1. Podstawowe pojęcia algebraiczne

Z – zbiór liczb całkowitych
Z^* - zbiór liczb całkowitych dodatnich (bez zera)
Z_0^* – zbiór liczb całkowitych dodatnich z zerem
Q – zbiór liczb wymiernych

1.1 Grupa

Jest to pewna struktura algebraiczna (zbiór z wyszczególnionym działaniem i elementem neutralnym)

$$(G,*,e) = (G,\bullet,1)$$

Gdzie:
G – zbiór
* - działanie
E – element neutralny, zazwyczaj oznaczamy przez 1

Aksjomaty, które spełnia Grupa:
1) łączność, np. a*(b*c)=(a*b)*c
2) a*1 = 1*a = a
3) $\forall_{a\in G}\exists_{a'\in G} \longrightarrow (a * a' = 1)$
4) Grupa jest abelowa (przemienna) jeśli a * b = b * a dla każdego a i b $\in$ G.

Grupą multiplikatywną nazywamy grupę G z działaniem mnożenia ($\bullet$) i elementem neutralnym 1.

Grupą addytywną nazywamy grupę G z działaniem (+) i elementem neutralnym 0.

Przykłady:

$$G=(Z,+,0)$$
$$G=(Z \setminus \{0\},\bullet,1)$$

1.2 Pierścień

$P=(P,+,\bullet;0,1)$

Klasy aksjomatów spełniane przez pierścień:
1) P z działaniem + i elementem 0 to grupa abelowa (warunki 1-4)
2) P z działaniem * i elementem 1 spełnia warunki 1,2 i 4
3) Rozdzielność dodawania względem mnożenia

$$\forall_{a,b,c\in P} a*(b+c) = a*b + a*c$$

Strukturę spełniającą te trzy klasy warunków nazywana jest **Pierścieniem przemiennym z jedynką**.

Neutralny element grupy multiplikatywnej nazywamy jedynką pierścienia.
Neutralny element grupy addytywnej nazywamy zerem pierścienia.

Przykład:
(pierścień wielomianów naz Z):

P=(Z [x],+,*,0,1)

1.3 Ciało

Jest to pierścień spełniający dodatkowy warunek:
Dla każdego niezerowego elementu a z ciała K istnieje element a' również należący do K, taki, że a * a'=1 tzn. każdy niezerowy element tego ciała posiada element odwrotny.

Przykład:

K = (Q,+,*,0,1)

Def.
Pierścień P nazywamy Dziedziną Całkowitości wtedy i tylko wtedy gdy zachodzi warunek

$$\forall_{a,b\in P} a*b = 0 \Rightarrow a = 0 \vee b = 0$$

(tzn. nie zawiera nitrywialnych dzielników zera).

1.4 Relacja podzielności (|) w dziedzinie całkowitości.

$$a \mid b \Rightarrow \exists_{c\in P} a*c = b$$ (a dzieli b)

Własności relacji podzielności:

1) zwrotność i przechodniość
2) $a \mid b \Rightarrow \forall_c a * c \vee b * c$
3) $a \mid b \wedge a \mid c \Rightarrow a \mid b * u + c * v \forall_{c,v \in P}$
4) Jeśli a dzieli 1 to element a jest odwracalny
5) Jeśli 0 dzieli a to ten element musi być równy 0

Def.
Elementy niezerowe a oraz b, należące do pierścienia P nazywamy **stowarzyszonymi** wtedy i tylko wtedy gdy a dzieli b oraz b dzieli a.

Wniosek:
Elementy są stowarzyszone wtedy i tylko wtedy gdy różnią się o element odwracalnym tzn.

$$\exists_{u \in P} a = u * b$$

Dowód:

$a \mid b \wedge b \mid a \Rightarrow \exists_{c_1, c_2 \in P} a * c1 = b \wedge b * c2 = a \Rightarrow a * c1 * c2 = a$

$a * (c_1 * c_2 - 1) = 0$

$(c_1 * c_2 - 1) = 0$

Zatem $c_1 * c_2 = 1$ z czego wynika, że c_1 oraz c_2 są elementami odwracalnymi.

Stowarzyszonym z 0 jest tylko 0, natomiast z 1 wszystkie elementy odwracalne pierścienia P.

Def.
Element a należący do pierścienia P, który nie jest stowarzyszony ani z 0 ani z 1 nazywamy nierozkładalnym wtedy i tylko wtedy gdy każdy dzielnik jest stowarzyszony z 1 lub nim samym.

Def.
Element a należący do pierścienia P nazywamy pierwszym wtedy i tylko wtedy gdy:

$$\forall_{a,b} a \mid b * c \Rightarrow a \mid b \vee a \mid c$$

I element a nie jest stowarzyszony z 0 ani 1.

Wniosek:
W dowolnej dziedzinie całkowitości P, każdy element pierwszy jest nierozkładalny.

Dowód:
Gdyby $p \in P$ był rozkładem to p = ab | ab skąd ab | a lub ab | b i dalej b | 1 lub a | 1 co jest niemożliwe.

Def.
Dziedzinę całkowitości P nazywamy **Dziedziną z Jendoznacznocią** Rozkładu (DJR) wtedy i tylko wtedy gdy:

1) każdy element rozkładalny jest iloczynem pewnej liczby elementów pierwszych
2) przedstawienie elementu rozkładalnego w postaci iloczynu elementów pierwszych jest jednoznaczne z dokładnością do porządku i stowarzyszenia.

Przykład:
$(Z,+,\bullet,1,0)$
6 = 2*3 = 3*2
6 = (-2)*(-3) ale -1 jest stowarzyszone z 1.

Tw.
Jeśli P jest Dziedziną z Jednoznacznością Rozładu to P[x] też jest Dziedziną z jednoznacznością Rozkładu.

Wniosek:
Każdy wielomian unormowany o współczynnikach całkowitych można przedstawić w postaci iloczynu unormowanych wielomianów nierozkładalnych nad Z.

Def.
Największym Wspólnym Dzielnikiem elementów a oraz b należących do pierścienia P jest taki element d należący do P że:
1) $d \mid a \wedge d \mid b$
2) $\forall_c c \mid a \wedge c \mid b \Rightarrow c \mid d$

Def.
Najmniejszą Wspólną Wielokrotnością elementów a oraz b należących do pierścienia P jest taki element m należący do P że:
1) $a \mid m \wedge b \mid m$
2) $\forall_c a \mid c \wedge b \mid c \Rightarrow m \mid c$

1.5 Relacja prostopadłości ($\perp$) w DJR

Niech P – dziedzina z jednoznacznością rozkładu, f,g $\in$ P.

Def.
Powiemy, że f jest prostopadłe do g ($f \perp g$) wtedy i tylko wtedy gdy NWD (f,g) = 1

Własność 1:
$h \perp f * g \Leftrightarrow h \perp f \wedge h \perp g$

Dowód:
Implikacja „$\Rightarrow$” jest oczywista. Dla dowodu „$\Leftarrow$” załóżmy, że $1 \neq h' = NWD(h, f * g)$
Wtedy $h' \mid ih' \mid f * g$. Niech p będzie elementem pierwszym dzielących h’. Wtedy p | f lub p | g i w konsekwencji p | NWD(h,f) lub p | NWD(h,g) przeczy założeniu i tym samym kończy dowód.

Własność 2:
$H \mid f * g \wedge h \perp f \Rightarrow h \mid g$

Dowód:
Niech $h = p_1^{\alpha_1} * ... * p_r^{\alpha_r}$ będzie rozkładem h na iloczyn elementów pierwszych. Ponieważ $h \perp f$ więc $p_i^{\alpha_i} \mid g, i = 1,...,r$ i w konsekwencji NWW $p_i^{\alpha_i} = \prod_i p_1^{\alpha_1} \mid g$
Wprost z definicji wynikają następujące własności relacji podzielności i prostopadłości:
- relacja podzielności jest relacją zwrotną, antysymetryczną i przechodnią, oraz spełnia następujący warunek:
Jeśli $(a,b) \in R$ i $a-k*b \neq 0$ to $(a,a-k*b \in R)$ dla dowolnego $k \in Z^+$

- relacja prostopadłości spełnia warunki dualne tzn. jest antyzwrotna, symetryczna, nieprzechodnia oraz spełnia warunek: Jeśli a < b i (a,b) $\in$ R to (a,b$\pm$a) $\in$ R

Odwrotnie można powiedzieć, że powyższe warunki charakteryzują relacje podzielności („|") i prostopadłości (jeśli R zawiera nietrywialną parę prostopadłą)

2. Pierścienie Euklidesa i struktura ilorazowa

2.1 Pierścień Euklidesa

Pierścieniem Euklidesowym nazywamy dziedzine całkowitości R, w której zadane jest dzielenie z resztą (a przez b $\neq 0$) oraz norma N:R$\longrightarrow$N$_0$ spełniająca warunki:

1) Dla każdego elementu a$\in$R i b$\in$R (b $\neq 0$) istnieja elementy q, r $\in$ R takie, że a = bq + r, gdzie N(r) < N(b) i norma spełnia warunki poniższe:
2) N(a)=0 $\Leftrightarrow$ a = 0
3) N(ab) = N(a)N(b)

q – iloraz z dzielenia a przez b
r- reszta z dzielenia a przez b

Przykład:
R = Z (klasyczny algorytm dzielenia z resztą)

Twierdzenie:
W pierścieniu euklidesowym R zachodzi równoważność
$f \perp g \Leftrightarrow \exists_{a,b\in P} af + bg = 1$

Dowód:

1) „$\Leftarrow$"
Wystarczy pokazać, że gdyby f$\not\perp$ g to nie zachodzi warunek af + bg = 1
Zatem NWD(f,g)=h, gdzie h nie jest elementem odwracalnym.

Wtedy:
$f = hf'$ i $g = hg'$
$1 = af + bg = ahf' + bhg' = h(af' + bg')$
Stąd h jest odwracalny a to przeczy założeniu.

3) „⇒”
NWD(f,g) = 1
$f = qg + r_1$ gdzie $N(r) < N(g)$
$g = g_1 r_1 + r_2$
$r_1 = g_2 r_2 + r_3$
…
$r_{k-1} = q_k r_k + r_{k+1}$
Skoro ciąg jest malejący to dojdzie do 0 i gdzieś się skończy
($r_k = 0$, $N(r_{k-1}) = 0$)

Czytając od dołu:
$r_k = r_{k-2} - q_{k-1} r_{k-1} = r_{k-2} - q_{k-1}(r_{k-3} - q_{k-3} r_{k-2}) = r_{k-2}(1 - q_{k-1} q_{k-2}) + r_{k-3}(-q_{k-1})$

$NWD(r_i, r_{i+1})$ jest niezmiennicze
$NWD(f,g) = 1 = \ldots = NWD(r_k, r_{k-1}) = NWD(r_k, q_k r_k) = r_k = 1$

Co więcej $r_k = \alpha r_{k-2} + \beta r_{k-1} = \alpha' r_{k-3} + \beta' r_{k-2} = \ldots = \alpha'' f + \beta'' g$
C.K.D.

Przykład:
R = Z N(a)=|a|
f=5,g=2
$\exists a, b \in Z : 5 * a + 2 * b = 1$
$5 = 2 * 2 + 1$
$1 = 5 * 2 * 2 = 5 * 1 + 2 * (-2) = 1 * f + (-2) * g^2$

Def.
Ideałem pierścienia R nazywamy grupę addytywną (R,+,0) spełniającą warunek:
Jeśli $a \in I$ to $ab \in I \forall b \in R$

Lemat:

W pierścieniu euklidesowym każdy ideał jest główny tzn. jest postaci:
$I = (f) = \{ bf, b \in R \}$

Dowód:
Niech $I \neq 0$ oraz g = I będzie lementem o minimalnej normie. Pokażemy , że I = (g).
Niech $f \in I$. Wystarczy zauważyć, że f=b*g dla pewnego $b \in R$, bo gdyby nie to f = g*q + r Nr < Ng to by przeczyło założeniu minimalności normy g. C.K.D.

Def.
Idea $I \subset R$ nazywamy maksymalnym wtedy i tylko wtedy, gdy zachodzi implikacja $\forall J(I \subset J \subset R \Rightarrow J = I \text{ lub } J = R$

Def.
$I \subset R$ nazywamy głównym wtedy i tylko wtedy, gdy I = (x), dla pewnego $x \in R$. Pierścień w którym ideał jest główny nazywamy pierścieniem ideałów głównych (PIG)

Twierdzenie:
W pierścieniu euklidesowym każdy ideał pierwszy jest maksymalny.

Dowód:
R i PIG zatem I = (f) i f jest elementem pierwszym. Pokażemy, że (f) jest ideałem maksymalnym:
Niech $(f) \subset J \subset R$ i niech $g \in J : J = (g)$ zatem f = gq dla pewnego $q \in R$
Ponieważ f jest pierwszy, więc zachodzi implikacja:
$f \mid gq \Rightarrow f \mid g$ lub $f \mid q$
$f \mid g \longrightarrow (f) = (g) \longrightarrow (g) = J = (f)$
$f \mid q \longrightarrow (f) = (q) \longrightarrow (g) = R$
C.K.D.

2.2 Grupa Jedności pierścienia (elementów odwracalnych pierścienia R)

Uwaga
Zbiór elementów odwracalnych pierścienia R ma strukturę grupy multiplikatywnej i jest oznaczany R^*. nazywamy go grupą jedności pierścienia R.

2.3 Struktury ilorazowe

Def.
Odwzorowanie $\varphi : R_1 \longrightarrow R_2$ nazywamy homomorfizmem pierścieni R_1 i R_2 wtedy i tylko wtedy gdy φ zachowuje działanie tj.

$$\varphi(a * b) = \varphi(a) * \varphi(b)$$
$$\forall_{a,b \in R_1} \varphi(a + b) = \varphi(a) + \varphi(b)$$

Jeśli φ jest wzajemnie jednoznaczne to φ nazywamy izomorfizmem pierścieni R_1 i R_2.
Jądrem homomorfizmu $\varphi: R_1 \longrightarrow R_2$ nazywamy zbiór:
$\ker\varphi = \{a \in R_1: \varphi(a) = 0\}$

Wniosek:
Jądro homomorfizmu $\varphi: R_1 \longrightarrow R_2$ jest ideałem pierścienia R_1.

2.4 Pierścień ilorazowy

Niech I będzie ideałem pierścienia R. Definiujemy relację (równoważności) „~” na zbiorze R x R.
$a \sim b \Leftrightarrow a - b \in I$
Na klasach abstrakcji $[a]=[a]_\sim$ mamy dobrze określone działania:

$[a]_\sim + [b]_\sim := [a+b]_\sim$
$[a]_\sim * [b]_\sim := [a*b]_\sim$

Wtedy zbiór klas abstrakcji tako kreślonymi działaniami jest pierścieniem ilorazowym, który oznaczamy R/I

Twierdzenie 1 (o izomorfizmie):
Niech $\varphi: R_1 \longrightarrow R_2$ będzie homomorfizmem pierścieni takim, że $\varphi(R_1) = R_2$ .Wtedy pierścień ilorazowy $R_1/\ker\varphi$ jest izomorficzny z R_2

Def.
Niech R_1, R_2 – dowolne pierścienie przemienne z 1. Na produkcie kartezjańskim R x R można zadać strukturę pierścienia w ten sposób, że działanie wykonujemy „po współrzędnych"

$$(a_1, b_2) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_2) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$$

Z elementem neutralnym (0,0) i jednością (1,1). Taki pierścień oznaczać będziemy $R_1 \oplus R_2$.

2.5 Twierdzenie Chińskie

(R, +, $\bullet$) – pierścień

Twierdzenie:
Jeśli $f \perp g$ to $\frac{R}{f * g} = \frac{R}{f} \oplus \frac{R}{g}$

Dowód:
Dla dowodu rozważymy homomorfizm pierścieni

$$\varphi: R \longrightarrow \frac{R}{f} \oplus \frac{R}{g}$$
$$\varphi(a(\mathrm{mod}\, f * g) : a(\mathrm{mod}\, f), a(\mathrm{mod}\, g))$$

Pokażemy, że ten homomorfizm jest izomorfizmem, tzn. że jądro $\ker\varphi$ jest trywialne ($\ker\varphi = 0$). Mamy:

$$\ker\varphi = \{a(\mathrm{mod}\, f * g) : a(\mathrm{mod}\, f) = 0 \wedge a(\mathrm{mod}\, g) = 0\} = \{a(\mathrm{mod}\, f * g) : f \mid a \wedge g \mid a\} =$$
$$= a(\mathrm{mod}\, f * g) : f * g \mid a = 0$$

Twierdzenie:
Jeśli $f \perp g$ to $(R|fg)^* = (R|f)^* \oplus (R|g)^*$

Dowód:

Dla dowodu rozważmy homomorfizm $\Phi^* : R_{fg}^{\perp} \longrightarrow R_f^{\perp} \oplus R_g^{\perp}$

$\Phi^*(a(\mathrm{mod}\, fg)) = (a(\mathrm{mod}\, f), a(\mathrm{mod}\, g))$

Ponieważ h $\perp$ fg $\Leftrightarrow$ h $\perp$ f i h $\perp$ g więc homomorfizm Φ^* jest dobrze określony i jest izomorfizmem.

Fakt:
R – dziedzina całkowitości
I – element pierwszy
Wtedy R/I jest ciałem

Twierdzenie:
R – pierścień euklidesowy
P – element pierwszy
$(R|p)^*$ jest podgrupą grupy $(R|p^a)^*$

Dowód:
Ponieważ R|p jest ciałem więc grupa jedności $(R|p)^*$ jest generowana przez pewien element a $\in$ $(R|p)^*$. Rozważamy homomorficzny naturalnie R $\longrightarrow$ R|p i R $\longrightarrow$ $R|p^a$. Na mocy twierdzenia o izomorfizmie istnieje homomorfizm h:$R|p^a$ $\longrightarrow$ R|p I niech h* będzie jego obcięciem do odpowiednich grup jedności.

Niech $\bar{a}$ będzie przeciwobrazem a przy działaniu h należącym do $R|p^a$.

Wtedy rząd $\bar{a}$ jest wielokrotnością rzędu a. Zatem rząd $\bar{a}$=k*$|(R|p)^*|$ w takim przypadku element $(\bar{a})^k$ generuje podgrup izomorficzną z grupą (R|p)*.