Algebra Abstrakcyjna

Przepisał: Ricko

Rok 2014/2015

Spis treści

1 Wykłady **3**

1.1 Wykład 1 - 07.10.14 . . . 3
1.1.1 Grupy . . . 3
1.1.2 Podgrupy i warstwy . . . 4
1.2 Wykład 2 - 14.10.14 . . . 5
1.2.1 Rząd grupy . . . 5
1.2.2 Rząd elementów grupy . . . 6
1.2.3 Zbiór generatorów grupy. Grupy skończenie generowane i grupy cykliczne . . . 6
1.3 Wykład 3 - 21.10.14 . . . 8
1.3.1 Homomorfizmy grup. Jądro i obraz . . . 8
1.3.2 Podgrupy normalne . . . 9
1.3.3 Centrum i komutant grupy . . . 9
1.3.4 Grupy proste . . . 10
1.4 Wykład 4 - 28.10.14 (prowadzony przez Prof. Sładka) . . . 10
1.5 Wykład 5 - 04.11.14 . . . 12
1.5.1 Skończenie generowane grupy abelowe . . . 13
1.5.2 Pierścienie i podpierścienie . . . 14
1.6 Wykład 6 - 18.11.14 . . . 15
1.6.1 Elementy odwracalne i dzielniki zera w pierścieniu . . . 15
1.6.2 Podpierścienie i ideały . . . 15
1.6.3 Pierścień ilorazowy . . . 16
1.6.4 Homomorfizmy pierścieni . . . 17
1.7 Wykład 7 - 25.11.14 . . . 18
1.7.1 Twierdzenia o izomorfizmie pierścieni . . . 18
1.7.2 Ciało ułamków pierścienia całkowitego . . . 18
1.7.3 Podzielność w pierścieniach całkowitych . . . 19
1.7.4 Największy wspólny dzielnik . . . 20
1.8 Wykład 8 - 02.12.14 . . . 20
1.8.1 Ideały pierwsze i maksymalne . . . 21
1.8.2 Pierścienie Euklidesowe . . . 22
1.9 Wykład 9 - 09.12.14 . . . 22
1.9.1 Pierścienie ideałów głównych ($P.I.D.$) . . . 24
1.9.2 Pierścienie z jednoznacznym rozkładem ($U.F.D$) . . . 24
1.10 Wykład 10 - 16.12.14 . . . 25
1.10.1 Pierścienie ułamków i lokalizacja . . . 26
1.10.2 Rozszerzenia ciał . . . 28
1.11 Wykład 11 - 13.01.15 . . . 29
1.11.1 Elementy algebraiczne i przestępne . . . 29
1.11.2 Algebraiczne i przestępne rozszerzenia proste . . . 29
1.11.3 Rozszerzenia algebraiczne . . . 30
1.12 Wykład 12 - 20.01.15 . . . 31
1.12.1 Ciało rozkładu wielomianu . . . 31
1.12.2 Charakterystyka ciała i podciało proste . . . 32
1.12.3 Ciała skończone . . . 33
1.12.4 Twierdzenie Abela o elemencie pierwotnym . . . 33

1.13 Wykład 13 - 27.01.15 33
1.13.1 Algebraiczne domknięcia ciała 34
1.13.2 Konstrukcje geometryczne 35

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:
$e = 1$
$a' = a^{-1}$

Przykłady:
1) Grupy addytywne (z dodawaniem)

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{Z}_n, +)$ $n \in \mathbb{N}$
- $(\mathbb{C}, +)$
- $(K, +)$ $K-$ dowolne ciało
- $(\mathbb{Z}[x], +)$ - wielomiany
- $(K[x], +)$ - pierścien wielomianów, gdzie K jest ciałem
- $(\mathbb{R}^2, +)$ - przestrzeń liniowa z dodawaniem wektorów
- $(V, +)$ - dowolna przestrzeń wektorowa

- $(K_m^n, +)$ - macierze
- $(\{0\}, +)$ - grupa trywialna

2) Grupy multiplikatywne (z mnożeniem)

- $(\mathbb{Q}^*, \cdot) \quad (K^* = K \backslash \{0\})$
- $(U(\mathbb{Z}_n), \cdot) \quad U(\mathbb{Z})_n = \{a \in \mathbb{Z}_n | NWD(a, n) = 1\}$
- $GL(n, k) = \{A \in K_n^n | \det A \neq 0\}$
- $SL(n, k) = \{A \in K_n^n | \det A = 1\}$

3) Grupy przekształceń

- X - zbiór
  $S(x) = \{f : X \to X\} \quad f$ - bijekcja
  z działaniem składania funkcji $\circ$
  $f \circ g : X \to f(g(x))$
  $1 : x \longmapsto x -$ element neutralny (identyczność)
- $S_n = S(\{1, ..., n\}) -$ permutacje (grupy permutacji)
- D_n - grupa izometrii n-kąta foremnego

4) Konstrukcje nowych grup z danych
a) Produkt kartezjański
$(G, \cdot), (H, *)$ - grupy
$G \times H = \{(a, b) | a \in G, b \in H\}$
$(G \times H) \circ (G \times H) \to G \times H$
$(a, b) \circ (c, d) = (a \cdot c, b * d)$
Indukcyjnie możemy uzyskać $G_1 \times ... \times G_n$
b) G - grupa $\emptyset \neq X$ - zbiór
$G^X = \{f : X \to G\}$
$f, g \in G^X \; f \bullet g : X \longrightarrow f(x) \cdot g(x)$
$\bullet$ - działanie w G^X
$\cdot$ - działanie w G
G^X jest grupą

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 $G \iff \forall_{a,b \in H} \; ab^{-1} \in H$
Dowód
$\Longrightarrow$
Proste, ponieważ wiemy, że z drugiego aksjomatu $\forall_{b \in H} \; b^{-1} \in H$ czyli b^{-1} jest elementem podgrupy, a z pierwszego, że jeśli $a \in H$ oraz $b^{-1} \in H$ to $ab^{-1} \in H$
$\Longleftarrow$
Szkic: $a = b \quad aa^{-1} = 1 \in H$
$a = 1 \quad b^{-1} \in H$
Dokładnie na ćwiczeniach

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 ($|a \cdot H| = |H|, a \in G$)
Dowód:
(2) $H = \{1, h_2, ...\}$ - w podgrupie H jest element neutralny
$a \in G$
$aH = \{a, ah_2, ..\} \Rightarrow a \in aH$
$G \subseteq \bigcup_{a \in G} aH$
$G \supseteq \bigcup_{a \in G} aH$ - suma podzbiorów grupy G
(3) $a \cdot h_1 = a \cdot h_2 \Rightarrow h_1 = h_2$ (mnożymy lewostronnie przez a^{-1})
Odwzorowanie
$H \ni h \longmapsto ah \in aH$ jest bijekcją stąd H i aH są równoliczne
(1) aH, bH - przypuśćmy, że nie są rozłączne
$\emptyset \neq aH \cap bH \Rightarrow \exists_{c \in G}\ c \in aH \cap bH$
$c = a \cdot h_1 \Rightarrow a = b \cdot h_2 \cdot h_1^{-1}$
$c = b \cdot h_2 \Rightarrow b = a \cdot h_1 \cdot h_2^{-1}$
$x \in a \cdot H \Rightarrow x = a \cdot h = b \cdot \underbrace{h_2 \cdot h_1^{-1} \cdot h}_{\in H} \Rightarrow x \in bH$, stąd $aH \subseteq bH$
$y \in b \cdot H \Rightarrow y = b \cdot h = a \cdot \underbrace{h_1 \cdot h_2^{-1} \cdot h'}_{\in H} \Rightarrow y \in aH$, stąd $bH \subseteq aH$
Zatem $aH = bH$
Twierdzenie wygląda analogicznie dla warstw prawostronnych

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

Przykłady:
(1) $\mathbb{R}^+ < \mathbb{R}^*$
$-1 \cdot \mathbb{R} = -10 \cdot \mathbb{R}$ - to samo w kontekście warstw!
$[\mathbb{R}* : \mathbb{R}^+] = |\{\mathbb{R}^+, -1 \cdot \mathbb{R}^*\}| = 2$
Z tw. Lagrange'a $\mathfrak{C} = \mathfrak{C} \cdot 2$
(2) $\{0, 3, 6, 9\} < \mathbb{Z}_{12}$
Warstwy:
$H = \{0, 3, 6, 9\} \quad |H| = 4$
$1 + H = \{1, 4, 7, 10\}$
$2 + H = \{2, 5, 8, 11\}$
Indeks: $[\mathbb{Z}_{12} : H] = 3$
Z tw. Lagrange'a $12 = 4 \cdot 3$
(3) D_n - grupa izometrii
Obroty - $O_n < D_n \qquad r = \left(\frac{2\Pi}{n}\right) \qquad s-$ symetria
Warstwy:
$O_n = \{1, r, r^2, ..., r^{n-1}\}$
$s \circ O_n = \{s, sr, sr^2, ..., sr^{n-1}\}$
$[D_n : O_n] = 2$
(4) $Gl(n, \mathbb{R})$
$Sl(n, \mathbb{R})$
Warstwy:

$$\begin{bmatrix} a & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{bmatrix} = \begin{bmatrix} a^{-1} & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{bmatrix} \cdot A$$

$[Gl(n, \mathbb{R}) : Sl(n, \mathbb{R}] = \mathfrak{C}$
$[Gl(n, \mathbb{Z}_p) : Sl(n, \mathbb{Z}_p] = p - 1$ (bez zera)

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 $r(a) = \infty$)
Przykłady:
(1) $\mathbb{Z} \quad r(1) \quad 1^k = 0$ (nigdy nie zajdzie) $\quad r(1) = -\infty$
$r(0) \quad 0^k = 0 \quad r(0) = 1$
Rząd elementu neutralnego zawsze równy jest 1
(2) $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$ - grupa z mnożeniem
$r(1) = 1$
$r(3) = 4$ bo $3^1 = 3 \quad 3^2 = 9 \quad 3^3 = 7 \quad 3^4 = 1$
$r(7) = 4$ bo $7^1 = 7 \quad 7^2 = 9 \quad 7^3 = 3 \quad 7^4 = 1$
$r(9) = 2$ bo $9^1 = 9 \quad 9^2 = 1$
Zadanie: (ćw)
$|G| < \infty \wedge a \in G \wedge r(a) = n \Rightarrow \{1, a, ..., a^{n-1}\} < G$
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
Dowód:
Ustalmy $a, b \in \langle A\rangle$. Wtedy $a, b \in H$ dla $H \in \mathcal{H}_A$, gdzie $\mathcal{H}_A = \{H < G \mid A \subseteq H\}$. Stąd $a \cdot b^{-1} \in H$ dla $H \in \mathcal{H}_A$, zatem $a \cdot b^{-1} \in \langle A\rangle$
Zauważmy, że $A \subseteq \langle A\rangle$, bo $A \subseteq H$ dla $H \in \mathcal{H}_A$
Jeśli H_0 jest dowolną podgrupą grupy G zawierającą A to $H_0 \in \mathcal{H}_A$ czyli $\langle A\rangle \subseteq H_0$

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

Przykłady:
(1) $\mathbb{Z} = \langle -1\rangle = \langle 1\rangle$ - grupa cykliczna
np. $1 + 1 + (-1) + (-1) + ...$ - tak można zbudowac każdy element z $\mathbb{Z}$
(2) $D_n = \langle r, s\rangle$ - grupa skończenie generowana
$O_n = \langle r\rangle$
(3) $\mathbb{Z}_n = \langle 1\rangle = \langle a\rangle$ gdzie $NWD(a, n) = 1$ - grupa cykliczna
(4) $U(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\} = \langle 3\rangle$ - grupa cykliczna, bo
$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 1$
$3^1 = 3 \quad 3^2 = 2 \quad 3^3 = 6 \quad 3^4 = 4 \quad 3^5 = 5 \quad 3^6 = 1$
(5) $U(\mathbb{Z}_8) = \{1, 3, 5, 7\} = \langle 3, 5\rangle$
$3^1 = 1 \quad 5^2 = 1 \quad 7^2 = 1 \quad 3 \cdot 5 = 7$

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

Stw.: Każda grupa cykliczna jest abelowa
Dowód: $G = \langle a\rangle = \{a^k \mid k \in \mathbb{Z}\}$
$a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k$

Tw.: Podgrupa grupy cyklicznej jest cykliczna
Dowód: Pokażemy, że H jest cykliczna
$H < \langle a\rangle = \{a^k \mid k \in \mathbb{Z}\}$
$l := \min\{k \in \mathbb{N}\backslash\{0\} \mid a^k \in H\}$ - na pewno istnieje
Pokażemy, że $H = \langle a^l\rangle$
" $\subseteq$ " $\quad a^l \in H \Rightarrow \langle a^l\rangle \subseteq H$
" $\supseteq$ " $\quad$ ustalmy $a^m \in H \quad (m \in \mathbb{Z})$
podzielimy m z resztą przez l
$m = l \cdot q + r$ gdzie $0 \leqslant r < l$
$a^m = a^{l\cdot q+r} = (a^l)^q \cdot a^r \Rightarrow a^r = \underbrace{(a^l)^{-q}}_{\in H} \cdot \underbrace{a^m}_{\in H} \Rightarrow a^r \in H$
Z minimalności $l \quad r = 0 \Rightarrow a^m = (a^l)^q$
dowolny element z G jest potęgą a^l

Przykład:
Jak wyglądają podgrupy grupy cyklicznej $\mathbb{Z}$
$\langle 0\rangle = \{0\}$
$\langle 1\rangle = \mathbb{Z}$

$\langle 2\rangle = \langle -2\rangle = 2\mathbb{Z} = \{a \in \mathbb{Z} \mid 2|a\}$
$\vdots$
$\langle n\rangle = \langle -n\rangle = n\mathbb{Z} = \{a \in \mathbb{Z} \mid n|a\}$

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) $Im\ \varphi < G'$
Dowód:
(1) Niepusty, bo $\varphi(1) = 1$ czyli 1 zawsze nalezy do jądra stąd $Ker\ \varphi \neq \emptyset$
Jeśli $a, b \in Ker\ \varphi$, pokażemy ,że $ab^{-1} \in Ker\ \varphi$
$\varphi(ab^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = \underbrace{\varphi(a)}_{1} \cdot \underbrace{\varphi(b^{-1})}_{1} = 1 \Rightarrow ab^{-1} \in Ker\ \varphi$ więc $Ker\ \varphi < G$
(2) $\varphi(1) = 1 \Rightarrow 1 \in Im\ \varphi \Rightarrow Im\ \varphi \neq \emptyset$
Niech $c, d \in Im\ \varphi$ to $c = \varphi(a), d = \varphi(b)$ dla pewnych $a, b \in G$. Wtedy $cd^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(ab^{-1})$.
Stąd $cd^{-1} \in Im\ \varphi$ i $Im\ \varphi < G'$

Przykłady:
1) $\varphi : G \to \{1\}$ $\quad \varphi(0) = 1$
homomorfizm trywialny $\quad Ker\ \varphi = G \quad Im\ \varphi = \{1\}$
2) $\varphi : \mathbb{Z} \to \mathbb{Z}_n \quad \varphi(a) = (a \mod n)$
$\varphi(a + b) = (a + b \mod n) = (a \mod n) \oplus (b \mod n)$
3) $\varphi : \mathbb{R}^* \to \mathbb{R}^+ \quad \varphi(a) = |a|$
$\varphi(a \cdot b) = |ab| = |a| \cdot |b| = \varphi(a) \cdot \varphi(b)$
$Ker\ \varphi = \{-1, 1\}$
$Im\ \varphi = \mathbb{R}^+$
4) $\varphi : \mathbb{R} \to \mathbb{R}^+ \quad \varphi(x) = e^x$
$\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y)$
$Ker\ \varphi = \{0\} \quad Im\ \varphi = (\mathbb{R}^+)$
5) $\varphi : Gl(n, k) \to K^* \quad \varphi(A) = \det A$
$Ker\ \varphi = Sl(n, k) \quad Im\ \varphi = K^*$

Zad.dom
Pokazać, że $\varphi : G \to G'$ jest monomorfizmem $\iff Ker\ \varphi = \{1\}$ - element neutralny

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 $\iff \forall_{a\in G}\ \forall_{h\in H}\ aha^{-1} \in H$
Dowód: $(\Rightarrow)$ $H \triangleleft G$ wtedy:
$Ha = aH$ czyli $h \cdot a = a \cdot h'$ dla dowolnych $h \in H, a \in G$
Wtedy $aha^{-1} = h' \in H$
$(\Leftarrow)$ $ah \in aH$
$ah = \underbrace{(aha)^{-1}}_{\in H} a = \underbrace{h_1}_{\in H} a \in Ha$
$ha \in Ha$
$ha = aa^{-1}ha = a(a^{-1} \cdot h \cdot a^{-1})^{-1}$
$ha \in aH$

Tw.: $\varphi : G \to G'$ - homomorfizm grup
$Ker\ \varphi \triangleleft G$
Dowód:
$a \in G \qquad h \in Ker\ \varphi$
$\varphi(aha^{-1}) = \varphi(a) \cdot \underbrace{\varphi(h)}_{1} \cdot \varphi(a^{-1}) = 1 \Rightarrow aha^{-1} \in Ker\ \varphi$

Przykłady:
1) $G \triangleleft G \qquad 1 \triangleleft G$
2) $n\mathbb{Z} \triangleleft \mathbb{Z}$
3) $Sl(n,k) \triangleleft Gl(n,k)$

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.: $Z(G) \triangleleft G$
Dowód:
* Niepusty, bo $1 \in Z(G)$
Ustalmy $a, b \in Z(G)$, pokażemy że $ab^{-1} \in Z(G)$
Niech $x \in G$
$xab^{-1} = axb^{-1} = a(bx^{-1})^{-1} = a(x^{-1}b)^{-1} = (ab^{-1})x$ stąd $ab^{-1} \in Z(G)$ czyli $Z(G) \triangleleft G$

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

Dowód:
Z definicji mamy, że $[G,G] < G$
Ustalmy $x \in G,\ h \in [G,G]$
Wtedy $h = h_1 \cdot ... \cdot h_n$ gdzie h_i - komutator
$xhx^{-1} = xh_1...xh_nx^{-1} = xh_1x^{-1} \cdot ... \cdot xh_nx^{-1}$
Pokażemy, że $xh_ix^{-1} \in [G,G]$ dla $i = 1...n$
$h_i = [a,b]$
$xh_ix^{-1} = xaba^{-1}b^{-1}x^{-1} = xax^{-1}\ xbx^{-1}\ xa^{-1}x^{-1}\ xb^{-1}x^{-1}\ \underbrace{(xax^{-1})}_{a}\ \underbrace{(xbx^{-1})}_{b}\ \underbrace{(xa^{-1}x)^{-1}}_{a^{-1}}\ \underbrace{(xb^{-1}x)^{-1}}_{b^{-1}}$

$[xax^{-1}, xbx^{-1}] \in [G,G]$
stąd $xhx^{-1} \in [G,G] \qquad [G,G] \triangleleft G$

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
Dowód:
$|G| = p$ - pierwsza $\qquad H < G$ z tw. Lagrange'a $[H]\big|[G]$
$|H| = 1 \qquad H = \{1\}$
$|H| = p \qquad H = G$

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 $aH = a'H,\ bH = b'H \Rightarrow abH = a'b'H$
Dowód:
$(\Rightarrow)$ z założenia $a^{-1}a' \in H,\ b^{-1}b' \in H$
Mamy pokazać, że $(ab)^{-1}a'b' \in H$
$(ab)^{-1}a'b' = b^{-1}a^{-1}a'b' = \underbrace{b^{-1}(a^{-1}a')b}_{\in H, bo\ H \triangleleft G} \qquad \underbrace{(b^{-1}b')}_{\in H (iloczyn\ dwoch\ z\ H)}$
$(\Leftarrow)$ - ćwiczenia

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 $Ker\ \kappa = H$
Dowód:
Grupa:
1. Łączność: $(aH)((bH)(cH)) = (aH)(bcH) = (a(bc)H) = ((ab)c)H = ((aH)(bH))(cH)$
2. Element neutralny $1 \cdot H$
3. Element odwrotny do aH to $a^{-1}H$

Homomorfizm:
$\kappa(a) \cdot \kappa(b) = abH = \kappa(ab)$
Jądro:
$Ker\ \kappa = \{a \in G : \kappa(a) = 1 \cdot H\} = \{a \in G : aH = 1 \cdot H\}\ \{a \in G : \underbrace{1^{-1}a}_{=a} \in H\} = H$

G/H - grupa ilorazowa grupy G względem H
κ - **epimorfizm kanoniczny**

Tw.: Podgrupa H grupy G jest normalna witw, gdy istnieje homomorfizm φ określony na G taki, że $H = Ker\ \varphi$
Dowód:
$(\Leftarrow)$ Było wcześniej
$(\Rightarrow)$ $H = Ker\ \kappa$, jeśli $A \triangleleft\ G$

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 $\varphi = \psi \circ \kappa$
Dowód:
Przyjmijmy, że takie ψ istnieje
$\psi(aH) = ?$ gdzie $H = Ker\ \varphi$
$\psi(aH) = \psi(\kappa(a)) = (\psi \circ \kappa)(a) = \varphi(a)$
Czy wzór jest poprawny?
Hipoteza:
$aH = a'H \overset{?}{\Rightarrow} \varphi(a) = \varphi(a')$
$\Downarrow$ $\Uparrow \setminus \cdot \varphi(a)$
$a^{-1}a' \in H = Ker\ \varphi \Rightarrow \varphi(a^{-1}) \cdot \varphi(a') = \varphi(a^{-1}a') = 1$
Możemy rozważać odwzorowanie $\psi : G/Ker\ \varphi \to G'$ $\psi(aH) = \varphi(a)$ (to jest jedyne odwzorowanie, które może spełniać tezę)
$\psi(aH \cdot bH) = \psi(abH) = \varphi(ab) = \varphi(a) \cdot \varphi(b) = \psi(aH) \cdot \psi(bH)$
$\psi \circ \kappa = \varphi$ (?)
$(\psi \circ \kappa)(a) = \psi(\kappa(a)) = \psi(aH) = \varphi(a)$
Zatem $\psi \circ \kappa = \varphi$

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 $\phi : X \to Y$
Dowód:
Określamy $\phi : X \to Y$ następująco
$\phi(K) = \kappa(K)$ dla $K \in X$
Rozważmy odwzorowanie $\psi : Y \to X$ określone
$\psi(L) = \kappa^{-1}(L)$ dla $L \in Y$
Wystarczy pokazać, że $\phi \circ \psi = id_Y$ oraz $\psi \circ \phi = id_x$
$L \in Y \Rightarrow (\phi \circ \psi)(L) = \kappa(\kappa^{-1}(L)) = L$ tzn. $\phi \circ \psi = id_Y$
$K \in X \Rightarrow (\psi \circ \phi)(K) = \kappa^{-1}(\kappa(K)) \supseteq L$ tzn.
Trzeba pokazać inkuzję w drugą stronę
Niech $g \in \kappa^1(\kappa(K)) \Rightarrow \kappa(g) \in \kappa(K) \Rightarrow \kappa(g) = \kappa(k)$ dla $k \in K \Rightarrow \kappa(gk^{-1}) = 1 \cdot H \Rightarrow gk^{-1} \in H \subset K \Rightarrow g = gk^{-1} \cdot k \in K$

Stąd $\kappa^{-1}(\kappa(K)) = K$
$\phi \circ \psi = id_X$

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 $[G,G] \in H$
Dowód:
$\Rightarrow$ Załóżmy, że $H \triangleleft G,\ G/H$ - abelowa
Stąd $aH \cdot bH = bH \cdot aH$
Zatem $\forall_{a,b \in H}\ [a,b] \in H$
$\underbrace{aba^{-1}b^{-1}}_{[a,b]} H = H$, a więc $[G,G] \subset H$
$\Leftarrow$ Przypuśćmy, że $[G,G] \subset H$ tzn. $\forall_{a,b \in G}\ aba^{-1}b^{-1} \in H$
H-normalna (?)
Weźmy $a \in G,\ h \in H$ i rozważmy
$aha^{-1} = \underbrace{(aha^{-1}h^{-1})}_{\in H} \underbrace{h}_{\in H} \in H$ tzn. $H \triangleleft G$
G/H-abelowa (?)
$aH \cdot bH = abH$
$ba \underbrace{(a^{-1}b^{-1}ab)}_{\in H} H = baH = bH \cdot aH$

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 $[G_{i+1}, G_{i+1}] \subset G_i$

Przykłady:
1. Każda grupa abelowa jest rozwiązalna ($\{1\} = G_0 \triangleleft G$)
2. D_n jest rozwiązalna, bo $\{id\} \triangleleft O_n \triangleleft D_n$
3. S_n jest rozwiązalna, bo można utworzyć ciąg $\{id\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$
4. Jeżeli G jest nieabelową grupą prostą to G nie jest rozwiązalna np. $g = A_5$
$f \in K[X]$ (wielomiany) $\longleftrightarrow G(K,f)$ - Grupa Galois wielomianów f
Równanie $f(x) = 0$ można efektywnie rozwiązać $\Leftrightarrow G(K,f)$ jest rozwiązalna

1.5 Wykład 5 - 04.11.14

Przypomnienie rzeczy z poprzedniego wykładu
Przykład zastosowania twierdzenia o izomorfizmie:
$\varphi : Gl(n,k) \to K^*$
$\varphi(A) = \det A$
$Ker\ \varphi = Sl(n,k)$
$Gl(n,k)/_{Sl(n,k)} \cong K^*$ - przenoszą się ciekawe własności

Rozwiązywalność:
• $\{1\} = H_0 \triangleleft H_1 \triangleleft ... \triangleleft H_n = G$
Zawsze zachodzi sytuacji $\{1\} \triangleleft G$, gdy G jest abelowa jest okej
$H_{n+1}/_{H_i}$ $G/_{\{1\}} \cong G$, gdy G nie jest abelowa to $G/_{\{1\}}$ tez nie jest abelowa (własności przenoszą sie przez izomorfizm)
• $\{1\} \triangleleft D_n$ - to nie jest dobry przykład
$\{1\} \triangleleft \underbrace{O_n}_{cykliczna} \underbrace{\triangleleft}_{indeks\ =\ 2} D_n$
$|\ D_n/_{O_n}\ | = 2 \to$ cykliczna $\to$ abelowa
• S_n parzyste permutacje - $A_n \triangleleft S_n$

$S_n/_{A_n}$ - abelowa
dla $n = 3$
$\{1\} \triangleleft \underbrace{A_3}_{3\ elementy} \triangleleft \underbrace{S_3}_{6\ elementow}$
$A_3/_{\{1\}} = 3$ cykle
$n = 4$
$\{1\} \triangleleft \underbrace{V_4}_{4\ elementy} \triangleleft \underbrace{A_4}_{12\ elementow} \triangleleft \underbrace{S_4}_{24\ elementy}$
$V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$
$n = 5$
$\{1\} \triangleleft \underbrace{A_5}_{prosta,\ nieabelowa} \triangleleft S_5$

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 $\mathbb{Z}_n$
Dowód:
$G = \langle a \rangle = \{1, a, a^2, ..., a^{n-1}\}$
$\varphi : G \to \mathbb{Z}_n$
$\varphi : a \longmapsto 1$
$\varphi(a^k) = \underbrace{1 \oplus ... \oplus 1}_{k} = k$
homomorfizm + epimorfizm + monomorfizm = izomorfizm

Tw.: Produkt grup skończenie generowanych jest grupą skończenie generowaną
Dowód:
$G = \langle a_1, ..., a_n \rangle$
$H = \langle b_1, ...b_m \rangle$
$G \times H = \langle (a_i, 1), (1, b_j) \mid i = 1...n\ j = 1...m \}$
$(a, b) = (a_1, 1)^{k_1} \cdot ... \cdot (a_n, 1)^{k_n} \cdot (1, b_1)^{l_1} \cdot ... \cdot (1, b_m)^{l_m}$
$a = a_i^{k_i} \cdot ... \cdot a_n^{k_n}$
$b = b_j^{l_j} \cdot ... \cdot b_m^{l_m}$

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)$n_i \geqslant 2 \qquad n_i | n_{i+1}$ dla $i = 1...s-1$
Szkic dowodu:
G - dowolna grupa abelowa
$T(G) = \{a \in G \mid r(a) < \infty\}$ - podgrupa **torsyjna**
$T(G) \triangleleft G$
$G/_{T(G)}$ - grupa **beztorsyjna** (jedynym elementem skończonego rzędu jest 1)
$G \cong \underbrace{G/_{T(G)}}_{\mathbb{Z}^k} \underbrace{\times T(G)}_{\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_s}}$ - skończone jeśli G skończenie generowane

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**

(1) Kwaterniony Hamiltona
$\mathbb{H} \ni h = a + bi + cj + dk \qquad a, b, c, d \in \mathbb{R}$
$i^2 = j^2 = k^2 = -1$
$ij = -ji = k$
$jk = -kj = i$
$ki = -ik = j$
$(a + bi + cj + dk) = a - bi - cj - dk$
2) Pierścień wielomianów: $\mathbb{R}[X], \mathbb{C}[X], \mathbb{Q}[X], \mathbb{Z}[X]$ - pierścienie przemienne z 1
3) $X \neq \emptyset$
$\mathcal{P}(X) = \{A \subseteq X\}$
$A \div B = A \backslash B \cup \ B \backslash A$ (dodawanie)
$A \cap B$ (mnożenie)

Konstrukcje nad pierścieniami
1) P_1, P_2 - pierścienie
$P_1 \times P_2 = \{(a, b) : a \in P_1, b \in P_2\}$
$(a, b) + (c, d) = (\underbrace{a + c}_{P_1}, \underbrace{b + d}_{P_2})$
$(a, b) \cdot (c, d) = (\underbrace{ac}_{P_1}, \underbrace{bd}_{P_2})$
Dzięki zastosowaniu indukcji otrzymać możemy $P_1 \times ... \times P_2$
2) $X \neq \emptyset$
$P^X = \{f : X \to P \mid f$ - funkcja $\}$
$f + g : x \longmapsto f(x) + g(x)$
$f \cdot g : x \longmapsto f(x) \cdot g(x)$
3) $P^\infty = \{(a_1, a_2, ...) \mid a_i \in P\}$
4) $\sum_{i=0}^{\infty} a_i x^i \quad a_i = 0$ prawie wszędzie
$(a_0, ..., a_n, 0, 0...)$
$P[X] = \{\sum_{i=0}^{\infty} a_i x^i \ \big| \ a_i = 0 \ \text{ prawie wszędzie } \}$
$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$
$\sum_{i=0}^{\infty} a_i x^i \cdot \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} c_i x^i$ gdzie $c_i = \sum_{j+k=i} a_j b_k$

5) $Mn(P) = \left\{ \begin{array}{ccc} a_{11} & \ldots & a_{1n} \\ & & \\ a_{n1} & & a_{nn} \end{array} \Big| a_{ij} \in P \right\}$
Z działaniami dodawanie i mnożenia macierzy
UMOWA
Pierścień - przemienny z 1

1.6 Wykład 6 - 18.11.14

1.6.1 Elementy odwracalne i dzielniki zera w pierścieniu

Def.: Element $a \in P\backslash\{0\}$ nazywamy **dzielnikiem zera** jeśli istnieje $b \in P\backslash\{0\}$ 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

Przykłady:
1) $\mathbb{Z}$ $D(\mathbb{Z}) = \emptyset$ $U(\mathbb{Z}) = \{-1, 1\}$
2) $\mathbb{Z}_6$ $D(\mathbb{Z}_6) = \{2, 3, 4\}$ $U(\mathbb{Z}_6) = \{1, 5\}$
3) $\mathbb{R}$ $D(\mathbb{R}) = \emptyset$ $U(\mathbb{R}) = \mathbb{R}^*$ pierścień całkowity
4) $\mathbb{Z}\times\mathbb{R}$ $D(\mathbb{Z}\times\mathbb{R}) = \{(a, 0), (0, b) \mid a \in \mathbb{Z}\backslash\{0\},\ b \in \mathbb{R}^*\}$ $U(\mathbb{Z}\times\mathbb{R}) = \{(a, b) \mid a \in \{-1, 1\},\ b \in \mathbb{R}^*\}$

Zadanie domowe:
P, Q - pierścienie
$D(P \times Q) = [(D_0(P) \times Q) \cup (P \times D_0(Q))]\backslash\{0\}$
$U(P \times Q) = U(P) \times U(Q)$
gdzie $D_0(P) = D(P) \cup \{0\},\ D_0(Q) = D(Q) \cup \{0\}$

Stw. Przypuśćmy, że $0 \neq a \in P\backslash D(P)$
$ab = ac \Rightarrow b = c$
Dowód:
$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow \underbrace{a}_{\neq 0}(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$

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

Tw.: $|P| < \infty \Rightarrow P = \{0\} \cup D(P) \cup U(P)$
Dowód:
$X \neq 0$ $x \in P$
Rozważmy funkcję $a \longmapsto ax$
$|P| < \infty$
f różnowartościowa: bijekcja (bo na zbiorze skończonym), $1 = x \cdot y$ $y \in P$ x - odwracalny
f nie jest różnowartościowa $ax = bx$, $a \neq b$, $b \in P$ $x\underbrace{(a - b)}_{\neq 0} = 0$, x - dzielnik zera

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

Def.: Podpierścień I pierścienia P nazywamy **ideałem** jeśli
$\forall_{a\in I}\ \forall_{x\in P}\quad ax \in I \qquad I \lhd P$

Przykłady:
1) $(0) \lhd P$ ideał zerowy
2) $n\mathbb{Z} \lhd \mathbb{Z}$
3) $\mathbb{Q} < \mathbb{R}$
4) $P < P[X]$

$\emptyset \neq A \subset P$
$(A) = \{ \sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N}, a_i \in A, x_i \in P \}$
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 $I \cap U(P) \neq \emptyset \Leftrightarrow I = P$
Dowód:
$(\Leftarrow)$
$I = P \ni 1$ odwracalna w każdym pierścieniu $(1 \in U(P))$
$(\Rightarrow)$
$U \in I \cap U(P) \Rightarrow U^{-1}U = 1 \in I \Rightarrow \forall_{x\in P}\ x \cdot 1 \in I \Rightarrow P = I$

Tw.: P jest ciałem $\Longleftrightarrow$ P ma dokładnie dwa ideały
Dowód:
$(\Rightarrow)$
$(0) \neq I \lhd P \Rightarrow \exists_{a\neq 0}\ a \in I \Rightarrow a \in U(P) \cap I \Rightarrow P = I$ (Z lematu)
$(\Leftarrow)$
$a \neq 0\ a \in P$
Rozważmy ideał główny generowany przez a
$(a) \neq (0) \Rightarrow (a) = P$ (dwa ideały)
$(a) = \{ax \mid x \in p\} \Rightarrow$ (z tego obok i z powyższego) $\Rightarrow 1 = ax \Rightarrow a \in U(P) \Rightarrow P$ - ciało

1.6.3 Pierścień ilorazowy

Niech I będzie ideałem pierścienia P $I \lhd P$
$x + I = \{x + a \mid a \in I\}$ - warstwa pierścienia P względem ideału I
$P/_I$ - zbiór warstw

Stw.: $x + I = y + I \Leftrightarrow x - y \in I$
Dowód:
$(\Rightarrow)$
$x + I = y + I \Rightarrow x \in y + I \Leftrightarrow \exists_{a\in I}\ x = y + a$ Przenosimy y na drugą stronę i mamy $\exists_{a\in I}\ x - y = a \in I$
$(\Leftarrow)$
$x + I \subset y + I$
$x + a = x + (y - x) + i = y + i \Rightarrow x + a \in y + I$
$a = (y - x) + \underbrace{i}_{\in I}$
Analogicznie: $y + b = y + (x - y) + j = x + j \Rightarrow y + b \in x + I$

Działania na zbiorze warstw:
$(a + I) + (b + I) = (a + b) + I$
$(a + I) \cdot (b + I) = (a \cdot b) + I$
Pokażemy, że działania sa poprawnie określone

$a + I = c + I \Leftrightarrow a - c \in I$
$b + I = d + I \Leftrightarrow b - d \in I$
$(a + b) - (c + d) = (a - c) + (b - d) \in I \Leftrightarrow (a + b) + I = (c + d) + I$
$ab - cd = ab + ad - ad - cd = \underbrace{\underbrace{a\underbrace{(b-d)}_{\in I}}_{\in I} - \underbrace{(a-c)}_{\in I}\underbrace{d}_{\in I}}_{\in I} \Rightarrow ab + I = cd + I$

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)

Przykłady:

1. $\varphi : P \to (0)$ homomorfizm zerowy
2. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$
   $\varphi(a) = (a \mod n)$
3. $\varphi : P[X] \to P \quad a \in P$
   $\varphi_a(f) = f(a)$ homomorfizm pierścieni
   $f(x) = \sum_{i=0}^{\infty} a_i x^i \qquad g(x) = \sum_{i=0}^{\infty} b_i x^i \qquad a_i, b_i = 0$ p.w.
   $\varphi_a(f + g) = \big(\sum_{i=0}^{\infty} (a_i + b_i)x^i\big) = \sum_{i=0}^{\infty} (a_i + b_i)a^i = \sum_{i=0}^{\infty} a_i a^i + \sum_{i=0}^{\infty} b_i a^i = f(a) + g(a) = \varphi_a(f) + \varphi_a(g)$
   $\varphi_a(fg) = \varphi_a\big(\sum_{i=0}^{\infty} \big(\sum_{k+j=i} a_k b_j\big)x^i\big) = \sum_{i=0}^{\infty} \big(\sum_{k+j=i} a_k b_j\big)a^i = \sum_{k=0}^{\infty} a_k x^k \cdot \sum_{j=0}^{\infty} b_j a^j = \varphi_a(f) \cdot \varphi_a(g)$
4. $x \neq \emptyset \quad \varphi_a : P^X \to P$
   $\varphi_a(f) = f(a) \qquad a \in X$
5. $I \triangleleft P$
   $\kappa : P \to P/_I$
   $\kappa(a) = a + I$ homomorfizm kanoniczny

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

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

Przykłady:

1. $Ker\ \varphi = P \qquad Im\ \varphi = 0$
2. $Ker\ \varphi = n\mathbb{Z} \qquad Im\ \varphi = \mathbb{Z}_n$
3. $Ker\ \varphi_a = \{f \in \mathbb{R}[X] \mid f(a) = 0\} \overset{tw.}{=} \{f \in \mathbb{R}[X] \mid (x - a)|f\} = f(a) = (x - a)g(x)$
   Twierdzenie Bezout
   $(a) = \{a \cdot b \mid b \in \mathbb{R}\}$
4. $Im\ \varphi_a = P$
5. $Ker\ \varphi = I \qquad Im\ \varphi = P/_I$

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
Dowód:
W jedną stronę oczywiste, w drugą:: homomorfizm $\kappa : P \to P/_I \quad I = Ker\ \kappa$

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 $I \triangleleft P,\ R < P$. Wtedy:

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

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

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

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

Zadanie Domowe:
$I \subset A \triangleleft P \Rightarrow A/_I \triangleleft P/_I$

Przykład:
$\mathbb{R}[X]/_{(x)} \cong R$
(x) - ideał główny generowany przez x
$\varphi : \mathbb{R}[X] \to R$
$\varphi(f) = f(0)$ - wymyślamy homomorfizm
przyporządkowanie wielomianowi wartości jest homomorfizmem
φ jest epimorfizmem, bo $\varphi(a) = a$
$Ker\ \varphi = \{f \in \mathbb{R}[X] \mid f(0) = 0\} = \{f \in \mathbb{R}[X] \mid f(x) = x \cdot g(x)\}$
$(x) = x \cdot g(x) \mid g(x) \in f[X]$
Z I twierdzenia o izomorfizmie $\mathbb{R}[X]/_{(x)} \cong R$

1.7.2 Ciało ułamków pierścienia całkowitego

P - pierścień całkowity (bez dzielników zera)
Na zbiorze $P \times P^*$ definiujemy relację (równoważności)
$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad - bc = 0$
$(a, b) \sim (c, d) \Leftrightarrow ad - bc = 0$
Zwrotna i symetryczna

Przechodniość:
$(a,b) \sim (c,d) \Leftrightarrow ad - bc = 0 \Leftrightarrow adf - bcf = 0$ (operacja możliwa bo pierścień jest całkowity)
$(c,d) \sim (e,f) \Leftrightarrow cf - de = 0$
$cf = de$ wstawiamy do pierwszego równania
$adf - bde = 0 \ / : d$ można dzielić przez, bo d nie jest dzielnikiem zera
$af - be = 0$
$(a,b) \sim (e,f)$ - mamy przechodniość
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:
$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$
Zadanie domowe: Sprawdzić czy te działania są poprawnie określone

Przypomnienie:
P - pierścień całkowity $\Rightarrow P[X]$ - pierścień całkowity
$f \cdot g = 0$
$f(a) \cdot g(a) = 0 \quad a \in P$
$f(a) \neq 0$
$g(a) = 0$

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

Przykłady:

1. $Quot(\mathbb{Z}) = \mathbb{Q}$
2. $Quot(K[X]) = K(X)$
   K - ciało $\qquad K(X) = \{\frac{f}{g} : f,g \in K[X],\ g \neq 0\}$ - ciało funkcji wymiernych
3. $Quot(P[X]) = \underbrace{Quot(P)}_{K}(X) \qquad P$ - pierścień całkowity
4. K - ciało $\qquad Quot(P) \cong K$ z dokładnością do izomorfizmu
   $a,b \in K \qquad \frac{a}{b} = \frac{ab^{-1}}{1} \longmapsto ab^{-1}$

1.7.3 Podzielność w pierścieniach całkowitych

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

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

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
Dowód:
Zakładamy, że $p \in P$ - pierwszy
Przypuśćmy, że $p = a \cdot b \Rightarrow a \in U(P) \vee b \in U(P)$
$P = a \cdot b \Rightarrow \begin{cases} a|p \wedge b|p \\ p|a \vee p|b \end{cases} \quad p - \text{pierwszy} \quad \Leftrightarrow p \sim a \vee p \sim b$ czyli $b \in U(P) \vee a \in U(P)$

Przykład: (że twierdzenie odwrotne nie zachodzi)
$P = \mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ (Ponadto ten zbiór jest też podpierścieniem $\mathbb{C}$)
P - pierścień przemienny z 1, całkowity (podpierścień pierścienia całkowitego $\mathbb{C}$)
$2 \in P$
Załóżmy, że $2 = (a + b\sqrt{-6})(c + d\sqrt{-6}) \Rightarrow |2|^2 = 4 = (a^2 + 6b^2)(c^2 + 6d^2) \Rightarrow 4 = 1 \cdot 4 \Rightarrow b = 0$ $a = \pm 1$
a - element odwracalny
2 jest nierozkładalna w $\mathbb{Z}[\sqrt{-6}]$
$-6 = \underbrace{\sqrt{-6} \cdot \sqrt{-6}}_{\in P} = \underbrace{2 \cdot (-3)}_{\in P}$
$2|\sqrt{-6} \cdot \sqrt{-6}$, ale $2 \not| \sqrt{-6}$, bo $\frac{1}{2}\sqrt{-6} \notin \mathbb{Z}[\sqrt{-6}] \Rightarrow 2$ nie jest elementem pierwszym w $\mathbb{Z}[\sqrt{-6}]$

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 $NWD(a, b) \sim 1$

Przykład:
$NWD(a, b)$ nie zawsze istnieje
$P = \mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$ - pierścień całkowity
$a = 6 \qquad b = 2\sqrt{-6}$
$6 = (a + b\sqrt{-6})(c + d\sqrt{-6})$
Podnosimy do kwadratu (sprzężenie)
$36 = (a^2 + 6b^2)(c^2 + 6d^2)$
Możliwe rozłożenia:
$1 \quad 36 \quad a = \pm 1 \quad b = 0 \ \sim 1$
~~$2 \quad 18$~~
~~$3 \quad 12$~~
$4 \quad 9 \quad a \pm 2 \quad b = 0 \ \sim 2$
$6 \quad 6 \quad a = 0 \quad b = \pm 1 \ \sim 1$
$\frac{6}{1} = 6 \qquad \frac{6}{2} = 3 \qquad \frac{6}{\sqrt{-6}} = -\sqrt{-6}$
$D(6) \sim \{1, 2, 3, \sqrt{-6}, 6\}$

$2\sqrt{-6}$
Podnosimy do kwadratu (sprzężenie)
$24 = (a^2 + 6b^2)(c^2 + 6d^2)$
$1 \quad 24 \quad a = \pm 1 \quad b = 0$
~~$2 \quad 12$~~
~~$3 \quad 8$~~
$4 \quad 6 \quad a = \pm 2 \quad b = 0$
$\frac{2\sqrt{-6}}{1} = 2\sqrt{-6}$
$\frac{2\sqrt{-6}}{2} = \sqrt{-6}$
$D(2\sqrt{-6}) \sim \{1, 2, \sqrt{-6}, 2\sqrt{-6}\}$

$D(6, 2\sqrt{-6}) = \{1, 2, \sqrt{-6}\}$
$2 \not| 1 \qquad \frac{1}{2} \notin \mathbb{Z}[\sqrt{-6}]$
$2 \not| \sqrt{-6} \qquad \frac{\sqrt{-6}}{2} \notin \mathbb{Z}[\sqrt{-6}]$
$\sqrt{-6} \not| 2 \qquad \frac{2}{\sqrt{-6}} = \frac{2\sqrt{-6}}{-6} = -\frac{1}{3}\sqrt{-6} \notin \mathbb{Z}[\sqrt{-6}] \Longrightarrow$
Nie ma $NWD(a, b)$

1.8.1 Ideały pierwsze i maksymalne

Def.: Ideał $I \lhd P$ nazywamy **pierwszym** jeśli:
$ab \in I \Rightarrow a \in I \vee b \in I$

Def.: Ideał właściwy $I \lhd P$ nazywamy **maksymalnym** jeśli:
$I \lhd J \lhd P \Rightarrow I = J \vee J = P$

Przykłady:
(0) jest ideałem pierwszym w pierścieniu całkowitym i maksymalnym w ciele

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
Dowód:
(1) Weźmy $a, b \in (p) \Leftrightarrow ab = p \cdot x \Leftrightarrow p|ab \Leftrightarrow p|a \vee p|b \Leftrightarrow a \in (p) \vee b \in (p)$
(2) ($\Rightarrow$) Przypuśćmy $(p) \lhd (a) \lhd P \Rightarrow p \in (a) \Rightarrow p = ab \Rightarrow$ (nierozkładalność) $a \in U(P) \vee b \in U(P) \Rightarrow (a) = P \vee p \sim a \Rightarrow (a) = (p)$
($\Leftarrow$) $p = ab \Rightarrow p \in (a) \Rightarrow (p) \lhd (a) \lhd P \Rightarrow (p) = (a) \vee (a) = P \Rightarrow p \sim a \vee a \in U(P) \Rightarrow b \in U(P) \vee a \in U(P)$
Stąd p jest nierozkładalny

Zadanie Domowe:
1) $a \sim b \Leftrightarrow (a) = (b)$
2) $a \in (b) \Leftrightarrow (a) \subset (c)$

Przykład: $P = \mathbb{Z}[X] \qquad I = (X - 2)$
I - pierwszy, ale nie maksymalny
$(X - 2) \subset (X - 2, 3) \subset P$ (ale bez równości)

Tw.: (o charakteryzacji ideałów za pomocą pierścieni ilorazowych)
1) $I \lhd P$ jest ideałem pierwszym $\Leftrightarrow P/_I$ jest pierścieniem całkowitym
2) $I \lhd P$ jest ideałem maksymalnym $\Leftrightarrow P/_I$ jest ciałem
Dowód:
1) $(a + I)(b + I) = (0 + I) \Leftrightarrow (ab + I) = I \Leftrightarrow ab \in I \Leftrightarrow a \in I \vee b \in I \Leftrightarrow a + I = I \vee b + I = I$
2) ($\Rightarrow$) Przypuśćmy, że $J \lhd P/_I$ Wtedy (z IV twierdzenia o izomorfizmie) $J = J/_I$, gdzie $I \lhd J \lhd P$
Z maksymalności $I \quad J = I \vee J = P$
Stąd $J = (0 + I)$ lub $J = P/_I \Rightarrow P/_I$ jest ciałem
($\Leftarrow$) Przypuśćmy, że $I \lhd J \lhd P$. Wtedy $J/_I \lhd P/_I$ - ciało
Stąd $J/_I = (0 + I) \vee J/_I = P/_I$, (z IV tw. o izomorfizmie:) $J = I \quad J = P \qquad \square$

Przykłady:
$\mathbb{Z}[X]/_{(X-2)} \cong \mathbb{Z} \Longrightarrow (x - a)$ jest ideałem pierwszym, ale nie maksymalnym w $\mathbb{Z}[X]$
$\mathbb{R}[X]/_{(X-2)} \cong \mathbb{R} \Longrightarrow (x - a)$ jest ideałem pierwszym i maksymalnym w $\mathbb{R}[X]$

Wn.: Każdy ideał maksymalny jest pierwszy

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

Przykład:
Dowolone ciało ma jeden ideał czyli jest pierścieniem lokalnym

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) $N(0) = 0$
2) $N(ab) = N(a) \cdot N(b)$
3) $\forall_{a,b \in P} \exists_{r,q \in P} \quad a = bq + t \wedge N(r) < N(b) \quad N(b) \neq 0$

Przykłady:
1) K - ciało $\qquad N(a) = 0$
2) $\mathbb{Z} \qquad N(a) = |a|$
3) $\mathbb{Z}[i] \qquad N(a + bi) = a^2 + b^2$
4) K - ciało, $K[X] \qquad N(f) = 2^{\deg f} \longleftarrow$ Zadanie domowe

Dowody:
Dwa pierwsze podpunkty są proste
3) $z = a + bi \; w = c + di \qquad a, b, c, d \in \mathbb{Z}$
$\frac{a+bi}{c+di} = q_1 + q_2 i \quad q_i \in \mathbb{Q}$
$k_1, k_2 \in \mathbb{Z} \quad |q_i - k_i| \leqslant \frac{1}{2}$
$a + bi = (c + di) \cdot (k_1 + k_2 i) + r \qquad\qquad z = wq + r \;\; N(r) < N(w)$
$r = (a + bi) - (c + di)(k_1 + k_2 i) = (c + di)\big[\frac{a+bi}{c+di} - (k_1 + k_2 i)\big]$
$= (c + di)[q_1 + q_2 i - k_1 - k_2 i] = c + di\big[(q_1 - k_1) + (q_2 - k_2)i\big]$
$N(r) = N(c + di) \cdot \big[\underbrace{(q_1 - k_2)^2}_{\leqslant \frac{1}{4}} + \underbrace{(q_2 - k_2)^2}_{\leqslant \frac{1}{4}}\big] \leqslant \frac{1}{2} N(w) < N(w) \qquad \square$

$P-$ pierścień euklidesowy
$a, b \in P \qquad 0 < N(b) < N(a)$
$a = b \cdot q_1 + r_1 \qquad N(r_1) < N(b)$
$b = r_1 q_2 + r_2 \qquad N(r_2) \leqslant N(r_1)$
$r_1 = r_2 q_3 + r_3 \qquad N(r_2) \leqslant N(r_2)$
$\vdots$
$r_{n-2} q_n + r_n$
$r_{n-1} q_{n+1} + x \qquad N(x) = 0 \Leftrightarrow x = 0$
Algorytm Euklidesa $\uparrow$

Tw.: W pierścieniach euklidesowych $NWD(a, b)$ zawsze istnieje (o ile $a \neq 0, b \neq 0$)
$r_n = r_{n-2} - r_{n-1} q_n$
$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$
$\vdots$
Trzeba pokazać, że $r_n = NWD(a, b)$

1.9 Wykład 9 - 09.12.14

Inna definicja pierścienia Euklidesowego

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

Przykłady: (z nową definicją)

1. K-ciało jest pierścieniem Euklidesowym z normą

$N(a) = \begin{cases} 0 & a = 0 \\ 1 & a \neq 0 \end{cases}$

W ciele r "znika"

2. $\mathbb{Z}$ $\quad |a| = N(a)$
3. $\mathbb{Z}[i]$ $\quad a^2 + b^2 = N(a + bi)$
4. $K[X]$ $\quad N(f) = 2^{\deg\ f}$

Tw.: W pierścieniu euklidesowym istnieje $NWD(a, b)$ $\ a, b \in P^*$
Dowód:
1 $\ a = bq_1 + r_1 \quad N(r_1) \quad r_n \mid a$
2 $\ b = r_1q_2 + r_2 \quad N(r_2) \quad r_n \mid b$
3 $\ r_1 = r_2q_3 + r_3 \quad N(r_3) \quad r_n \mid r_1$
$\vdots$
n $\ r_{n-2} = r_{n-1}q_n + r_n \quad N(r_n) \quad r_n \mid r_{n-2}$
$n+1$ $\ r_{n-1} = r_nq_{n+1} + 0 \quad N(0) = 0 \quad r_n \mid r_{n-1}$
Niemalejący ciąg reszt $\uparrow$
Pokażemy, że $r_n = NWd(a, b)$
Przypuśćmy, że $c|a \wedge c|b$
$\Downarrow$
$c|r_1$
$c|r_2$
$c|r_3$
$\vdots$
$c|r_n$
Stąd mamy, że $r_n \sim NWD(a, b)$
Ten algorytm działa w każdym pierścieniu euklidesowym
Istnieją $x, y \in P$ takie, że $NWD(a, b) = ax + by$

Zadanie domowe:
$P-$pierścień euklidesowy
1) $N(a) = 1 \iff a \in U(P)$
2) $N(a) = p$ (liczba pierwsza) $\Rightarrow a$-nierozkładalny

Tw.: W pierścieniu euklidesowym każdy ideał jest główny
Dowód:
$I \triangleleft P$ - euklidesowy
$I = (0)$ - główny
Możemy założyć, że I nie jest zerowy $(I \neq (0))$
Rozważmy zbiór $N = \{N(a) : a \in I \backslash \{0\}\} \subseteq \mathbb{N}$
Każdy podzbiór liczb naturalnych jest dobrze uporządkowany. Zbiór N ma zatem element minimalny $k = N(d)$ dla pewnego $d \in I$
Pokażemy, że ideał I jest generowany przez element d
Inkluzja $\supseteq$ jest oczywista
Ustalmy $a \in I$. Wtedy istnieją $q, r \in P$ takie, że $a = dq + r$ i $N(r) < N(d)$
Zauważmy, że $\underbrace{r}_{\in I} = \underbrace{a}_{\in I} - \underbrace{dq}_{\in I}$.
Z minimalności $N(d)$, mamy że $N(r) = 0$, zatem $r = 0$
Zatem jeśli $r = 0,\ a = dq,\ a \in I$(a należy do ideału generowanego przez d, $I \subseteq (d)$ $\quad \square$

Przykłady: (pierścienie nieeuklidesowych)

1. $NWD(6, 2\sqrt{-6})$ nie istnieje, więc $\mathbb{Z}\sqrt{-6}$ nie jest euklidesowy
2. $(x, 2)$ nie jest główny w $\mathbb{Z}[x]$ stąd $\mathbb{Z}[x]$ nie jest euklidesowy

3. $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} \quad D \in \mathbb{Z} \quad D \neq a^2 \quad a \in \mathbb{Z}$
   $N(a + bi) = |a^2 + b^2 D|$
   $\frac{a+b\sqrt{D}}{c+d\sqrt{D}} = q_1 + q_2\sqrt{D} \qquad q_1, q_2 \in \mathbb{Q} \quad k_i \in \mathbb{Z}$
   $|k_i - q_i| \leqslant \frac{1}{2}$
   $(a + b\sqrt{D}) = (c + d\sqrt{D})(k_1 + k_2\sqrt{D}) + r$
   $r(a + b\sqrt{D}) - (c + d\sqrt{D})(k_1 + k_2\sqrt{D})$
   $r = (c + d\sqrt{D})[(q_1 - k_1) + (q_2 - k_2)\sqrt{D}]$
   Norma: $|(q_1 - k_1)^2 - (q_2 - k_2) \cdot D| < 1$ Wtedy mamy normę euklidesową
   $D = \pm 2$ - wtedy jest to pierścień euklidesowy (nie przekracza 1)
   $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\sqrt{3}]$ - pierścienie euklidesowe

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
Wskazówka:
$\exists_d \quad \underbrace{(a, b)}_{\text{ideał główny}} = (d)$
Należy pokazać, że d to $NWD(a, b)$ oraz jednoznaczność (dwa ideały są równe to ich elementy są stowarzyszone)

Tw.: W pierścieniu ideałów głównych każdy ideał pierwszy jest maksymalny
Dowód:
$I \triangleleft P \quad P - P.I.D$
$I = (p)$ - ideał pierwszy $\Leftrightarrow$ p - element pierwszy $\Rightarrow$ p - element nierozkładalny $\Leftrightarrow$ (p) jest ideałem maksymalnym w rodzinie ideałów głównych $\Rightarrow$ I jest maksymalny $\square$

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

Przykład:
$P[X] - P.I.D. \Leftrightarrow P$ jest ciałem
$(\Leftarrow) P$ - ciało, $P[X]$ - euklidesowy $\Rightarrow P - P.I.D.$
$(\Rightarrow) P[X]/_{(x)} \cong P$
$P[X] - P.I.D. \Rightarrow P[X]$ - pierścień całkowity $\Rightarrow P$ - całkowity, stąd i z powyższej linijki mamy: (x) - ideał pierwszy $\Rightarrow (x)$ - ideał maksymalny $\Rightarrow P$ jest ciałem (ilorazujemy przez ideał maksymalny)

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 $\delta \in S_n$)

Przykłady:

1. K - ciało (nie ma takich a)

2. $\mathbb{Z}$ (Zasadnicze Twierdzenie Arytmetyki)

3. $\mathbb{Z}[\sqrt{-6}]$
   $6 = 2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$
   $2 = (a + bi\sqrt{-6})(c + di\sqrt{-6})$
   $4 = (a^2 + 6b^2)(c^2 + 6d^2)$ (kwadraty modułów)
   $\not{2} \not{\cdot} \not{2} \Rightarrow a = \pm 1 \in U(P)$
   To nie jest rozkład, 2 jest nierozkładalna
   $6 = 2 \cdot 3 = -(\sqrt{-6}) \cdot \sqrt{-6}$
   Elementy nierozkładalne (dwa różne rozkłady)
   $\mathbb{Z}[\sqrt{-6}]$ nie jest *U.F.D.*
   W $\mathbb{Z}$ $6 = 2 \cdot 3 = (-2) \cdot (-3)$ - stowarzyszenie

Tw.: W pierścieniu z jednoznacznym rozkładem każdy element nierozkładalny jest pierwszy
Dowód:
$P - U.F.D$
$p \in P^* \backslash U(P)$ p - nierozkładalny
Przypuśćmy, że $p|ab \Rightarrow ab = p \cdot k \quad k \in P \Rightarrow \underbrace{(p_1 \cdot ... \cdot p_n)}_{\text{rozkład } a} \cdot \underbrace{(q_1 \cdot ... \cdot q_m)}_{\text{rozkład } b} = p \underbrace{(r_1 \cdot ... \cdot r_s)}_{\text{rozkład } k}$
p_i, q_j, r_l - elementy nierozkładalne
Z jednoznaczności rozkładu:
$\exists_i \ p \sim p_i \vee \exists_j \ p \sim q_j \Rightarrow p|a \vee p|b$

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
Dowód:
($\Rightarrow$) Poprzednie twierdzenie
($\Leftarrow$)
Przypuśćmy, że $a = (p_1 \cdot ... \cdot p_n) = (q_1 \cdot ... \cdot q_m)$
$p_i, q_j -$ nierozkładalne
Indukcja:
$n = 1$ - oczywiste
$\left.\begin{array}{l} p_1 - \text{el. nierozkładalny - pierwszy} \\ p_1 | q_1 \cdot ... \cdot q_m \end{array}\right\} \Longrightarrow p_1 | q_j \quad j \in \{1...m\}$
Bez straty ogólności $p_1|q_1$
Wtedy
$\left.\begin{array}{l} q_1 = p_1 \cdot x \\ q_1 - \text{nierozkładalny} \end{array}\right\} \Longrightarrow x \in U(P) \Rightarrow q_1 \sim p_1$
$a = p_1 \cdot (p_2 \cdot ... \cdot p_n) = p_1 \cdot (x \cdot q_2 \cdot ... \cdot q_m)$
Z założenia indukcyjnego: $n = m \quad p \sim q\delta(i)$ dla $\delta(i) \in S_n$

Tw.: $P - P.I.D. \Rightarrow P - U.F.D.$
Dowód:
Wystarczy pokazać na mocy poprzedniego twierdzenia, że każdy element $a \in P * \backslash U(P)$ ma rozkład na elementy nierozkładalne
Szkic:
$a = r_1 \cdot r_2 = (r_{11} \cdot r_{12}) \cdot r_2 = ...$

1.10 Wykład 10 - 16.12.14

Tw.: $P - P.I.D. \Rightarrow P - U.F.D.$
Dowód:
$r \in P^* \backslash U(P)$
r - nierozkładalny $\vee \ r = r_1 \cdot r_2$
r_1 - nierozkładalny $\vee \ r_1 = r_{11} \cdot r_{12} \cdot r_2$
r_{11} - nierozkładalny $\vee \ r_{11} = r_{111} \cdot r_{112} \cdot ...$

...
$r = r_1 \cdot r_2 = r_{11} \cdot r_{12} \cdot r_2 = r_{111} \cdot r_{112} \cdot r_{12} \cdot r_2 = ...$
$\underbrace{(r)}_{=I_0} \subset \underbrace{(r_1)}_{=I_1} \subset \underbrace{(r_{11})}_{=I_2} \subset ...$
$\bigcup_{i=0}^{\infty} I_i \lhd P$
$P - P.I.D. \Rightarrow \bigcup_{i=0}^{\infty} I_i = (a)$ dla pewnego $a \in P$
Dla pewnego $n,\ a \in I_n$
$(a) \subseteq I_n \subseteq I_{n+1} \subseteq ... \subseteq (a)$
$I_n = \underbrace{(r_{1...1})}_{n} = \underbrace{(r_{1...1})}_{n+1}$
$\underbrace{r_{1...1}}_{n} \sim \underbrace{r_{1...1}}_{n+1} \sim ... \sim a$
Ponieważ w P każdy element nierozkładalny jest pierwszy więc na mocy poprzedniego twierdzenia P jest pierścieniem $U.F.D.$

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 $U.F.D.$
Dowód: (Zad. dom.)
Ciała: $\mathbb{R}, \mathbb{C}, \mathbb{Z}_p$
Pierścienie euklidesowe: $K[x], \mathbb{Z}[i], \mathbb{Z}[\sqrt{\pm 2}], \mathbb{Z}$
$P.I.D. : \mathbb{Z}[\frac{\sqrt{-19}}{2}]$
$U.F.D. : \mathbb{Z}[x_1...x_n], K[x_1...x_n]$
Pierścienie całkowite: $\mathbb{Z}[\sqrt{-6}], \mathbb{Z}[\sqrt{5}]$

NWD, NWW są w $U.F.D.$

Przypomnienie:
$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^0 ...$
$64 = 2^6 \cdot 3^0 \cdot 5^0 \cdot 7^0 ...$
$NWD(72, 64) = 2^3 \cdot 3^0 \cdot 5^0 \cdot 7^0 ...$
$NWD(72, 64) = 2^6 \cdot 3^2 \cdot 5^0 \cdot 7^0 ...$
$P - U.F.D.$
$\mathbb{P}$ - zbiór reprezentantów elementów nierozkładalnych klas abstrakcji relacji stowarzyszenia
Wtedy $a \in P^* \backslash U(P)$
$a \sim \prod_{p \in \mathbb{P}} P^{V_p(a)}$
$V_p(a) \in \mathbb{N} \cup \{0\}$
$V_p(a) = \max\{n \in \mathbb{N} \cup \{0\} : p^n | a\}$
$V_p(a) = 0$ prawie wszędzie

Uwaga:
$a|b \Leftrightarrow \forall_{p \in \mathbb{P}}\ V_p(a) \leqslant V_p(b)$
$a \sim \prod_{p \in \mathbb{P}}\ p^{V_p(a)} \qquad b \sim \prod_{p \in \mathbb{P}}\ p^{V_P(b)}$
$NWD(a, b) \sim \prod_{p \in \mathbb{P}}\ p^{\min\{V_p(a), V_p(a)\}}$
$NWW(a, b) \sim \prod_{p \in \mathbb{P}}\ p^{\max\{V_p(a), V_p(a)\}}$

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. $a, b \in S \Rightarrow ab \in S$

Przykłady:

1. $U(P)$
2. $P-$ całkowity $\Rightarrow P^* = S$
3. $S = P \backslash D_0(P)$
4. $\underbrace{I \lhd P}_{\text{właściwy}} \Rightarrow S = 1 + I$

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

Przykłady:

1. $S = U(P)$
   $\varphi : P \to S^{-1}P$ jest epimorfizmem, bo $as^{-1} \mapsto \frac{a}{s}$
   φ - izomorfizm $\quad \frac{a}{s} = \frac{as^{-1}}{1}$
   $S^{-1}P \cong P$
2. $P =$ pierścień całkowity
   $S = P^*$
   $S^{-1}P = Quot(P)$

Lem.: Jeśli I jest ideałem pierwszym pierścienia P to $P/_I$ jest zbiorem multiplikatywnym
Dowód:
$1 \notin I \Rightarrow 1 \in P/_I$
$0 \in I \Rightarrow 0 \notin P/_I$
$ab \notin P/_I \Rightarrow ab \in I \Rightarrow a \in I \ \vee \ b \in I \Rightarrow a \notin P/_I \ \vee \ b \notin P/_I$

Tw.: Niech I będzie ideałem pierwszym pierścienia P i niech $S = P/_I$. Wtedy S^{-1} jest pierścieniem lokalnym (ma dokładnie jeden ideał maksymalny)
Dowód:
$S^{-1}P = \{\frac{a}{s} : a \in P, s \notin I\}$
$S^{-1}I = \{\frac{a}{s} : a \in I, s \notin I\}$
$\underbrace{\frac{a_1}{s_1}}_{\in I} - \underbrace{\frac{a_2}{s_2}}_{\in I} = \frac{a_1 s_2 - a_2 s_1 \ \in I}{s_1 s_2 \ \notin I} \in S^{-1}I$
$\frac{a}{s_1} \cdot \frac{x}{s_2} = \frac{ax \ \in I}{s_1 s_2 \ \notin I} \in S^{-1}I$

$S^{-1}P/_{S^{-1}I} = \{\frac{a}{s} : a \in \underbrace{P/_I}_{S} \ \wedge \ \underbrace{s \in P/_I}_{S}\} = U(S^{-1}P)$

Czyli wszystkie właściwe ideały pierścienia $S^{-1}P$ zawierają się w $S^{-1}I$ tzn. $S^{-1}I$ jest jedynym ideałem maksymalnym pierścienia $S^{-1}P$

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

Przykłady:

1. $Z_{(P)} = \{\frac{a}{b} \in Q \mid NWD(a,b) = 1 \Rightarrow p \not| \ b\}$
2. $K[x]_{(x)} = \{x^k \frac{f(x)}{g(x)} \mid f(0) \neq 0 \ \wedge \ g(0) \neq 0 \ \wedge \ k > 0\}$

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 $[L:K] < \infty$

Przykłady:

1. $\mathbb{C}/_{\mathbb{R}} \qquad z = 1 \cdot x + yi \quad x, y \in \mathbb{R}$
   $\mathcal{B}_{\mathbb{C}/_{\mathbb{R}}} = \{1, i\} \qquad [\mathbb{C} : \mathbb{R}] = 2$
2. $K(x)/_K$ - nie jest roszerzeniem skończonym
   $(1, x, x^2...)$ - liniowo niezależne

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

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

Dowód:
$\mathcal{B}_{L/_K} = \underbrace{(\alpha_1 ... \alpha_n)}_{\in L}$
$\mathcal{B}_{M/_K} = \underbrace{(\beta_1 ... \beta_m)}_{\in M}$
Pokażemy, że $\mathcal{B} = (\alpha_i, ..., \beta_j, ...)$ $i = 1..n, \ j = 1..m$ jest bazą $M/_K$
Ustalmy $\beta \in M$
$\beta = \sum_{j=1}^{m} b_j \beta_j \qquad b_j \in L$ - przedstawienie jest jednoznaczne
$b_j = \sum_{i=1}^{n} a_{ij} \cdot \alpha_i \quad a_{ij} \in K$ - przedstawienie jest jednoznaczne
$\beta = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} \alpha_i \beta_j \quad a_{ij} \in K$ - przedstawienie jest jednoznaczne
Stąd: $\mathcal{B}$ jest bazą $M/_K \qquad |\mathcal{B}| = nm$

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**

Przykłady:

1. Każdy element $a \in K$ jest algebraiczny nad $K \quad (f(x) = x - a)$
2. $\sqrt{2}$ jest algebraiczny nad $\mathbb{Q} \quad (f(x) = x^2 - 2)$
3. $i \in \mathbb{C}$ jest algebraiczny nad $\mathbb{Q}$ i $\mathbb{R} \quad (f(x) = x^2 + 1)$
4. $\sqrt{x}$ jest algebraiczny nad $R(X)$ (funkcje) $\quad (f(T) = T^2 - x)$
5. $\sqrt{2} + \sqrt{3}$ jest algebraiczne nad $\mathbb{Q} \quad (f(x) = x^4 - 10x^2 + 1)$
6. Π, e nie są algebraiczne nad $\mathbb{Q}$, ale są algebraiczne nad $\mathbb{R}$

Liczby algebraiczne to elementy algebraiczne nad $\mathbb{Q}$
Liczby przestępne to elementy przestępne nad $\mathbb{Q}$

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
Dowód:
Niech f będzie wielomianem najniższego stopnia o własności $f(\alpha) = 0$. BSO możemy założyć, że f jest unormowany. Przypuśćmy, że $f(x) = f_1(x) \cdot f_2(x)$ (rozkładalny), gdzie $\deg f_i < \deg f$
Wtedy $0 = f(\alpha) = f_1(\alpha) \cdot f_2(\alpha)$ i ponieważ ciało L jest pierścieniem całkowitym otrzymujemy, że $f_1(\alpha) = 0$ lub $f_2(\alpha) = 0$ co jest sprzeczne z minimalnością stopnia wielomianu f
Przypuśćmy, że $g(\alpha) = 0$ i $\deg g = \deg f$, g-unormowany. Wtedy $f(x) = g(x) \cdot \underbrace{q(x)}_{\text{stała}} + r(x)$ i $\deg r(x) < \deg g(x)$
Mamy $0 = f(\alpha) = r(\alpha)$ czyli z minimalności $\deg f$ mamy $r = 0$
Z nierozkładalności f otrzymujemy, że $f \sim g$. Ponieważ f i g sa unormowane mamy $f = g \qquad \square$

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 $\beta \in K(\alpha)$ $\quad \beta \xrightarrow{\varphi_\alpha^{-1}} a_0 + a_1 x + ... + a_{n-1}x^{n-1} + (f)$
  $n - \deg f$
  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. $[K(\alpha) : K] = n = \deg f$

Przykłady:

1. $\alpha = \sqrt{2} \quad f(x) = x^2 - 2$
   Wielomian ten jest: unormowany, $f(\sqrt{2}) = 0$, nierozkładalny z kryterium Eisensteina dla $p = 2$ lub $I = (2)$ (zależnie od wersji kryterium), stąd f jest minimalny
   $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$
   Baza: $\mathbb{Q}(\sqrt{2})/_{\mathbb{Q}} = \{1, \sqrt{2}\}$
   $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}i : a, b \in \mathbb{Q}\}$

2. $\alpha = 1 + \sqrt[3]{2}$
   $x = 1 + \sqrt[3]{2} \quad x - 1 = \sqrt[3]{2}\Big|^3 \Rightarrow x^3 - 3x^2 + 3x - 3 = 0$ - minimalny z kryterium Eisensteina
   $f(x) = x^3 - 3x^2 + 3x - 3$
   $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$
   $\mathcal{B}_{\mathbb{Q}(\alpha)/_{\mathbb{Q}}} = \{1, \alpha, \alpha^2\}$
   $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\} = \{(a + b + c + 1) + (b + 2c)\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\} = \{d + e\sqrt[3]{2} + f\sqrt[3]{4} : d, e, f \in \mathbb{Q}\} = \mathbb{Q}(\sqrt[3]{2})$

3. $\varepsilon_3 = \cos\frac{2\Pi}{c} + i\sin\frac{2\Pi}{3} = -\frac{1}{2} \qquad z^3 = 1$
   $x^3 - 1 = (x - 1)(x^2 + x + 1)$ - nierozkładalny nad $\mathbb{R}$
   $f(x) = x^2 + x + 1$ - wielomian minimalny dla ε_3
   $[\mathbb{Q}(\varepsilon_3) : \mathbb{Q}] = 2$
   $\mathcal{B}_{\mathbb{Q}}(\varepsilon_3)/_{\mathbb{Q}} = \{1, \varepsilon_3\}$
   $\mathbb{Q}(\varepsilon_3) = \{a + b \cdot \varepsilon_3 : a, b \in \mathbb{Q}\}$

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
Dowód:
$[L : K] < \infty$
Ustalmy $\alpha \in L$
Przypuśćmy, że α - przestępny nad K
Wtedy $[K(\alpha) : K] = \infty$
$K < K(\alpha) < L$
Z twierdzenia o wieży ciał mamy sprzeczność
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
Dowód:
$\{\alpha_1, ..., \alpha_n\}$ - Baza $L/_K$
$L = K(\alpha_1, ..., \alpha_n)$ - skończenie generowane

$$\left.\begin{array}{l} K < \underbrace{K(\alpha_i)}_{\in L} < L \\ [L : K] < \infty \end{array}\right\} \Longrightarrow [K(\alpha_i) : K] < \infty \Leftrightarrow \alpha_i \text{ - algebraiczne nad } K$$

Wn.: $K \subset L, L_{\text{alg}} = \{\alpha \in L : \alpha$ - element algebraiczny nad $K\}$ jest ciałem
Dowód:
$\alpha, \beta \in L_{\text{alg}} \Rightarrow \alpha, \beta$ - algebraiczne nad K
$K(\alpha, \beta)$ - rozszerzenie skończone ciała $K \Rightarrow K(\alpha, \beta)/_K$ - rozszerzenie algebraiczne

$$\left.\begin{array}{l} \text{Weźmy } \alpha, \beta \in K(\alpha, \beta) \\ \beta \neq 0,\ \alpha\beta^{-1} \in K(\alpha, \beta) \end{array}\right\} \Rightarrow \alpha - \beta \text{ i } \alpha\beta^{-1} \text{ - algebraiczne nad } K \Rightarrow \alpha - \beta \wedge \alpha\beta^{-1} \in L_{\text{alg}}$$

Czyli jest to zbiór domknięty ze wzlgędu na działanie

Tw.: $K < L < M \ \wedge \ L/_K$ - algebraiczne $\wedge\ M/_L$ - algebraiczne $\Rightarrow M/_K$ - algebraiczne
Dowód:
$\alpha \in M,\ \alpha$ - algebraiczny nad L (bo $M/_L$ - rozszerzenie algebraiczne)
$\exists_{f \in L[x]}\ f(\alpha) = 0$
$f(x) = a_0 + a_1 x + ... + a_n x^n$, gdzie $a_i \in L$. Rozważmy ciało $K(a_0, ..., a_n)$
$[K(a_0, ..., a_n) : K] < \infty$
$[K(a_0, ..., a_n, \alpha) : K(a_0, ..., a_n)] \leqslant n < \infty$ Stosując twierdzenie o wieży ciał otrzymujemy
$[K(a_0, ..., a_n)(\alpha) : K] < \infty \Rightarrow K(a_0, ..., a_n, \alpha)$ - rozszerzenie algebraiczne ciała $K \Rightarrow \alpha$ - algebraiczne nad K

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
Dowód:
Ideał (f) zawiera się w pewnym ideale maksymalnym I.
Rozważmy homomorfizm kanoniczny $\kappa : K[x] \to \underbrace{K[x]/_I}_{\text{ciało}} := L$. Odwzorowanie $\kappa\big|_K : K \to L$ jest zanurzeniem ciała K w ciało L (czyli ciało K możemy traktować jako podciało ciała L)
Obliczmy $f(\kappa(x))$
$f(\kappa(x)) = a_0 + a_1\kappa(x) + ... + a_n(\kappa(x))^n = a_0 + a_1(x+I) + ... + a_n(x+I)^n = \underbrace{(a_0 + a_1 x + ... + a_n x^n)}_{f(x)} + I = 0$
w L

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

Dowód: (indukcja po $\deg f$)
$\deg f = 1 \Rightarrow f$ - liniowy
Załóżmy, że $\deg f = n-1$, f - rozkładalny. Czy $\deg f = n > 1$?
Z lematu istnieje $K/_L$ takie, że $f(x) = (x-\alpha_1)\cdot g(x)$, gdzie $\alpha_i \in K_1, g \in K_1[x]$ i $\deg g = n-1$
Z założenia indukcyjnego istnieje L/K_1 takie, że $g(x) \sim (x-\alpha_1)...(x-\alpha_n) \quad \alpha_1,...,\alpha_n \in L$
Wtedy $f(x) \sim (x-\alpha_1)...(x-\alpha_n)$ - rozkład w $L[x]$

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

Przykłady:

1. $\underbrace{f(x)}_{\in\mathbb{Q}[x]} = x^4 - 5x^2 + 6 = (x^2-2)(x^2-3) = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$
   $\mathbb{Q}(\sqrt{2}, \underbrace{-\sqrt{2}}_{\text{przeciwny do}\sqrt{2}}, \sqrt{3}, \underbrace{-\sqrt{3}}_{\text{przeciwny do}\sqrt{3}}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ - ciało rozkł.
   Jeśli chcemy sprawdzić stopień rozszerzenia:
   Wieża ciał: $\mathbb{Q} < \mathbb{Q}(\sqrt{2}) < \mathbb{Q}(\sqrt{2},\sqrt{3})$
   $\mathbb{Q} < \mathbb{Q}(\sqrt{2}) : x^2-2$ - wielomian nierozkładalny - minimalny dla $\sqrt{2}$ oraz $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, Baza: $\{1,\sqrt{2}\}$
   $\mathbb{Q}(\sqrt{2}) < \mathbb{Q}(\sqrt{2},\sqrt{3}) : x^2-3$ - wielomian nierozkładalny w $\mathbb{Q}(\sqrt{2})$ - minimalny dla $\sqrt{3}$ oraz $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$, Baza: $\{1,\sqrt{3}\}$
   $\big[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\big] = 4$. Baza: $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$
2. $f \in \mathbb{Q}[x],\ f(x) = x^6 - 1 = (x-1)(x-\varepsilon_6)(x-\varepsilon_6^2)\cdot...\cdot(x-\varepsilon_6^n) \qquad \varepsilon_6 = \cos\frac{2\Pi}{6} + i\sin\frac{2\Pi}{6}$

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
Dowód:
$char\ K = n$, gdzie $n = s\cdot t \quad 1 < s,t < n$

$$\left.\begin{array}{l} n\cdot 1 = (s\cdot 1)(t\cdot 1) = 0 \text{ w } K \\ K - \text{ciało} \Rightarrow \text{p. całkowity} \end{array}\right\} \Rightarrow \text{sprzeczność}$$

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)
Dowód:

1. $\varphi : \mathbb{Z} \to K,\ \varphi(K) = \underbrace{1 + ... + 1}_{K} = k \cdot 1$ - jest to monomorfizm pierścieni

   Odwzorowanie $\Phi : \mathbb{Q} \to K$ dane wzorem $\Phi(\frac{k}{l}) = (k \cdot 1)(l \cdot 1)^{-1} = \varphi(k) \cdot \varphi(l)^{-1}$ jest zanurzeniem ciała $\mathbb{Q}$ w ciało K

2. $\varphi : \mathbb{Z}_p \to K \quad \varphi(K) = k \cdot 1$ - zanurzenie ciał

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 $n \in \mathbb{N}$

Przykład:
$\mathbb{Z}_p(x)$ - ciało nieskończone charakterystyki p

Tw.: Dla dowolnej liczby $n \in \mathbb{N}$ istnieje ciało o p^n elementach
Dowód:
Weźmy $f \in \mathbb{Z}_p[x]$, taki że $f(x) = x^{p^n} - x$. Istnieje ciało K, w którym $f(x) = (x - \alpha_1) \cdot ... \cdot (x - \alpha_{p^n})$
Niech $L := \{\alpha_1, ..., \alpha_{p^n}\}$. Wystarczy pokazać, że L jest ciałem.

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
Dowód:
$f(x) = (x - \alpha)^k \cdot g(x)$
$f'(x) = (x - \alpha)^{k-1} \cdot g(x) + (x - \alpha)^k \cdot g'(x) = (x - \alpha)^{k-1} \cdot h(x)$
$\neg NWD(f, f') \sim 1,\ char\ K = 0 \Rightarrow \deg f' = \deg f - 1 \Rightarrow f' \neq 0$
f - nierozkładalny, $NWD(f, f') \sim 1$ - sprzeczność

Przykład:
$K = \mathbb{Z}_p(x^p),\ f(t) = t^p - x^p \in K[x],\ x \notin K,\ f(x) = 0 \quad f(t) = (t - x)^p,\ f'(t) = 0$

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 $\gamma \in L$)
Dowód:
Pokażemy krok indukcyjny czyli $\underbrace{K(\alpha, \beta)}_{\text{alg.}} = K(\gamma)$ dla pewnego $\gamma \in K(\alpha, \beta)$

$K[x] \ni f(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_k)$ - wielomian minimalny dla α nad ciałem K
$K[x] \ni g(x) = (x - \beta_1)(x - \beta_2)...(x - \beta_l)$ - wielomian minimalny dla β nad ciałem K
Załóżmy:
$\alpha_1 = \alpha$

$\beta_1 = \beta$
Rozważmy zbiór $\{\frac{\alpha_i - \alpha}{\beta - \beta_j}\ i = 1...k,\ j = 2...l\} = A$
Z charakterystyki wiemy, że K jest nieskończone, stąd: $K \backslash A \neq \emptyset$
Ustalmy $d \in K \backslash A$
Definiujemy $\gamma = \alpha + d\beta$
Pokażemy, że $\beta \in K(\gamma)$ " $\subseteq$ "
Weźmy
$K(\gamma)[x] \ni r(x) := f(\gamma - dx) \Rightarrow r(\beta) = 0$
$K(\gamma)[x] \ni h(x)$ - wielomian minimalny dla β nad ciałem $K(\gamma)$
Mamy $h(x) \big| g(x) \wedge h(x) \big| r(x)$
Z tego wynika, że pierwiastki wielomianu h należą do zbioru $\{\beta_1 ... \beta_l\}$
Przypuśćmy, że $r(\beta_j) \qquad (\beta_j \neq \beta) \Rightarrow$
$f(\underbrace{\gamma - d\beta_i}_{\alpha_i}) = 0$
$\gamma - d\beta_j = \alpha_i$
$\alpha + d\beta - d\beta_j = \alpha_i$
$\alpha + d(\beta - \beta_j) = \alpha_i$
$d = \frac{\alpha_i - \alpha}{\beta - \beta_j}$ - sprzeczność
Jedynym pierwiastkiem h jest β to oznacza $h(x) = x - \beta$
$\beta \in K(\gamma)$
Wtedy:
$\alpha = \underbrace{\gamma}_{\in K(\gamma)} - d \underbrace{\underbrace{\beta}_{\in K(\gamma)}}_{\in K(\gamma)}$
Zatem $K(\alpha, \beta) \subset K(\gamma)$

Przykład:
$d = 1$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$
Wielomian minimalny dla $\sqrt{2} : (x - \sqrt{2})(x + \sqrt{2})$
Wielomian minimalny dla $\sqrt{3} : (x - \sqrt{3})(x + \sqrt{3})$

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

Przykład: $\mathbb{C}$
Ciała skończone odpadają: $K = \{a_1, ..., a_n\} \qquad f(x) = (x - a_1)...(x - a_n) + 1$ - Nie ma pierwiastka w tym ciele!

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

Przykład:
$\bar{\mathbb{Q}} = \{z \in \mathbb{C} : \exists_{f \in \mathbb{Q}[x]} f(z) = 0\} \subseteq \mathbb{C}$ - nieprzeliczalne
Przeliczalne ciało algebraicznie domknięte

1.13.2 Konstrukcje geometryczne

$\alpha \in \mathbb{N}$ - da się skonstruować
$\alpha \in \mathbb{Q}$ - da się skonstruować (Tw. Talesa)
$\sqrt{n},\ n \in \mathbb{N}$ - da się skonstruować (przeciwprostokątne kolejnych trójkątów prostokątnych)
$\sqrt[3]{2}$ =?

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
Dowód:
α, β - konstruowalne (dodatnie)
$\alpha + \beta$ - da się
$\alpha - \beta$ - da się
$\alpha\beta$ - da się (Tw. Talesa)
$\frac{\alpha}{\beta}$ - da się (Tw. Talesa)

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 $a_{i-1} \in K_{i-1}$
Dowód:
($\Leftarrow$)
$K(\sqrt{a}) \ni x + y\sqrt{a}$ - konstruowalne, itd. wchodzimy do góry
($\Rightarrow$)
$ax + by + c = 0$
$dx + ey + f = 0$
$F = K($ współczynników prostych i okręgów, za pomocą których konstruujemy element $\alpha)$
Wystarczy pokazać, że w takiej konstrukcji każdy element $\alpha \in K(\sqrt{a})$

1. Punkt przecięcia dwóch prostych
   $\begin{cases} k_1x + k_2y + k_3 = 0 \\ l_1x + l_2y + l_3 = 0 \end{cases}$ $\Rightarrow$ punkt przecięcia ma współrzędne w K
2. Punkt przecięcia prostej i okręgu
   $\begin{cases} k_1x + k_2y + k_3 = 0 \\ x^2 + y^2 + l_1x + l_2y + l_3 = 0 \end{cases}$ $\Rightarrow Ax^2 + Bx + C = 0$ (wszystkie współczynniki z K)
   $x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A} \in K(\sqrt{a})$
3. Przecięcie się okręgów
   $\begin{cases} x^2 + y^2 + k_1x + k_2y + k_3 = 0 \\ l_1x + l_2y + l_3 = 0 \end{cases} \Rightarrow \begin{array}{l} x^2 + y^2 + k_1x + k_2y + k_3 = 0 \\ (k_1 - l_1)x + (k_2 - l_2)y + (k_3 - l_3) = 0 \end{array}$
   Wracamy do pkt.2

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 $\Rightarrow \alpha$ jest pierwiastkiem wielomianu nierozkładalnego $f \in \mathbb{Q}[x]$ $\deg f = 2^k$

Przykłady:

- Kwadratura koła
  $\sqrt{\Pi}$ - nie jest liczbą algebraiczną
- Podwojenie sześcianu
  $f(x) = x^3 - 2$ - nierozkładalny, stopień nie jest potęgą 2

- Trysekcja kąta
  φ - dany kąt
  $\cos 3\varphi = 4\cos^3 \varphi - 3\cos \varphi$
  $\cos \varphi = 4\cos^3 \frac{\varphi}{3} - 3\cos \frac{\varphi}{3}$
  $f(x) = 4x^3 - 3x - \cos \varphi$
  Jeśli f jest nierozkładalny to konstrukcja nie jest wykonalna

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