (o izomorfizmie pierścieni)

Jeśli $\varphi : P \to R$ jest homomorfizmem pierścieni i $Ker\ \varphi = I$ to istnieje dokładnie jeden homomorfizm $\psi : P/_I \to R$ taki, że $\varphi = \psi \circ \kappa$ - homomorfizm kanoniczny

Tw.:(o izomorfizmie)

Jeśli $\varphi : P \to R$ jest homomorfizmem pierścieni to $P/_{Ker\ \varphi} \cong Im\ \varphi$

Tw.:(o izomorfizmie)

Niech $I \lhd P,\ R < P$. Wtedy:

1. $R + I = \{a + b \mid a \in R, b \in I\} < P$
2. $R \cap I \lhd R$
3. $R + I/_I \cong R/_{R\ \cap\ I}$

Tw.:(o izomorfizmie) Niech $I \lhd P,\ J \lhd P,\ I \subset J$ Wtedy:

1. $J/_I \lhd P/_I$
2. $^{P/_I}\big/_{J/_I} \cong P/_J$

Tw.:(o izomorfizmie) Istnieje bijekcja między zbiorem podpierścieni pierścienia P zawierających $I \lhd P$, a zbiorem podpierścieni pierścieni $P/_I$

1.7.2 Ciało ułamków pierścienia całkowitego

P - pierścień całkowity (bez dzielników zera)

Na zbiorze $P \times P^*$ definiujemy relację (równoważności)

$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad - bc = 0$

$(a, b) \sim (c, d) \Leftrightarrow ad - bc = 0$

Klasę abstrakcji względem powyższej relacji wyznaczoną przez (a, b) nazywamy ułamkiem o liczniku a i mianowniku b i oznaczamy $\frac{a}{b}$

$Quot(P)$ - zbiór wszystkich ułamków

Wprowadzamy działania na tym zbiorze dodawania i mnożenia:

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

Tw.: $Quot(P)$ z powyższym działaniami na ułamkach jest ciałem

1.7.3 Podzielność w pierścieniach całkowitych

Def.: P - pierścień całkowity, $a, b \in P$

1. Mówimy, że a dzieli b jeśli istnieje $c \in P$ taki, że $b = a \cdot c$ $(a|b)$
2. Mówimy, że a i b są stowarzyszone jeśli $a|b$ i $b|a$ $(a \sim b)$

Wn.: $a \sim b \Leftrightarrow \exists_{u \in U(P)}\ a = bu \longleftarrow$ **Zadanie Domowe**

Def.:

1. Element niezerowy i nieodwracalny $p \in P$ nazywamy **nierozkładalnym** jeśli zachodzi implikacja $p = a \cdot b \Rightarrow a \in U(P) \vee b \in U(P)$
2. Element niezerowy i nieodwracalny $p \in P$ nazywamy **pierwszym** jeśli zachodzi implikacja $p|ab \Rightarrow p|a \vee p|b$

Tw.: Każdy element pierwszy jest nierozkładalny

1.7.4 Największy wspólny dzielnik

Def.: Największym wspólnym dzielnikiem elementów $a, b \in P(NWD(a, b))$ nazywamy element d taki, że

1) $d|a \wedge d|b$

2) $c|a \cap c|b \Rightarrow c|d$

$NWD(a, b) \sim d$

Def.:Najmniejszą wspólną wielokrotnością elementów $a, b \in P(NWW(a, b))$ nazywamy element w taki, że

1) $a|w \wedge b|w$

2) $a|c \cap b|c \Rightarrow w|c$

$NWW(a, b) \sim w$

1.8 Wykład 8 - 02.12.14

Def.: Elementy $a, b \in P$ nazywamy **względnie pierwszymi** jeśli $NWD(a, b) \sim 1$

1.8.1 Ideały pierwsze i maksymalne

Def.: Ideał $I \triangleleft P$ nazywamy **pierwszym** jeśli:

$ab \in I \Rightarrow a \in I \vee b \in I$

Def.: Ideał właściwy $I \triangleleft P$ nazywamy **maksymalnym** jeśli:

$I \triangleleft J \triangleleft P \Rightarrow I = J \vee J = P$

Tw.: P - pierścień całkowity, $p \in P*$

1) p jest elementem pierwszym witw, gdy (p) jest ideałem pierwszym

2) p jest elementem nierozkładalnym kiedy (p) jest maksymalny w rodzinie ideałów głównym pierścienia P

Tw.: (o charakteryzacji ideałów za pomocą pierścieni ilorazowych)

1) $I \triangleleft P$ jest ideałem pierwszym $\Leftrightarrow P/_I$ jest pierścieniem całkowitym

2) $I \triangleleft P$ jest ideałem maksymalnym $\Leftrightarrow P/_I$ jest ciałem

Wn.: Każdy ideał maksymalny jest pierwszy

Def.: Pierścień całkowity P nazywamy **pierścieniem lokalnym** jeśli ma on dokładnie jeden ideał maksymalny

1.8.2 Pierścienie Euklidesowe

Def.: Pierścień całkowity nazywamy **euklidesowym** jeśli istnieje funkcja $N : P \to \mathbb{N} \cup \{0\}$ (zwana normą euklidesową) o własnościach:

1. $N(a) = 0 \Leftrightarrow a = 0$
2. $N(ab) = N(a) \cdot N(b)$
3. $\forall_{a \in P} \ \forall_{b \in P^*} \ \exists_{q,r} \ \ a = b \cdot q + r \wedge (r = 0 \vee N(r) < N(b))$

Tw.: W pierścieniach euklidesowych $NWD(a, b)$ zawsze istnieje (o ile $a \neq 0, b \neq 0$)

1.9 Wykład 9 - 09.12.14

Tw.: W pierścieniu euklidesowym istnieje $NWD(a, b) \ \ a, b \in P^*$

Tw.: W pierścieniu euklidesowym każdy ideał jest główny

1.9.1 Pierścienie ideałów głównych $(P.I.D.)$

Def. Pierścieniem ideałów głównych nazywamy pierścień, w którym każdy ideał jest główny

Wn.: Każdy pierścień euklidesowy jest pierścieniem ideałów głównych

Przykład: (pierścienia ideałów głównych, nie będący pierścieniem euklidesowym)
$\mathbb{Z}[\frac{1}{2}\sqrt{-19}]$

Tw.: (zadanie domowe)
W pierścieniu ideałów głównych istnieje $NWD(a,b)$ dla $a,b \in P*$ i jest on wyznaczony jednoznacznie z dokładnością do stowarzyszenia

Tw.: W pierścieniu ideałów głównych każdy ideał pierwszy jest maksymalny

Wn.: W $P.I.D.$ każdy element nierozkładalny jest pierwszy

1.9.2 Pierścienie z jednoznacznym rozkładem $(U.F.D)$

Def.: Pierścień całkowity P nazywamy **pierścieniem z jednoznacznym rozkładem** jeśli każdy element $a \in P\backslash\{0\}, a$ - nieodwracalny można zapisać jako iloczyn elementów nierozkładalnych; to przedstawienie jest jednoznaczne z dokładnością do kolejności
$a = p_1 \cdot ... \cdot p_n$ p_i - nierozkładalny
$a = q_1 \cdot ... \cdot q_m$ q_j - nierozkładalny
$p_1 \sim q(\delta(i))$ dla permutacji $\delta \in S_n$)

Tw.: W pierścieniu z jednoznacznym rozkładem każdy element nierozkładalny jest pierwszy

Tw.: Niech P będzie pierścieniem, w którym każdy element $a \in P^*\backslash U(P)$ można przedstawić w postaci iloczynu elementów nierozkładalnych
P jest $U.F.D \Leftrightarrow$ gdy każdy element nierozkładalny jest pierwszy

Tw.: $P - P.I.D. \Rightarrow P - U.F.D.$

1.10 Wykład 10 - 16.12.14

Uwaga: Pierścień, w którym każdy wznoszący (wstępujący) łańcuch ideałów stabilizuje się ($I_1 \subset I_2 \subset ... \Rightarrow \exists_n I_n = i_{n+1} = ...$) nazywamy **pierścieniem noetherowskim**. Równoważnie są to pierścienie, w których każdy ideał jest skończenie generowany

Tw.: Jeśli P jest *U.F.D.* to $P[x]$ jest *U.F.D.*

1.10.1 Pierścienie ułamków i lokalizacja

P - pierścień przemienny z 1

Def.: Podzbiór $\emptyset \neq S \subset P$ nazywamy **zbiorem multiplikatywnym** jeśli:

1. $0 \notin S$
2. $1 \in S$
3. $a, b \in S \Rightarrow ab \in S$

Konstrukcja pierścienia ułamków

$S-$ zbiór multiplikatywny

$P \times S$ - definiujemy relację: $(a_1 s_1) \sim (a_2 s_2) \Leftrightarrow \exists_{s \in S}\ s(a_1 s_2 - a_2 s_1) = 0$

$\frac{a}{s}$ - klasa abstrakcji względem powyższej relacji równoważności

$S^{-1}P$ - zbiór ułamków (klas abstrakcji) z działaniami:

$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + s_1 a_2}{s_1 s_2}$

$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$

Tw.:

1. $S^{-1}P$ jest pierścieniem z 1
2. Odwzorowanie $\varphi : P \to S^{-1}P \quad \varphi(a) = \frac{a}{1}$ jest monomorfizmem
3. $\varphi(S) \subset U(S^{-1}P)$

Def.: Pierścień $S^{-1}P$ nazywamy pierścieniem ułamków względem zbioru multiplikatywnego **Lem.:** Jeśli I jest ideałem pierwszym pierścienia P to $P/_I$ jest zbiorem multiplikatywnym

Tw.: Niech I będzie ideałem pierwszym pierścienia P i niech $S = P/_I$. Wtedy S^{-1} jest pierścieniem

lokalnym (ma dokładnie jeden ideał maksymalny)

Def.: Pierścień $S^{-1}P$ z powyższego twierdzenia nazywamy **lokalizacją** pierścienia względem ideału pierwszego I i oznaczamy P_I

1.10.2 Rozszerzenia ciał

$\underbrace{K}_{\text{podciało ciała } L} \subset \underbrace{L}_{\text{rozszerzenie ciała } K}$ Ozn: $L/_K$

Fakt: L jest przestrzenią wektorową nad ciałem K

Def.:

1. Bazą rozszerzenia $L/_K$ nazywamy baze przestrzeni wektorowej L nad K
2. Stopniem rozszerzenia $L/_K$ nazywamy liczbę $[L:K] = \dim_k L$
3. Rozszerzenie $L/_K$ jest skończone jeśli $[L:K] < \infty$

Tw.(o wieży ciał)
Niech $K \subset L \subset M$

1. $[L:K] < \infty \ \wedge \ [M:L] < \infty \Rightarrow [M:K] < \infty$
2. $[M:K] = [M:L] \cdot [L:K]$

1.11 Wykład 11 - 13.01.15

Def.: Niech $L/_K \quad \emptyset \neq A \subset L$
Najmniejsze ciało zawierające K i A nazywamy **rozszerzeniem ciała** K generowanym przez zbiór A i piszemy $K(A)$
Rozszerzenie $K(\alpha_1 ... \alpha_n)$ nazywamy **skończenie generowanym**
Rozszerzenie $K(\alpha)$ nazywamy roszerzeniem **prostym**

Fakt
Każdy nietrywialny homomorfizm ciał jest monomorfizmem (zanurzenie)
$\varphi : K \longrightarrow L$
Ciało ma dwa ideały, odrzucamy nietrywialny (całe K), zostaje jeden ideał stąd mamy monomorfizm

1.11.1 Elementy algebraiczne i przestępne

Def.: Element $\alpha \in L$ nazywamy **elementem algebraicznym** nad K jeśli istnieje wielomian $f \in K[x]$ taki, że $f(\alpha) = 0$

Element, który nie jest algebraiczny nad K nazywamy **elementem przestępnym**

Tw.: Niech α będzie elementem algebraicznym nad ciałem K. Istnieje wielomian $f \in K[x]$ nierozkładalny, unormowany i taki, że $f(\alpha) = 0$. Wielomian f wyznaczony jest jednoznacznie

Def.: Wielomian f z powyższego twierdzenia nazywamy **wielomianem minimalnym** elementu algebraicznego α. Stopień f nazywamy **stopniem elementu algebraicznego** α

Uwaga: Jeśli f jest wielomianem minimalnym elementu algebraicznego α i $g(\alpha) = 0$ to $f \big| g$

1.11.2 Algebraiczne i przestępne rozszerzenia proste

$K(\alpha) \qquad L/_K \qquad \alpha \in L$

$\varphi_\alpha : K[x] \longrightarrow L \qquad \varphi_\alpha(f) = f(\alpha)$

$Im\ \varphi_\alpha := K[\alpha]$ - jest to najmniejszy pierścień zawierający K i α

Rozważmy dwa przypadki:

- Przypadek I

  α jest elementem przestępnym

  Wtedy $Ker\ \varphi_\alpha = (0)$ czyli φ_α jest monomorfizmem i $K[\alpha] \cong K[x]$ stąd $K(\alpha) = Quot(K[\alpha]) \cong K(x) = Quot(K[x])$

  $[K(\alpha) : K] = \infty$

  np. $\mathbb{Q}(\Pi) \cong \mathbb{Q}(x)$, gdzie $\mathbb{Q}(\Pi) = \{\frac{f(\Pi)}{g(\Pi)} : f, g \in \mathbb{Q}[x]\}$

- Przypadek II

  α jest elementem algebraicznym

  Niech f będzie wielomianem minimalnym α

  Wtedy $Ker\ \varphi_\alpha = (f)$. Zatem z I twierdzenia o izomorfizmie $K[\alpha] \cong K[x]/_{(f)}$, gdzie f jest wielomianem minimalnym, nierozkładalnym $\Rightarrow$ pierwszym, stąd ten ideał jest maksymalny

  Ideał (f) jest maksymalny w $K[x]$

  Zatem $K[\alpha] = K(\alpha)$ jest ciałem

  Ustalmy $\beta \in K(\alpha) \qquad \beta \xrightarrow{\varphi_\alpha^{-1}} a_0 + a_1 x + ... + a_{n-1}x^{n-1} + (f)$

  $n - \deg f$

Po podstawieniu na $x\alpha$

$\beta = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$

β ma jednoznaczne przestawienie w tej postaci

$(1, \alpha, \alpha^2, ..., \alpha^{n-1})$ jest bazą rozszerzenia $K(\alpha)/_K \quad [K(\alpha) : K] = n$

Tw.: Niech α będzie elementem algebraicznym nad K i f będzie wielomianem minimalnym dla $\alpha, \deg f = n$. Wtedy

1. $K(\alpha) = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in K\}$
2. $(1, \alpha, ..., \alpha^{n-1})$ jest bazą rozszerzenia $K(\alpha)/_K$
3. $[K(\alpha) : K] = n = \deg f$

1.11.3 Rozszerzenia algebraiczne

Def.: Rozszerzenie L ciała K nazywamy **algebraicznym** jeśli każdy element $\alpha \in L$ jest algebraiczny nad K

Tw.: Każde rozszerzenie skończone jest algebraiczne

Uwaga: Odwrotne nie jest prawdziwe:
$\mathbb{Q}(\{\sqrt{p} : p-$ pierwsza $\})$ jest nieskończonym rozszerzeniem algebraicznym $\mathbb{Q}$

1.12 Wykład 12 - 20.01.15

Tw.: $L/_K$ jest rozszerzeniem skończonym $\Leftrightarrow$ L jest skończenie generowanym rozszerzeniem algebraicznym

Wn.: $K \subset L, L_{\text{alg}} = \{\alpha \in L : \alpha$ - element algebraiczny nad $K\}$ jest ciałem

Tw.: $K < L < M \ \wedge \ L/_K$ - algebraiczne $\ \wedge \ M/_L$ - algebraiczne $\Rightarrow M/_K$ - algebraiczne

1.12.1 Ciało rozkładu wielomianu

Lem.: Dla $f \in K[x]$, gdzie $\deg f > 0$ istnieje rozszerzenie $L/_K$, w którym f ma pierwiastek

Tw.: Dla dowolnego $f \in K[x], \ \deg f > 0$ istnieje rozszerzenie $L/_K$, w którym f rozkłada się na iloczym

czynników liniowych

Def.: Przypuśćmy, że $f(x) \sim (x-\alpha_1)...(x-\alpha_n), \alpha_i \in L/_K$. Wtedy ciało $K(\alpha_1,...,\alpha_n)$ nazywamy ciałem rozkładu wielomianu f

Uwaga: Ciało rozkładu wielomianu $f \in K[x]$

1. jest rozszerzeniem skończonym ciała K
2. jest najmniejszym ciałem, w którym f rozkłada się na czynniki liniowe
3. jest wyznaczone jednoznacznie z dokładnością do izomorfizmu

1.12.2 Charakterystyka ciała i podciało proste

Def.: Najmniejszą liczbę naturalną n, taką że $n \cdot 1 = \underbrace{1+...+1}_{n} = 0$ w K nazywamy charakterystyką ciała K ($char\ K = n$)
Jeśli takie n nie istnieje to mówimy, że $char\ K = 0$

Def.: Ciało K nazywamy prostym jeśli nie zawiera żadnych podciał właściwych

Tw.: Jeśli $char\ K \neq 0$ to $char\ K$ jest liczbą pierwszą

Tw.:

1. $char\ K = 0 \Rightarrow \mathbb{Q} \subseteq K$
2. $char\ K = p$ - pierwsza $\Rightarrow \mathbb{Z}_p \subset K$

(Z dokładnością do izomorfizmu)

Wn.: Każde ciało proste charakterystyki 0 jest izomorficzne z $\mathbb{Q}$

Wn.: Każde ciało proste $char\ K = p$ jest izomorficzne z $\mathbb{Z}_p$

1.12.3 Ciała skończone

Uwaga: Ciała charakterystyki 0 nie sa ciałami skończonymi $\Rightarrow$ ciała skończone mają charakterystykę p

Zadanie: Jeśli K jest ciałem skończonym $char\ K = p$ to $|K| = p^n$ dla pewnego $n \in \mathbb{N}$

Tw.: Dla dowolnej liczby $n \in \mathbb{N}$ istnieje ciało o p^n elementach

Uwaga: Ciało L z poprzedniego twierdzenia jest wyznaczone jednoznacznie z dokładnością do izomorfizmu.

Konstrukcja ciała o p^n elementach

Znajdujemy wielomian f nierozkładalny nad $\mathbb{Z}_p$ stopnia n

$\mathbb{Z}_p[x]/_{(f)} = L \quad |L| = p^n$

Np. ciało o 9 elementach: $9 = 3^2$. Weźmy $\mathbb{Z}_3$. Szukamy f nierozkładalnego $f(x) = x^2 + 1$. Nasze ciało to $\mathbb{Z}_3[x]/_{(x^2+1)}$

1.12.4 Twierdzenie Abela o elemencie pierwotnym

Lem.: Wielomian nierozkładalny nad ciałem $K,\ charK = 0$ ma tylko pierwiastki jednokrotne

1.13 Wykład 13 - 27.01.15

Tw.: (Abela o elemencie pierwotnym)

Jeśli $char\ K = 0$ oraz $L/_K$ jest skończone to $L = K(\gamma)$ (rozszerzenie proste o pewien element $\gamma \in L$)

1.13.1 Algebraiczne domknięcia ciała

Def.: Ciałem algebraicznie domkniętym K nazywamy ciało takie, że każdy $f \in K[x],\ \deg f > 0$ ma pierwiastek w K

Tw.: Następujące warunki są równoważne:

1. K - ciało algebraicznie domknięte
2. Każdy $f \in K[x]$ rozkłada się nad K na czynniki liniowe
3. K nie ma nietrywialnych rozszerzeń algebraicznych

Def.: Ciało L nazywamy **algebraicznym domknięciem** ciała K, jeśli:

1. L jest ciałem algebraicznie domkniętym
2. $L/_K$ jest rozszerzeniem algebraicznym

Tw.: Każde ciało ma algebraiczne domknięcie i jest ono wyznaczone jednoznacznie z dokładnością do izomorfizmu ($\bar{K}$) - algebraiczne domknięcie ciała K

1.13.2 Konstrukcje geometryczne

Def.: Liczbę $\alpha \in \mathbb{R}$ nazywamy **konstruowalną** jeśli mozna skonstruować odcinek o długości $|\alpha|$ za pomocą cyrkla i linijki

Tw.: Liczby konstruowalne tworzą ciało

Tw.: Liczba $\alpha \in \mathbb{R}$ jest konstruowalna witw, gdy istnieje ciąg rozszerzeń $\mathbb{Q} = K_0 \subset K_1 \subset ... \subset K_n \subset \mathbb{R}$ taki, że $\alpha \in K_n$ oraz $K_i = K_{i-1}(\sqrt{a_{i-1}})$ gdzie $a_{i-1} \in K_{i-1}$

Wn.: Z twierdzenia o wieży ciał wynika, że jeśli $\alpha \in \mathbb{R}$ jest konstruowalna to $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$

Wn.: (Tw. Wentzela)
$\alpha \in \mathbb{R}^+$ - konstruowalna $\Rightarrow$ α jest pierwiastkiem wielomianu nierozkładalnego $f \in \mathbb{Q}[x]$ $\deg f = 2^k$

Przepisał: Robert Nazar
Zastrzegam sobie prawo do błędów, proszę zgłaszać każdą nieprawidłowość znalezioną w tekście w celu naniesienia odpowiednich poprawek.