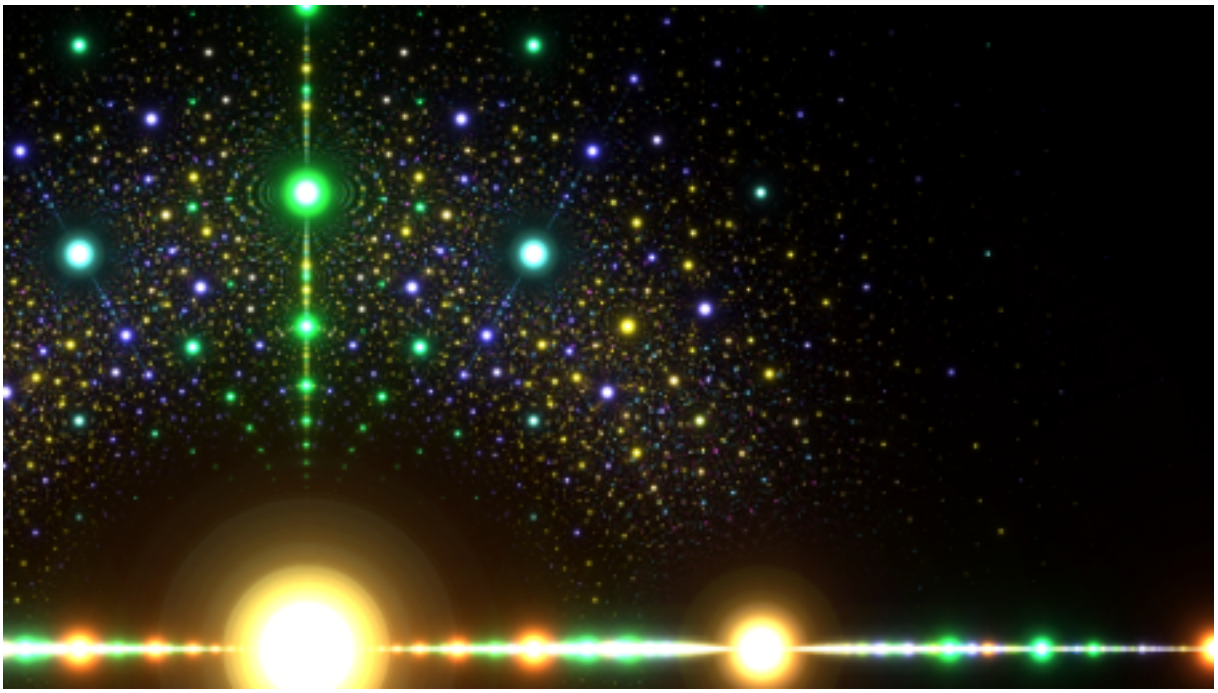
“Dziewięć dla śmiertelników”



Algebraiczne niebo. Pierwiastki zespolone wielomianów o współczynnikach całkowitych.

Uwaga: W całym skrypcie rzeczy intuicyjne i objaśnienia pisane są *italikami* (ale również treści definicji, twierdzeń i lematów są pisane italikami – nie omylcie się!). W książkowych dowodach te wyjaśnienia są zwykle pomijane.

1.1 Dwie definicje pierścienia

1. *Intuicyjna – do zrozumienia.*

   Pierścień jest to struktura, gdzie można sensownie dodawać i mnożyć.

2. *Formalna – do dowodu.*

   Definicja *Pierścieniem (z jedynką) będę nazywać zbiór R, z określonymi działaniami $+$ i $\cdot$ takimi, że*

   (a) R jest grupą przemienną ze względu na $+$, której element neutralny oznaczam 0.

   (b) Dla wszystkich $a, b \in R$ mamy $a \cdot b \in R$.

   (c) Działanie $\cdot$ jest łączne, tj. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ dla wszystkich $a, b, c \in R$.

   (d) Istnieje element neutralny mnożenia $e \in R$:

   $$e \cdot a = a \cdot e = a$$

   dla wszystkich $a \in R$. Element ten jest jedyny (rozumowanie podobne jak dla grup), oznaczamy go 1 i nazywamy jedynką:

   $$1 \cdot a = a \cdot 1 = a$$

(e) Działanie $\cdot$ jest rozdzielne względem $+$:

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

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

dla wszystkich $a, b, c \in R$.

Trochę własności:

Dla każdego $a \in R$ zachodzi

$$a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$$

odejmujemy $a\cdot 0$ stronami i otrzymujemy $0 = a\cdot 0$.
Dla każdych $a, b \in R$ zachodzi

$$-ab = (-a)b = a(-b)$$

Dowód: $ab - ab = 0 = a0 = a(b+(-b)) = ab + a(-b)$, stąd $-ab = a(-b)$. Analogicznie $ab - ab = 0 = (a+(-a))b = ab + (-a)b$, więc $-ab = (-a)b$.

1.2 Własności pierścieni i ideały

1. **Definicja** *Niech R będzie pierścieniem. Powiemy, że R jest przemienny, jeżeli*

   $$a\cdot b = b\cdot a$$

   dla wszystkich $a, b \in R$.

2. Jeżeli $R_1, R_2, \ldots, R_n$ są pierścieniami to definiujemy pierścień

   $$R_1 \times R_2 \times \cdots \times R_n$$

   jako zbiór $R_1 \times R_2 \times \cdots \times R_n$ z działaniami "po współrzędnych".

3. **Definicja (Ideał)** *Niech R będzie pierścieniem. Podzbiór J pierścienia R nazywamy ideałem jeżeli:*

   (a) I jest podgrupą przemienną ze względu na $+$.
   (b) Dla dowolnego $r \in R, i \in I$ zachodzi

   $$r\cdot i \in I \text{ oraz } i\cdot r \in I$$

   "J jest ideałem R" oznaczamy przez $J \lhd R$.

4. Pojęcie ideału rozszerza pojęcie kongruencji:
   Piszemy $a \equiv b \mod I$ jeżeli $b - a \in I$. Załóżmy, że

   $$a \equiv b \mod I, \quad c \equiv d \mod I$$

   Wtedy (m. in.)

   $$b \equiv a \mod I$$

   $$a + c \equiv b + d \mod I$$

   $$a - c \equiv b - d \mod I$$

   $$ac \equiv bd \mod I$$

   Udowodnię dla przykładu ostatnią (najtrudniejszą) własność.

   $$a \equiv b \mod I \Rightarrow a - b \in I \Rightarrow (a-b)c \in I$$

   $$c \equiv d \mod I \Rightarrow d - c \in I \Rightarrow b(d-c) \in I$$

   $$(a-b)c \in I,\ b(d-c) \in I \Rightarrow ac - bd = (a-b)c - b(d-c) \in I \Rightarrow ac \equiv bd \mod I$$

5. W dowolnym pierścieniu R mamy dwa ideały: R i $\{0\}$. *Warto to sprawdzić, żeby oswoić się z definicją ideału!*

1.3 Zastosowanie – ideały w $\mathbb{Z}$ i nie tylko.

ZADANIE
Znaleźć wszystkie ideały pierścienia $\mathbb{Z}$.
ROZWIĄZANIE.

TEZA: Ideały $\mathbb{Z}$ to zbiory liczb postaci $\{\dots, -2n, -n, 0, n, 2n, \dots\}$ gdzie n jest liczbą całkowitą.
Krócej zbiór $\{\dots, -2n, -n, 0, n, 2n, \dots\}$ zapiszemy jako $\mathbb{Z} \cdot n$.
DOWÓD:

1. Zbiór $\mathbb{Z} \cdot n$ jest ideałem w $\mathbb{Z}$.

   Po pierwsze mamy sprawdzić, że da się sensownie dodawać:

   Poniższy dowód to typowe pałowanie z definicji: mamy zbiór elementów o danej własności (tutaj: elementy są podzielne przez n) i przeliczamy kolejne aksjomaty grupy metodą: tłumaczymy założenia aksjomaty (np. mamy $a, b \in \mathbb{Z}n$) na język własności: ($n|a$ i $n|b$), po czym tłumaczymy tezę ($a+b \in \mathbb{Z}n$) na język własności: $n|a+b$ i dowód nagle okazuje się trywialny :)

   - Dwa elementy ideału – liczby podzielne przez n dają w sumie liczbę podzielną przez n a więc element ideału.
   - Dodawanie jest łączne tj. $a+(b+c) = (a+b)+c$ dla wszystkich $a, b, c \in \mathbb{Z}n$, gdyż $a+(b+c) = (a+b)+c$ dla wszystkich $a, b, c \in \mathbb{Z}$, a $\mathbb{Z}n \subseteq \mathbb{Z}$.
   - Liczba 0 – element neutralny dodawania jest podzielna przez n, czyli $0 \in \mathbb{Z}n$ i mamy w ideale element neutralny.
   - Dla każdej liczby $a \in \mathbb{Z}n$ liczba $-a$ także jest podzielna przez n, a więc należy do $\mathbb{Z}n$.

   Następnie sprawdzamy, czy spełniona jest własność: dla wszystkich $r \in \mathbb{Z}$ i $i \in \mathbb{Z}n$ zachodzi $ri, ir \in \mathbb{Z}n$.

   Weźmy dowolne $r \in \mathbb{Z}, i \in \mathbb{Z}n$. Po pierwsze $ri = ir$.

   $i \in \mathbb{Z}n$, więc $n|i$, czyli $n|ri$ ergo $ri \in \mathbb{Z}n$.

2. Rozważmy teraz dowolny ideał $I \lhd \mathbb{Z}$. Chcemy pokazać, że I jest postaci $\mathbb{Z}k$ dla pewnego $k \in \mathbb{Z}$.

   Trzeba dla danego I jakoś zgadnąć to k. Hm, co wyróżnia n w $\mathbb{Z}n$? Ależ tak – n jest liczbą o najmniejszym module!

   Jeżeli $I = \{0\}$ to nie ma sprawy. Załóżmy, że $I \neq \{0\}$.

   Niech l będzie niezerowym elementem I o najmniejszym module. Chcemy udowodnić, że $I = \mathbb{Z}l$.

   Po pierwsze $l \in I$ i I jest ideałem, zatem $2l = l+l \in I$, $3l = 2l+l \in I$ itd., analogicznie $0 = l-l \in I$, $-l = 0-l \in I$, $-2l = -l-l \in I$ itd.

   Ostatecznie $\mathbb{Z}l \subseteq I$.

   Wystarczy więc udowodnić, że $I \subseteq \mathbb{Z}l$.

   Weźmy dowolne $i \in I$. Zauważmy że element $i \mod l$ czyli reszta z dzielenia i przez l także należy do I! Faktycznie dodając lub odejmując l od i dostatecznie wiele razy otrzymujemy $i \mod l$ i nie wychodzimy z ideału (*Bo stosujemy tylko dodawanie i odejmowanie a te nie wybijają nas z ideału*)!

   Ale $|i \mod l| < |l|$. Element l miał najmniejszy moduł spośród elementów niezerowych a $i \mod l$ ma mniejszy moduł, zatem $i \mod l = 0$, $l|i$, $i \in \mathbb{Z}l$. Dowolny element I należy do $\mathbb{Z}l$, czyli $I \subseteq \mathbb{Z}l$. To kończy dowód.

Wniosek *Zwykłe kongruencje* $\mod n$ *to kongruencje* $\mod \mathbb{Z}n$ *w sensie powyższej definicji. Zatem jedyne sensowne kongruencje, które da się opisać na* $\mathbb{Z}$ *to kongruencje* $\mod n$.

Lemat *Niech $I \lhd R$ i $J \lhd R$ będą ideałami pierścienia R. Wtedy $I \cap J$ (*zbiór będący przecięciem zbiorów*) jest ideałem R.*

Dowód. *Cóż, trzeba przeliczyć aksjomaty...*

Jeżeli $a, b \in I \cap J$ to $a, b \in I$ a I jest ideałem, więc $a + b \in I$. Analogicznie $a, b \in J$ a J jest ideałem stąd $a + b \in J$.

$a + b \in I, J$, czyli $a + b \in I \cap J$.

Pozostałe aksjomaty związane z dodawaniem przelicza się podobnie i zostawiam to czytelnikowi.

Udowodnijmy jeszcze, że jeżeli $i \in I \cap J$ a $r \in R$ to $ri, ir \in I \cap J$.

$i \in I \cap J$, stąd $i \in I$, czyli (I – ideał), $ri \in I$. Analogicznie $i \in J$, czyli $ri \in J$. Łącznie $ri \in I \cap J$. Identycznie argumentując $ir \in I \cap J$. ■

Lemat *Niech R i S będą pierścieniami z 1. Wtedy każdy ideał $I \lhd R \times S$ jest postaci $I = J \times K$, gdzie $J \lhd R$ i $K \lhd S$.*

Ten lemat oddaje istotę: w pierścieniu działa się po współrzędnych, niezależnie od siebie.

Dowód. *Dowód nieco inny niż na kółku.*

Po pierwsze zauważmy, że $R \times \{0\}$ i $\{0\} \times S$ są ideałami w $R \times S$. Można to przeliczyć bezpośrednio, a po krótkim zastanowieniu powinno to być oczywiste.

Niech I będzie dowolnym ideałem $R \times S$.

Rozważmy rzuty I na pierwszą i drugą współrzędną:

$$J' := I \cap (R \times \{0\}) \qquad K' := I \cap (\{0\} \times R)$$

Z poprzedniego lematu wiemy, że J', K' są ideałami w $R \times S$.

Zauważmy, że każdy element J' ma drugą współrzędną zerową, zatem J' jest postaci $J \times \{0\}$ dla pewnego zbioru J. J' jest ideałem $R \times S$, a więc J jest ideałem R (ew. sprawdzenie bezpośrednie).

Analogicznie $K' = \{0\} \times K$ i K jest ideałem S.

Twierdzę, że $I = J \times K$. Udowodnię zawierania $I \subseteq J \times K$ oraz $J \times K \subseteq I$.

$I \subseteq J \times K$. Weźmy dowolne $(j, k) \in I$. I jest ideałem, zatem $(j, k) \cdot (1, 0) = (j, 0) \in I$. Ale również $(j, 0) \in R \times \{0\}$, a więc $(j, 0) \in I \cap (R \times \{0\}) = J'$, z zatem $j \in J$.

Analogicznie $(j, k)(0, 1) = (0, k) \in K'$ czyli $k \in K$. Tym samym $(j, k) \in J \times K$.

$J \times K \subseteq I$.

Weźmy dowolne $j \in J$ i $k \in K$. Z definicji J, J' mamy $(j, 0) \in J' \subseteq I$. Analogicznie z definicji K, K' zachodzi $(0, k) \in K' \subseteq I$.

Zatem $(j, k) = (j, 0) + (0, k) \in I$ bowiem $(j, 0), (0, k) \in I$. ■

Wniosek *Wszystkie ideały pierścienia $\mathbb{Z} \times \mathbb{Z}$ są postaci $\mathbb{Z}k \times \mathbb{Z}l$ dla pewnych $k, l \in \mathbb{Z}$.*