The $\mathbb{Z}$ is not enough.

1.1 Pierścień ilorazowy

Uwaga: Formalizmy / Watch out: formalisms ahead.

Załóżmy, że mamy pierścień R i ideał $I \lhd R$.

Podzielmy pierścień R na zbiory reszt z dzielenia przez I tj. zgodnie z zasadą, że a i b są w jednym zbiorze wtedy i tylko wtedy, gdy

$$a \equiv b \mod I$$

Bardzo formalnie: Tak można podzielić, gdyż $a \equiv a$ dla każdego elementu, $a \equiv b$ jest równoważne $b \equiv a$ oraz $a \equiv b \equiv c$ implikuje $a \equiv c$.

Dla danego $a \in R$ resztą a modulo I będę nazywać zbiór wszystkich elementów R, które przystają do elementu a modulo I. Będę ten zbiór oznaczać jako $a \mod I$.

Twierdzę, że zbiór wszystkich reszt to pierścień z działaniami

$$(a \mod I) + (b \mod I) = (a + b \mod I)$$

$$-(a \mod I) = (-a \mod I)$$

$$(a \mod I) \cdot (b \mod I) = (ab \mod I)$$

tworzy pierścień, który nazywam *pierścieniem ilorazowym R przez I* i oznaczam R/I albo $\frac{R}{I}$.

1.2 Epimorfizmy i izomorfizmy

Na poprzednim kółku potykaliśmy się o takie nienazywalne kulturalnie rzeczy jak "widać, że to działanie jest na pierwszej współrzędnej, ale jak to uzasadnić formalnie?". Do uzasadniania takich rzeczy służy pojęcie izomorfizmu.

Intuicyjnie epimorfizm jest sensowną funkcją na, innymi słowy funkcją, która zachowuje wszystkie algebraiczne własności.

Definicja (Epimorfizm) *Niech R i R' będą pierścieniami. Epimorfizmem pomiędzy pierścieniami R i R' nazywamy każdą funkcję $f : R \to S$, przyjmującą każdą możliwą wartość z S oraz taką, że*

$$f(x + y) = f(x) + f(y)$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

Uwaga: $+, \cdot$ z lewej strony wykonywane są w pierścieniu R, a te z prawej strony – w pierścieniu S.

Lemat *Jeżeli f jest epimorfizmem to $f(0)$ jest równe zeru pierścienia S, a $f(1)$ jest równe jedynce pierścienia S, krócej $f(0) = 0, f(1) = 1$.*

Dowód.

$f(0) = f(0 + 0) = f(0) + f(0)$, stąd (odejmujemy od prawej strony lewą) $f(0) = 0$.

W pierścieniu S istnieje 1. Funkcja f przyjmuje wszystkie wartości, zatem istnieje takie $b \in R$, że $f(b) = 1$.

Obliczam $f(1) = f(1) \cdot 1 = f(1) \cdot f(b) = f(1 \cdot b) = f(b) = 1$. ■

Definicja (Jądro) *Dla danego epimorfizmu $f : R \to S$ definiujemy* jądro *f jako*

$$\ker f := \{r \in R \mid f(r) = 0\}$$

Lemat *Jeżeli $f : R \to S$ jest epimorfizmem to* $\ker f \lhd R$.

Definicja (Izomorfizm) *Funkcję $f : R \to R'$ nazywamy izomorfizmem, jeżeli f jest różnowartościowa.*

Jak wiemy istnieje wtedy funkcja $f^{-1} : R' \to R$. Dodatkowo f^{-1} zachowuje dodawanie i mnożenie, więc f^{-1} jest również izomorfizmem.

Mówimy, że pierścienie R, R' są izomorficzne jeżeli istnieje pomiędzy nimi izomorfizm. Zapisujemy to jako $R \simeq R'$.

Dla algebraika pierścienie izomorficzne są identyczne – cała struktura jest zachowana przez odpowiednie przekształcenia.

Wniosek *Epimorfizm jest izomorfizmem wtedy i tylko wtedy, gdy jego jądro jest zerowe.*

Wniosek *Jeżeli I jest ideałem R, to przekształcenie $f : R \to R/I$ dane wzorem*

$$f(x) = x \mod I$$

jest epimorfizmem z jądrem I.

Twierdzenie (* Pierwsze twierdzenie o izomorfizmie) *Jeżeli $f : R \to S$ jest epimorfizmem to*

$$\frac{R}{\ker f} \simeq S$$

1.3 Przykłady ideałów i pierścieni ilorazowych

1. *Motywacją całej teorii pierścieni (do czasu) był $\mathbb{Z}$ zatem:*

   Rozważmy $\mathbb{Z}n \lhd \mathbb{Z}$. Pierścień ilorazowy $\frac{\mathbb{Z}}{\mathbb{Z}n}$ to n-elementowy pierścień reszt z dzielenia przez n.

2. Rozważmy pierścień wielomianów $\mathbb{R}[x]$ i wielomiany bez wyrazu wolnego: $x\mathbb{R}[x]$.

   Wtedy $x\mathbb{R}[x] \lhd \mathbb{R}[x]$ oraz

   $$\frac{\mathbb{R}[x]}{x\mathbb{R}[x]} \simeq \mathbb{R}$$

3. Rozważmy funkcje z odcinka $[0, 1]$ w $\mathbb{R}$, dla dalszego użycia oznaczmy zbiór tych funkcji przez $\mathcal{F}$. Funkcje te tworzą pierścień z działaniami po wartościach:

   $$(f + g)(x) := f(x) + g(x)$$

   $$(-f)(x) := -f(x)$$

   $$(f \cdot g)(x) := f(x) \cdot g(x)$$

   Podzbiór $I := \{f \in \mathcal{F} \mid f(0) = 0\}$ jest ideałem pierścienia $\mathcal{F}$.

   * Uzasadnij, że $\frac{\mathcal{F}}{I} \simeq \mathbb{R}$.

1.4 Przykłady epimorfizmów i izomorfizmów

1. Jeżeli $\mathcal{F}$ jest pierścieniem funkcji z $[0, 1]$ w $\mathbb{R}$ z dodawaniem i mnożeniem po wartościach (jak wyżej) to przypisanie funkcji jej wartości w 0, formalniej $ev : \mathcal{F} \to \mathbb{R}$ dane przez

   $$ev(f) = f(0)$$

   jest epimorfizmem o jądrze $\{f \in \mathcal{F} \mid f(0) = 0\}$.

2. Pierścienie $\mathbb{Z} \times \{0\}$ oraz $\mathbb{Z}$ są izomorficzne przez izomorfizm $(z, 0) \to z$.

1.5 Zastosowanie

Lemat *Dla dowolnych liczb naturalnych a, b zachodzi równoważność*

$$NWD(a,b) = 1 \Leftrightarrow \text{ istnieją } t, u \in \mathbb{Z} : ta + ub = 1.$$

Twierdzenie (Algebraiczne chińskie twierdzenie o resztach) *Jeżeli liczby $k_1, \ldots, k_m$ są parami względnie pierwsze tj. $NWD(k_i, k_j) = 1$ dla wszystkich i, j oraz $n = k_1 k_2 \ldots k_m$, to*

$$\frac{\mathbb{Z}}{\mathbb{Z}n} \simeq \frac{\mathbb{Z}}{\mathbb{Z}k_1} \times \frac{\mathbb{Z}}{\mathbb{Z}k_2} \times \cdots \times \frac{\mathbb{Z}}{\mathbb{Z}k_m}$$

Wniosek (Chińskie twierdzenie o resztach) *Jeżeli liczby $k_1, \ldots, k_m$ są parami względnie pierwsze tj. $NWD(k_i, k_j) = 1$ dla wszystkich i, j liczby $r_1, \ldots, r_m$ są całkowite oraz $n = k_1 k_2 \ldots k_m$, to istnieje dokładnie jedna liczba całkowita M z przedziału $[0, n)$ spełniająca równania*

$$M \equiv r_1 \mod k_1$$

$$M \equiv r_2 \mod k_2$$

$$\ldots$$

$$M \equiv r_m \mod k_m$$

Wniosek *Funkcja Eulera ϕ jest zdefiniowana dla każdego n naturalnego jako ilość liczb naturalnych mniejszych od n i względnie pierwszych z n.*

Jeżeli $k_1, \ldots, k_m$ są parami względnie pierwsze, to

$$\phi(k_1 k_2 \ldots k_m) = \phi(k_1) \cdot \phi(k_2) \cdot \ldots \cdot \phi(k_m)$$

Jeżeli $n = p_1^{a_1} \ldots p_k^{a_k}$ jest rozkładem n na czynniki pierwsze, to $\phi(n) = \phi(p_1^{a_1}) \ldots \phi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdot \ldots \cdot \left(p_k^{a_k} - p_k^{a_k - 1}\right)$.

Zadanie (Tegoroczny Konkurs Matematyczny PB – klasy pierwsze, zadanie 2, uogólnione.) *Niech $n = p_1^{a_1} \cdot \ldots p_k^{a_k}$ będzie rozkładem liczby naturalnej $n > 1$ na czynniki pierwsze. Wtedy liczb całkowitych a z przedziału $[0, n)$ spełniających równanie*

$$a^2 \equiv a \mod n$$

jest dokładnie 2^k.