PIERŚCIENIE I CIAŁA
Wykład 6

Przypomnijmy, że niepusty podzbiór I pierścienia P jest ideałem, gdy

(1) $\bigwedge\limits_{a,b\in I} a-b\in I$

(2) $\bigwedge\limits_{a\in I}\bigwedge\limits_{x\in P} ax\in I,\ xa\in I.$

Ideałowi I odpowiada relacja równoważności $\equiv$ zdefiniowana wzorem:

$$x\equiv y\ (\mathrm{mod}\ I)\Leftrightarrow x-y\in I, \tag{1}$$

gdzie $x,y\in P$. W zbiorze P/I wszystkich klas abstrakcji względem relacji $\equiv$ określamy działania wzorami

$$[a]+[b]=[a+b],\quad [a][b]=[ab],$$

gdzie $a,b\in P$ i w ten sposób P/I staje się pierścieniem, który nazywamy pierścieniem ilorazowym. Jego elementem zerowym jest $[0]=I$ i jeśli w P istnieje jedynka, to $[1]$ jest jedynką w P/I. Jeśli P jest pierścieniem przemiennym, to również P/I jest pierścieniem przemiennym.

Dla tego, żeby pierścień ilorazowy P/I był pierścieniem całkowitym, czyli pierścieniem przemiennym z $1\neq 0$ nie zawierający niezerowych dzielników zera konieczna jest dodatkowa własność ideału I. Mówimy, że ideał I pierścienia P jest ***ideałem pierwszym***, jeśli I jest ideałem właściwym i

$$\bigwedge_{x,y\in P} xy\in I\Rightarrow (x\in I \text{ lub } y\in I).$$

Warunek ten przenosi się na większą liczbę czynników, więc jeśli iloczyn skończenie wielu elementów pierścienia P należy do ideału I, to co najmniej jeden z nich należy do I.

Twierdzenie 1. *Niech I będzie właściwym ideałem pierścienia P. Pierścień ilorazowy P/I nie zawiera niezerowych dzielników zera wtedy i tylko wtedy, gdy I jest ideałem pierwszym.*

Wniosek 1. *Niech I będzie ideałem właściwym pierścienia przemiennego P z $1\neq 0$. Wówczas I jest ideałem pierwszym wtedy i tylko wtedy, gdy P/I jest pierścieniem całkowitym.*

Również dla tego, żeby pierścień ilorazowy P/I był ciałem konieczna jest dodatkowa własność ideału I.

Mówimy, że ideał I pierścienia P jest ***maksymalny***, jeśli jest on elementem maksymalnym w zbiorze W wszystkich ideałów właściwych pierścienia P. Zatem ideał I jest maksymalny wtedy i tylko wtedy, gdy $I\neq P$ i nie istnieje ideał J taki, że $I\subset J$, $I\neq J$ oraz $J\neq P$.

Twierdzenie 2. *Niech I będzie ideałem właściwym pierścienia przemiennego P z $1\neq 0$. Pierścień ilorazowy P/I jest ciałem wtedy i tylko wtedy, gdy I jest ideałem maksymalnym.*

Ponieważ ciało jest pierścieniem całkowitym, więc z wniosku 1 i twierdzenia 2 otrzymujemy następujący rezultat.

Wniosek 2. *Niech I będzie ideałem właściwym pierścienia przemiennego P z $1 \neq 0$. Jeżeli ideał I jest maksymalny, to I jest pierwszy.*

Przykład 1. W pierścieniu $\mathbb{Z}[x]$ wielomianów o współczynnikach całkowitych zbiór

$$I = \{f \in \mathbb{Z}[x] : f(0) = 0\}$$

jest ideałem. Jeśli $fg \in I$, to $f(0)g(0) = 0$, więc $f(0) = 0$, czyli $f \in I$ lub $g(0) = 0$, czyli $g \in I$. Zatem I jest ideałem pierwszym.

Nie jest to jednak ideał maksymalny, gdyż

$$J = \{f \in \mathbb{Z}[x] : f(0) \text{ jest liczbą parzystą}\}$$

jest ideałem w $\mathbb{Z}[x]$ takim, że $I \subset J$, $J \neq I$ oraz $J \neq \mathbb{Z}[x]$.

Twierdzenie 3. *Niech P będzie skończonym pierścieniem przemiennym z $1 \neq 0$. Dowolny element $a \in P$ jest albo elementem odwracalnym, albo dzielnikiem zera.*

Dowód. Dla $a \in P$, $a \neq 0$ rozważmy funkcję $f(x) = ax$, gdzie $x \in P$. Jeżeli f jest funkcją różnowartościową, to zbiór $f(P) \subset P$ ma tyle samo elementów, co P, a więc $f(P) = P$. Zatem dla każdego $y \in P$ istnieje $x \in P$ taki, że $y = f(x) = ax$. W szczególności dla $y = 1$ dostajemy $x \in P$ taki, że $ax = 1$, co pokazuje, że element a jest odwracalny i $a^{-1} = x$.

Załóżmy teraz, że funkcja f nie jest różnowartościowa. Wtedy istnieją $x_1, x_2 \in P$ takie, że $x_1 \neq x_2$ i $ax_1 = f(x_1) = f(x_2) = ax_2$. Zatem

$$a(x_1 - x_2) = ax_1 - ax_2 = 0$$

i ponieważ $x_1 - x_2 \neq 0$, wiec a jest dzielnikiem zera. □

Dla pierścienia $\mathbb{Z}_n$, $n > 1$, niezerowy element $a \in \mathbb{Z}_n$ jest dzielnikiem zera wtedy i tylko wtedy, gdy a nie jest względnie pierwszy z n, zaś liczby $a \in \mathbb{Z}_n$, które sa względnie pierwsze z n są elementami odwracalnymi.

Przykład 2. W pierścieniu $\mathbb{Z}_6$ mamy

$$2 \odot_6 3 = r_6(6) = 0, \quad 4 \odot_6 3 = r_6(12) = 0,$$

więc 2, 3, 4 są dzielnikami zera. Natomiast 1 i 5 są elementami odwracalnymi. W szczególności

$$5 \odot_6 5 = r_6(25) = 1,$$

czyli $5^{-1} = 5$.

Z twierdzenia 3 wynika następujący wniosek.

Wniosek 3. *Skończony pierścień przemienny z $1 \neq 0$ jest ciałem wtedy i tylko wtedy, gdy jest pierścieniem całkowitym.*

W szczególności pierścień $\mathbb{Z}_n$, $n > 1$, jest ciałem wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

Teoria podzielności w pierścieniach całkowitych

Niech P będzie pierścieniem całkowitym. Dla $a, b \in P$ mówimy, że a dzieli b jeśli istnieje $c \in P$ takie, że $b = ca$. Piszemy wtedy $a \mid b$.

Elementy $a, b \in P$ są stowarzyszone, jeśli $a \mid b$ i $b \mid a$. Piszemy wtedy $a \sim b$. Warunek ten jest równoważny temu, że istnieje element odwracalny $u \in P$ taki, że $b = ua$. W szczególności warunek $a \sim 1$ oznacza, że a jest elementem odwracalnym. Relacja stowarzyszenia jest relacją równoważności w pierścieniu P.

Przykład 3.
1. Jedynymi elementami odwracalnymi w pierścieniu $\mathbb{Z}$ są: -1 i 1. Zatem liczby $a, b \in \mathbb{Z}$ są stowarzyszone, gdy $a = \pm b$, czyli $|a| = |b|$.
2. Liczby -1, 1, $-i$, i są elementami odwracalnymi w pierścieniu $\mathbb{Z}[i]$. Są to jedyne elementy odwracalne. Aby się o tym przekonać, zauważmy, że jeśli $z = a + bi$, gdzie $a, b \in \mathbb{Z}$ jest elementem odwracalnym w pierścieniu $\mathbb{Z}[i]$, to $zw = 1$ dla pewnego $w \in \mathbb{Z}[i]$. Zatem

$$1 = |zw|^2 = |z|^2|w|^2,$$

przy czym $|z|^2$ i $|w|^2$ są liczbami naturalnymi. Stąd $|z|^2 = a^2 + b^2 = 1$. Ale a^2 i b^2 są liczbami naturalnymi, więc $a^2 = 1$ i $b^2 = 0$ lub $a^2 = 0$ i $b^2 = 1$. W pierwszym przypadku $z = \pm 1$, zaś w drugim $z = \pm i$.

Zatem dla $z \in \mathbb{Z}[i]$ elementami pierścienia $\mathbb{Z}[i]$ stowarzyszonymi z z są iz, $-z$, $-iz$. Te cztery punkty płaszczyzny zespolonej są wierzchołkami kwadratu ośrodku 0.

Dla liczby całkowitej n następujące warunki sa równoważne:

- n jest liczbą pierwszą, czyli jedynymi dzielnikami n są ± 1 i $\pm n$,
- jeśli n dzieli iloczyn ab, gdzie $a, b \in \mathbb{Z}$, to n dzieli a lub n dzieli b.

Mówimy, że niezerowy element $a \in P$ jest ***pierwszy***, jeśli a nie jest odwracalny oraz jeżeli

$$\bigwedge_{b,c \in P} a \mid bc \Rightarrow (a \mid b \text{ lub } a \mid c).$$

Oznacza to, że jeżeli a dzieli iloczyn dwóch elementów, to a dzieli któryś z czynników. Warunek ten można przenieść na większą liczbę czynników.

Mówimy, że niezerowy element $a \in P$ jest ***nierozkładalny***, jeśli a nie jest odwracalny oraz

$$\bigwedge_{b,c \in P} a = bc \Rightarrow (b \sim 1 \text{ lub } c \sim 1).$$

Warunek ten jest równoważny temu, że

$$\bigwedge_{b \in P} b \mid a \Rightarrow (b \sim 1 \text{ lub } b \sim a),$$

a więc nierozkładalność elementu a można interpretować w ten sposób, że a nie ma dzielników właściwych, czyli niestowarzyszonych ani z 1, ani z a.

Twierdzenie 4. *Każdy element pierwszy jest nierozkładalny.*

W pierścieniu $\mathbb{Z}$ dla liczby $m \in \mathbb{Z}$ różnej od 0 i ± 1 następujące warunki są równoważne:

$$m \text{ jest liczbą pierwszą } \Leftrightarrow m \text{ jest nierozkładalny } \Leftrightarrow m \text{ jest pierwszy.}$$

W pewnych pierścieniach istnieją jednak elementy nierozkładalne, które nie są pierwsze.

Ideały główne

Niech P będzie pierścieniem przemiennym. Dla $a_1, a_2, ..., a_n \in P$ zbiór

$$(a_1, a_2, ..., a_n) = \{a_1x_1 + a_2x_2 + ... + a_nx_n : x_1, x_2, ..., x_n \in P\}$$

jest ideałem. Nazywamy go ideałem generowanym przez elementy $a_1, a_2, ..., a_n$. W najprostszym przypadku otrzymujemy ideał generowany przez pojedynczy element $a \in P$:

$$(a) = \{ax : x \in P\} = \{b \in P : a \mid b\}$$

Nazywamy go ***ideałem głównym*** generowanym przez a. Mówimy, że P jest pierścieniem ideałów głównych, gdy P każdy ideał w P jest ideałem głównym.

Przykład 4.
1. Pierścień $\mathbb{Z}$ jest pierścieniem ideałów głównych.
2. Pierścień $\mathbb{Z}[x]$ wielomianów o współczynnikach całkowitych nie jest pierścieniem ideałów głównych. Rzeczywiście, rozważmy ideał

$$I = (2, x) = \{2g(x) + xh(x) : g, h \in \mathbb{Z}[x]\}.$$

Zauważmy, że wielomiany należące do I mają parzyste wyrazy wolne. Gdyby I był ideałem głównym, to istniałby wielomian $f \in \mathbb{Z}[x]$ taki, że

$$I = (f) = \{f(x)w(x) : w \in \mathbb{Z}[x]\}.$$

Ponieważ $2 \in I$, więc $2 = f(x)w(x)$, co pokazuje, że f jest wielomianem stałym, czyli $f(x) = a_0 \in \mathbb{Z}$. Ale $x \in I$, więc $x = f(x)w(x)$ dla pewnego wielomianu $w \in \mathbb{Z}[x]$. Stąd $1 = f(1)w(1) = a_0w(1)$, zatem $f(x) = a_0 = \pm 1$. Jest to sprzeczne z założeniem, że $f \in I$, gdyż wielomiany należące do I mają parzyste wyrazy wolne.

Dla $I = (a)$ warunek $c \in I$ jest równoważny temu, że $a \mid c$. Zatem warunek $x \equiv y \pmod{I}$ oznacza w tym przypadku, że $a \mid (x - y)$. Mówimy wtedy, że x przystaje do y modulo a.

Uwaga 1. Niech a, b będą elementami pierścienia całkowitego P. Rozważmy ideały $I = (a)$, $J = (b)$ generowane przez te elementy. Wtedy

(1) warunek $a \mid b$ jest równoważny temu, że $J \subset I$,
(2) warunek $a \sim b$ jest równoważny temu, że $J = I$.

Twierdzenie 5. *Niezerowy element a pierścienia całkowitego P jest pierwszy wtedy i tylko wtedy, gdy $I = (a)$ jest ideałem pierwszym.*

Dowód. Załóżmy, że a jest elementem pierwszym. Jeżeli $bc \in I$, to $a|bc$ i z założenia wynika, że $a|b$, czyli $b \in I$ lub $a|c$, czyli $c \in I$. Zatem I jest ideałem pierwszym.

Załóżmy teraz, że $I = (a)$ jest ideałem pierwszym. Jeżeli $a|bc$, to $bc \in I$ i z założenia wynika, że $b \in I$, czyli $a|b$ lub $c \in I$, czyli $a|c$. Pokazuje to, że a jest elementem pierwszym. □

Powyższe twierdzenie w połączeniu z wnioskiem 1 daje nam następujący wniosek.

Wniosek 4. *Niech a będzie niezerowym elementem pierścienia całkowitego P. Pierścień ilorazowy P/I, gdzie $I = (a)$ jest pierścieniem całkowitym wtedy i tylko wtedy, gdy a jest elementem pierwszym.*

Twierdzenie 6. *Niech P będzie pierścieniem całkowitym ideałów głównych. Element $a \in P$ jest nierozkładalny wtedy i tylko wtedy, gdy $I = (a)$ jest ideałem maksymalnym.*

Dowód. Załóżmy, że $a \in P$ jest elementem nierozkładalnym i J jest ideałem w P takim, że $I = (a) \subset J$. Ponieważ P jest pierścieniem ideałów głównych, więc $J = (b)$ dla pewnego $b \in P$. Mamy $a \in J = (b)$, zatem $b \mid a$ i ponieważ a jest elementem nierozkładalnym, więc $b \sim 1$ lub $b \sim a$. W pierwszym przypadku $1 = b^{-1}b \in J$, czyli $J = P$, zaś w drugim $J = I$. Stąd I jest ideałem maksymalnym.

Na odwrót, jeśli I jest ideałem maksymalnym i $b \mid a$, to $I \subset J = (b)$, a zatem $J = P$ lub $J = I$. W pierwszym przypadku $1 \in J$, czyli $b \mid 1$, więc $b \sim 1$, zaś w drugim $a \mid b$, więc $a \sim b$. □

Z twierdzeń 6 i 2 wynika następujący wniosek.

Wniosek 5. *Niech P będzie pierścieniem całkowitym ideałów głównych i $a \in P$. Pierścień ilorazowy P/I, gdzie $I = (a)$ jest ciałem wtedy i tylko wtedy, gdy a jest elementem nierozkładalnym.*

Wniosek ten uogólnia fakt znany dla pierścienia liczb całkowitych, w którym $n \in \mathbb{N} \setminus \{1\}$ jest liczbą pierwszą wtedy i tylko wtedy, gdy pierścień ilorazowy $\mathbb{Z}/(n)$, który jest izomorficzny z $\mathbb{Z}_n$ jest ciałem.

Z twierdzenia 4 wiemy, że w dowolnym pierścieniu całkowitym każdy element pierwszy jest nierozkładalny. Jeśli P jest pierścieniem ideałów głównych, to korzystając z twierdzenia 6, wniosku 2 i wniosku 4 otrzymujemy zależność odwrotną.

Wniosek 6. *Niech P będzie pierścieniem całkowitym ideałów głównych. Element $a \in P$ jest pierwszy wtedy i tylko wtedy, gdy a jest nierozkładalny.*

Pierścienie Gaussa

Rysunek 1. Carl Friedrich Gauss (1777–1855)

Gauss już jako małe dziecko wykazywał nieprzeciętne zdolności matematyczne – w wieku 3 lat umiał dodawać i wytknął ojcu błąd podczas naliczania dniówki dla pomocników przy pracy ogrodniczej. Jak sam żartobliwie twierdził, nauczył się rachować, zanim jeszcze

zaczął mówić. W 1784 roku Gauss został posłany do szkoły. Po dwóch latach rozpoczął naukę arytmetyki i objawił swój nieprzeciętny talent, rozwiązując z miejsca zadanie, jakie nauczyciel podał w klasie. Zadanie polegało na dodaniu do siebie liczb od 1 do 100. Gauss jako pierwszy oddał tabliczkę, na której nie było żadnych obliczeń a jedynie prawidłowe rozwiązanie końcowe, a następnie wytłumaczył nauczycielowi, w jaki sposób doszedł do wyniku. Na uniwersytecie w Getyndze Gauss studiował matematykę, astronomię, fizykę, filologię i historię. Początkowo wahał się, czy zajmować się głównie językami starożytnymi, czy matematyką – w końcu zdecydował się na drugą opcję. Po studiach został profesorem astronomii i dyrektorem obserwatorium astronomicznego na uniwersytecie w Getyndze. Przysłużył się dla teorii liczb, geometrii, algebry, analizy, probabilistyki, metod numerycznych, statystyki i fizyki matematycznej; jest uważany za jednego z pionierów geometrii nieeuklidesowej. Krótko po śmierci pobrano mózg Gaussa i prowadzono nad nim badania naukowe mające stwierdzić, czy geniusz naukowy Gaussa ma odzwuerciedlenie w budowie mózgu. W 2013 roku odkryto, że jeszcze w XIX w. doszło do pomyłki – mózg przechowywany jako Gaussa okazał się mózgiem innego człowieka.

Mówimy, że pierścień całkowity P jest ***pierścieniem Gaussa***, jeśli każdy element niezerowy i nieodwracalny $a \in P$ można przedstawić w postaci

$$a = a_1 a_2 ... a_n,$$

gdzie $a_1, a_2, ..., a_n \in P$ są elementami nierozkładalnymi, przy czym rozkład ten jest jednoznaczny w tym sensie, że z równości

$$a_1 a_2 ... a_n = b_1 b_2 ... b_m,$$

gdzie $a_1, a_2, ..., a_n, b_1, b_2, ..., b_m \in P$ są elementami nierozkładalnymi wynika, że $n = m$ i istnieje permutacja σ zbioru $\{1, 2, ..., n\}$ taka, że $a_i \sim b_{\sigma(i)}$ dla $i = 1, 2, ..., n$.

Twierdzenie 7. *Pierścień całkowity P jest pierścieniem Gaussa wtedy i tylko wtedy, gdy każdy element nierozkładalny w P jest elementem pierwszym.*

Standardowym przykładem pierścienia Gaussa jest pierścień liczb całkowitych $\mathbb{Z}$.

Oznaczenie: dla elementów $a_1, a_2, ..., a_n$ pierścienia P iloczyn $a_1 a_2 ... a_n$ zapisujemy też jako $\prod_{i=1}^{n} a_i$.

W pierścieniu Gaussa każdy niezerowy i nieodwracalny $a \in P$ można zapisać jako $a = \prod_{i=1}^{k} c_i$, gdzie $c_1, c_2, ..., c_n \in P$ są elementami nierozkładalnymi. Czynniki w rozkładzie mogą się powtarzać w tym sensie, że mogą być ze sobą stowarzyszone. Łącząc stowarzyszone czynniki otrzymujemy rozkład $a = u \prod_{i=1}^{n} a_i^{p_i}$, gdzie $p_1, ..., p_n \in \mathbb{N}$, $u \sim 1$, zaś $a_1, a_2, ..., a_n \in P$ są elementami nierozkładalnymi wzajemnie niestowarzyszonymi, czyli takimi, że $a_i \not\sim a_j$ dla $i \neq j$. Inny element $b \in P$ może w rozkładzie mieć inne czynniki nierozkładalne, ale dostawiając ewentualnie w rozkładach a i b brakujące czynniki w potędze 0 możemy zapisać

$$a = u \prod_{i=1}^{n} a_i^{p_i}, \quad b = v \prod_{i=1}^{n} a_i^{q_i}, \tag{2}$$

gdzie $u \sim 1$, $v \sim 1$, $p_1, ..., p_n, q_1, ..., q_n \in \mathbb{N} \cup \{0\}$.

Twierdzenie 8. *Niech a, b będą elementami pierścienia Gaussa, których rozkłady na czynniki pierwsze mają postać* (2)*. Wtedy warunek $a \mid b$ jest równoważny temu, że $p_i \leqslant q_i$ dla każdego $i = 1, ..., n$.*