9. Homomorfizmy i ideały.

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

9.1. Definicja. *Jądrem homomorfizmu $\varphi : R \to P$ nazywamy zbiór*

$$ker\,\varphi = \{x \in R\colon \varphi(x) = 0\}.$$

Jądro homomorfizmu ma następujące własności:
a) jest podgrupą grupy addytywnej pierścienia R
b) $\forall_{x\in R}\forall_{a\in ker\,\varphi}\ a \cdot x \in ker\,\varphi$.

9.2. Definicja. **Ideałem** *pierścienia R nazywamy taką podgrupę I grupy addytywnej tego pierścienia, która spełnia warunek:*
$\forall_{x\in R\ a\in I}\ a \cdot x \in I$.
Używamy oznaczenia $I \trianglelefteq R$.

9.3. Przykłady.
1) Jądro dowolnego homomorfizmu jest ideałem.
2) $\{0\} \trianglelefteq R$ jest ideałem, który nazywamy ideałem zerowym.
3) Dla elementu $a \in R$ zbiór $\{ax \mid x \in R\}$ jest ideałem. Ideał ten oznaczamy symbolem (a).
3) W pierścieniu liczb całkowitych $\mathbb{Z}$, podgrupy grupy addytywnej są postaci, $n\mathbb{Z}$, dla pewnego $n \in \mathbb{N}$. Każda z nich jest ideałem, gdyż jest jądrem homomorfizmu $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = x \pmod n$.
4) $R \trianglelefteq R$ — ten ideał nazywamy niewłaściwym. Jest on jądrem homomorfizmu trywialnego w pierścień zerowy.

Ideał nazywamy **właściwym**, jeżeli jest różny od całego pierścienia. Odnotujmy przydatne, choć oczywiste, stwierdzenie:

9.4. Stwierdzenie. *Ideał jest właściwy wtedy i tylko wtedy, gdy nie zawiera* 1.

Dowód. Jeżeli ideał zawiera 1, to $\forall_{x\in R}\ x \cdot 1 = x \in I$, czyli $I = R$. □
Wobec powyższego, ideał właściwy nie jest podpierścieniem pierścienia przemiennego z jedynką.

Używając pojęcia ideału można podać wygodną charakteryzację tych pierścieni, które są ciałami.

9.5. Stwierdzenie. *Pierścień jest ciałem wtedy i tylko wtedy, gdy jest niezerowy i jedynymi jego ideałami są ideał zerowy i cały pierścień.*

Dowód. $\Rightarrow$ Jeżeli $\{0\} \neq I \trianglelefteq R$, to istnieje $x \neq 0$, $x \in I$. Wówczas $x \cdot x^{-1} = 1 \in I$, zatem $I = R$.
$\Leftarrow$ Jeżeli $x \neq 0$, to $\{0\} \neq (x)$, więc $(x) = R$ i $1 \in (x)$ — co oznacza, że istnieje y, dla którego $xy = 1$. □

Odnotujmy jeszcze następujące, łatwe do udowodnienia, własności ideałów (analogiczne do odpowiednich własności podgrup normalnych):
1) Jeżeli $\varphi : R \longrightarrow P$ jest homomorfizmem i $J \trianglelefteq P$, to $\varphi^{-1}(J) \trianglelefteq R$.
2) Jeżeli $\varphi : R \longrightarrow P$ jest epimorfizmem i $I \trianglelefteq R$, to $\varphi(I) \trianglelefteq P$.
Jeżeli o przekształceniu φ zakładamy tylko tyle, że jest homomorfizmem, to w każdym razie możemy twierdzić, że $\varphi(I) \trianglelefteq \mathrm{im}\,(\varphi)$.

3) Jeżeli $I_k \trianglelefteq R$ dla $k \in K$ to $\bigcap_{k\in K} I_k \trianglelefteq R$.

Pierścień ilorazowy

Niech $I \trianglelefteq R$ będzie ideałem.

9.6. Definicja. *Niech $I \trianglelefteq R$ będzie ideałem. Wówczas* **pierścieniem ilorazowym** *nazywamy zbiór warstw R/I z działaniami:*

$$(x+I)+(y+I) = (x+y)+I$$
$$(x+I)\cdot(y+I) = x\cdot y + I$$
$$-(x+I) = -x+I$$

i warstwami: $1+I$ jako jedynką, I jako zerem.
Przekształcenie $\pi : R \to R/I$ zadane wzorem $\pi(x) = x+I$ jest epimorfizmem, $ker\,\pi = I$.

9.7. Uwaga Należy sprawdzić, że powyższa definicja jest dobra - to znaczy, że działania są dobrze określone (nie zależą od wyboru reprezentantów warstw) i spełniają aksjomaty pierścienia przemiennego z 1. To, że ideał jest podgrupą przemiennej grupy addytywnej pierścienia zapewnia poprawność dodawania warstw, zaś to że ideał jest "pułapką" na mnożenie poprawność mnożenia warstw. Spełnienie aksjomatów jest oczywiste.

Konstrukcja pierścienia ilorazowego pozwala na analizę homomorfizmów.

9.8. Twierdzenie o homomorfizmie. *Jeżeli $\varphi : R \to P$ jest homomorfizmem, to istnieje dokładnie jeden homomorfizm $\tilde{\varphi} : R/ker\,\varphi \to P$, taki że $\varphi = \tilde{\varphi}\circ\pi$, gdzie $\pi : R \to R/ker\,\varphi$. Homomorfizm $\tilde{\varphi} : R/ker\,\varphi \to \varphi(R)$ jest izomorfizmem i istnieje wzajemnie jednoznaczna odpowiedniość między ideałami pierścienia $\varphi(R)$ a ideałami R zawierającymi $ker\,\varphi$.*

Dowód. Szukanym homomorfizmem jest $\tilde{\varphi}(x+ker\,\varphi) = \varphi(x)$. Sprawdzenia wymaga tylko to, że $\tilde{\varphi}$ jest dobrze określone. □

9.9. Przykład. Rozpatrzmy homomorfizm $\varphi : \mathbb{Z}[X] \to \mathbb{C}$, $\varphi(X) = \sqrt{d}$, gdzie d jest liczba bezkwadratową. Jego jądro $\ker\varphi = \{f \in \mathbb{Z}[X]\colon f(\sqrt{d}) = 0\}$. Wyłączając $X^2 - d$ przed nawias możemy dowolny wielomian przedstawić w postaci $f = (x^2 - d)g + aX + b$. Zatem $\ker\varphi = \{(X^2-d)f, f \in \mathbb{Z}[X]\}$. Jest jasne, że $\mathrm{im}\,\varphi = \mathbb{Z}[\sqrt{d}]$ a więc $\mathbb{Z}[X]/(X^2-d) \cong \mathbb{Z}[\sqrt{d}]$.

Wróćmy do własności ideałów. Z faktu, że część wspólna rodziny ideałów jest ideałem, wynika, że dla każdego podzbioru $A \subseteq R$ istnieje najmniejszy ze względu na zawieranie ideał pierścienia R zawierający zbiór A — oznacza się go przez (A) i nazywa **ideałem generowanym** przez A. Nietrudno znaleźć postać elementów ideału (A).

9.10. Stwierdzenie. *Jeżeli $A \subseteq R$, $A \neq \emptyset$, to*

$$(A) = \{a_1x_1 + \cdots + a_jx_j : j \in \mathbb{N},\ a_i \in A,\ x_i \in R\}.$$

Dowód. Łatwo sprawdzić, że każdy ideał zawierający zbiór A zawiera powyższy zbiór i że zbiór ten *jest* ideałem. □

9.11. Przykład. Jeżeli $i \trianglelefteq R$ oraz $J \trianglelefteq R$ to zgodnie z powyższym stwierdzeniem $(I \cup J) = \{x+y\colon x \in I,\ y \in J\}$. Ideał ten będziemy więc nazywali suma ideałów I i J oznaczając go symbolem $I + J$.

9.12. Definicja. *Ideał $I \trianglelefteq R$ nazywamy* **ideałem głównym** *wtedy i tylko wtedy, gdy istnieje element $a \in R$, taki że $I = (a) = \{ax : x \in R\}$.*

9.13. Stwierdzenie. *W pierścieniu $\mathbb{Z}$ i w pierścieniu $k[X]$ (wielomianów nad ciałem k każdy ideał jest główny.*

Dowód. Dla niezerowego ideału w pierścieniu $\mathbb{Z}$ generatorem jest liczba całkowita o najmniejszym module spośród liczb różnych od zera należących do ideału. W przypadku pierścienia wielomianów należy wziąć wielomian najmniejszego stopnia spośród niezerowych wielomianów należących do ideału. □

Powyższa własność jest na tyle istotna, że wyodrębnia się klasę pierścieni,które ją posiadają.

9.14. Definicja. *Dziedzinę całkowitości nazywamy* **dziedziną ideałów głównych** *wtedy i tylko wtedy, gdy każdy jej ideał jest główny.*

W zależności od własności pierścienia ilorazowego będziemy wyróżniać pewne ideały.

9.15. Definicja. *Ideał $I \trianglelefteq R$ nazywamy* **ideałem pierwszym** *wtedy i tylko wtedy, gdy R/I jest dziedziną całkowitości.*
Ideał $I \trianglelefteq R$ nazywamy **ideałem maksymalnym** *wtedy i tylko wtedy, gdy R/I jest ciałem.*

9.16. Uwaga. *W pierścieniu R ideał zerowy jest pierwszy wtedy i tylko wtedy, gdy R jest dziedziną całkowitości.*

Zauważmy, że ideały pierwsze i maksymalne są z definicji ideałami właściwymi. Oczywiście, każdy ideał maksymalny jest pierwszy.

Podamy warunki równoważne tym z definicji i wówczas będzie widać dlaczego używa się nazw — pierwszy i maksymalny.

9.17. Stwierdzenie. *Ideał $I \trianglelefteq R$ jest pierwszy wtedy i tylko wtedy, gdy $I \neq R$ oraz dla dowolnych $x, y \in R$, jeżeli $xy \in I$, to $x \in I$ lub $y \in I$.*
Ideał $I \trianglelefteq R$ jest maksymalny wtedy i tylko wtedy, gdy jest elementem maksymalnym, ze względu na zawieranie, w zbiorze właściwych ideałów R (oznacza to, że $I \neq R$ oraz jeżeli $J \trianglelefteq R$ i $I \subseteq J$, to $I = J$ lub $J = R$).

Dowód. W obydwu wypadkach możemy ograniczyć rozważania do sytuacji, gdy I jest ideałem właściwym. W przeciwnym razie iloraz jest pierścieniem zerowym, a więc nie jest ani dziedziną całkowitości, ani ciałem. Zakładamy zatem, że $I \neq R$.

Pierścień R/I jest dziedziną całkowitości wtedy i tylko wtedy, gdy z równości $(x + I) \cdot (y + I) = xy + I = 0 + I$ wynika, że $(x + I = 0 + I \ \vee \ y + I = 0 + I)$,
a zatem wtedy i tylko wtedy, gdy z $xy \in I$ wynika, że $(x \in I \ \vee \ y \in I)$.

Pierścień R/I jest ciałem wtedy i tylko wtedy, gdy jego jedynymi ideałami są ideał zerowy oraz cały pierścień R/I, a zatem (wobec wzajemnie jednoznacznej odpowiedniości między ideałami pierścienia ilorazowego R/I a ideałami pierścienia R zawierającymi I) wtedy i tylko wtedy, gdy z $I \subseteq J \trianglelefteq R$ wynika $(I = J \vee J = R)$.
□

9.18. Twierdzenie. *Każdy ideał właściwy I jest zawarty w pewnym ideale maksymalnym.*

Dowód. Rozpatrzmy zbiór ideałów właściwych zawierających I, z częściowym porządkiem wyznaczonym przez zawieranie. Łańcuchami† są wówczas wstępujące rodziny ideałów. Każdy łańcuch ma zatem ograniczenie górne, bo suma wstępującej rodziny ideałów właściwych jest ideałem właściwym (nie zawiera jedynki, bo nie zawiera jej żaden z sumowanych składników). Na mocy lematu Zorna w zbiorze tym istnieje więc element maksymalny. □

9.19. Wniosek. *Każdy niezerowy pierścień można odwzorować epimorficznie na pewne ciało.* □

9.20. Przykłady.

1) Niech X będzie przestrzenią topologiczną, a $C(X)$ pierścieniem funkcji ciągłych o wartościach rzeczywistych. Niech $x_0 \in X$. Ideał $\{f\colon f(x_0) = 0\} = I_{x_0}$ jest jądrem epimorfizmu $\phi : C(X) \to R$, określonego wzorem $\phi_f(x_0) = f(x_0)$, a więc jest maksymalny.

Następne dwa przykłady ilustrują ważną metodę otrzymywania interesujących ciał jako pierścieni ilorazowych pierścienia wielomianów nad ciałem.

2) Ideał $(x^2 + 1) \trianglelefteq \mathbb{R}[X]$ jest maksymalny, i $\mathbb{R}[X]/(x^2 + 1) \cong \mathbb{C}$. Izomorfizm jest wyznaczony przez przyporządkowanie warstwie $x + (x^2 + 1)$ liczby i.
3) Łatwo sprawdzić, że $\mathbb{Z}_2[X]/(X^2 + X + 1)$ jest ciałem o czterech elementach, więc ideał $(X^2 + X + 1)$ jest maksymalny.
1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ jest pierścieniem skończonym. Zatem ideał główny (n) jest maksymalny wtedy i tylko wtedy, gdy jest pierwszy, a więc wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

   Własność ta przysługuje dziedzinom ideałów głównych.

9.21. Twierdzenie. *Jeżeli pierścień jest dziedziną całkowitości, to w zbiorze właściwych ideałów głównych ideały pierwsze różne od zerowego, są maksymalne ze względu na zawieranie.*

Dowód. Niech $I = (a)$, $a \neq 0$ będzie ideałem pierwszym i niech $I \subseteq J$, gdzie $J = (b)$. Zatem $a = bc$ i z tego, że ideał I jest pierwszy wynika, że $b \in I$ lub $c \in I$.

W pierwszym przypadku $(b) \subseteq I$, co dowodzi równości $(a) = I = J = (b)$.

Jeżeli $c \in I$, to $c = ad$, więc $a = bad$ i $a(bd - 1) = 0$. Pierścień R jest dziedziną, $a \neq 0$, więc $bd = 1 \in J$ i $J = R$. □

Jako wniosek otrzymujemy następujące ważne twierdzenie.

9.22. Twierdzenie. *W dziedzinie ideałów głównych każdy niezerowy ideał pierwszy jest maksymalny.*

Twierdzenie chińskie o resztach.

Ustalenie z jakim pierścieniem jest izomorficzny dany pierścień ilorazowy bywa trudne. W wielu sytuacjach w sukurs przychodzi "chińskie twierdzenie o resztach." Zacznijmy od definicji:

9.23. Definicja. *Ideały $I_1 \trianglelefteq R$, $I_2 \trianglelefteq R$ nazywamy względnie pierwszymi wtedy i tylko wtedy, gdy $I_1 + I_2 = R$.*

Zauważmy, że ideały $I_1 \trianglelefteq R$, $I_2 \trianglelefteq R$ są względnie pierwsze jeżeli istnieją elementy $x \in I_1$, $y \in I_2$, dla których $x + y = 1$.

† tzn. podzbiorami liniowo uporządkowanymi.

9.24. Twierdzenie chińskie o resztach. *Niech $I_1, \ldots, I_n$ będą parami względnie pierwszymi ideałami pierścienia R. Niech*

$$\varphi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

będzie homomorfizmem danym wzorem:

$$\varphi(x) = (x + I_1, x + I_2, \ldots, x + I_n).$$

Wówczas:
a) homomorfizm φ jest epimorfizmem.
b) $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_n$
Zatem:

$$R/(I_1 \cap I_2 \cap \cdots \cap I_n) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

Zanim przystąpimy do dowodu twierdzenia przeanalizujmy przykład. Niech $R = \mathbb{Z}$, $I_1 = (3), I_2 = (10), I_3 = (7)$. Założenia są spełnione. Spróbujmy znaleźć element $x \in \mathbb{Z}$, taki że $\varphi(x) = (2 + (3), 3 + (10), 2 + (7))$. Oznacza to, że szukamy liczby całkowitej x, której reszta przy dzieleniu przez 3 wynosi 2, przez 10 wynosi 3, a przez 7 wynosi 2. Z tego, że $3, 10, 7$ są parami względnie pierwsze mamy:

$$\begin{array}{ccccc} 3 \cdot 7 & + & (-2) \cdot 10 & = & 1 \\ (-3) \cdot 3 & + & 10 & = & 1 \\ 7 & + & (-2) \cdot 3 & = & 1. \end{array}$$

Zatem liczba $a_2 = 3 \cdot 7 \cdot (-3) \cdot 3 = (1 - (-2) \cdot 10)(1 - 10)$ daje resztę 1 przy dzieleniu przez 10 oraz reszte 0 przy dzieleniu przez 3 i przez 7, zaś $3a_2$ daje resztę 3 przy dzieleniu przez 10 oraz reszte 0 przy dzieleniu przez 3 i przez 7. Postępując analogicznie znajdujemy $a_1 = 70$, $a_3 = 120$. Ostatecznie $x = 2a_1 + 3a_2 + 2a_3$ jest szukaną liczbą całkowitą. Dowód twierdzenia w postaci ogólnej przebiega podobnie.
Dowód. Teza punktu b) jest oczywista i prawdziwa dla dowolnego ciągu ideałów $I_1, \ldots, I_n$.

Aby dowieść surjektywności odwzorowania φ wystarczy pokazać, że wszystkie elementy postaci $(0, \ldots, 0, y + I, 0, \ldots, 0)$ *są w obrazie* odwzorowania φ. Wynika to z faktu, że $\varphi(R)$ jest podpierścieniem w rozpatrywanym produkcie, a podpierścień generowany przez tego rodzaju elementy jest równy całemu produktowi. W celu dalszego uproszczenia rozpatrywanej sytuacji zauważmy, że jeżeli $\varphi(x) = (0, \ldots, 0, 1 + I, 0, \ldots, 0)$, to $\varphi(x \cdot y) = (0, \ldots, 0, y + I, 0, \ldots, 0)$. Wystarczy zatem pokazać, że w obrazie odwzorowania φ są wszystkie elementy postaci $(0, \ldots, 0, 1+I, 0, \ldots, 0)$. Nie ograniczając ogólności rozważań (a zyskując na przejrzystości zapisu) możemy zająć się przypadkiem elementu $(1+I, 0, \ldots, 0)$. Naszym celem jest wskazanie elementu a, takiego że $1 - a \in I_1$, a dla $i > 1$ zachodzi $a \in I_i$. Ale taki element łatwo wskazać:

Z założenia że ideały I_1 oraz I_i są względnie pierwsze wynika, że istnieją elementy $x_i \in I_1$ oraz $y_i \in I_i$, dla których $x_i + y_i = 1$. Wówczas element a zdefiniowany jako

$$a = \prod_{i \neq 1} (1 - x_i)$$

lub równoważnie

$$a = \prod_{i \neq 1} y_i$$

spełnia warunki:

$$a - 1 \in I_1 \quad \text{(to ze względu na pierwszy zapis)}$$

oraz:

$$a \in I_i \quad \text{dla } i \neq 1, \text{ (to ze względu na drugi zapis)},$$

co właśnie chcieliśmy uzyskać.

Kończy to dowód punktu a) a wraz z twierdzeniem o izomorfizmie dowód całego twierdzenia. □

Praktyczne zastosowanie twierdzenia chińskiego o resztach wymaga przedstawienia ideału I w postaci części wspólnej skończonej liczby ideałów względnie pierwszych. Okaże sie, że dla pewnej klasy pierścieni będziemy umieli to zrobić.