Spis treści

Przedmowa . . . 9
1. Afiniczne zbiory algebraiczne . . . 11
   1.1. Definicja zbiorów afinicznych . . . 11
   1.2. Twierdzenie Hilberta o bazie . . . 16
   1.3. Twierdzenie Hilberta o zerach . . . 17
   1.4. Ideał podzbioru afinicznego . . . 19
   1.5. Topologia Zariskiego . . . 21
   1.6. Pierścień funkcji regularnych i jego spektrum . . . 23
   1.7. Zbiory nierozkładalne . . . 25
   1.8. Funkcje wymierne . . . 29
   1.9. Snop funkcji regularnych . . . 32
   1.10. Morfizmy zbiorów afinicznych . . . 33
   1.11. Iloczyny zbiorów afinicznych . . . 37
   1.12. Twierdzenie Chevalleya o obrazie . . . 40
   1.13. Przekształcenia wymierne . . . 43
   1.14. Przestrzenie ze snopami funkcji . . . 46
   1.15. Podzbiory analityczne przestrzeni zespolonych . . . 48
   1.16. Snopy, schematy afiniczne . . . 49
   Zadania . . . 55
2. Rzutowe zbiory algebraiczne . . . 57
   2.1. Definicja zbiorów rzutowych . . . 57
   2.2. Algebry z gradacją . . . 59
   2.3. Własności zbiorów rzutowych . . . 60
   2.4. Funkcje wymierne na zbiorach rzutowych . . . 61
   2.5. Morfizmy zbiorów rzutowych . . . 62
   2.6. Iloczyny zbiorów rzutowych . . . 63
   2.7. Zbiory rzutowe a zbiory afiniczne . . . 64
   2.8. Algebra z gradacją zbioru rzutowego . . . 66
   Zadania . . . 67
3. Ogólne zbiory algebraiczne . . . 69
   3.1. Definicja ogólnych zbiorów algebraicznych i ich morfizmów . . . 69
   3.2. Podstawowe własności zbiorów algebraicznych . . . 72
   3.3. Schematy . . . 73
   3.4. Własności morfizmów . . . 75

3.5. Problemy i metody geometrii algebraicznej . . . 80
3.6. Przekształcenia wymierne w przestrzenie rzutowe . . . 85
Zadania . . . 89
4. Grupy algebraiczne . . . 91
4.1. Definicja grupy algebraicznej . . . 91
4.2. Afiniczne grupy algebraiczne . . . 94
4.3. Algebry Hopfa . . . 96
4.4. Działania grup na zbiorach algebraicznych . . . 97
Zadania . . . 99
5. Przykłady konstrukcji zbiorów algebraicznych . . . 101
5.1. Grassmanniany . . . 101
5.2. Zanurzenia torusa . . . 104
5.3. Zbiory warstw podgrupy grupy algebraicznej . . . 107
Zadania . . . 110
6. Wymiar zbiorów algebraicznych . . . 111
6.1. Własności stopni przestępnych . . . 111
6.2. Definicja wymiaru . . . 112
6.3. Własności wymiaru . . . 113
6.4. Wymiar Krulla . . . 117
Zadania . . . 117
7. Teoria lokalna . . . 120
7.1. Pierścienie lokalne . . . 121
7.2. Topologia adyczna . . . 122
7.3. Przestrzeń kostyczna, różniczka funkcji . . . 123
7.4. Przestrzeń styczna . . . 124
7.5. Pierścienie regularne i normalne . . . 128
7.6. Punkty gładkie . . . 130
7.7. Układy parametrów . . . 131
7.8. Formy różniczkowe i pola styczne . . . 135
7.9. Różniczki Kählera . . . 136
Zadania . . . 138
8. Zbiory gładkie i zbiory normalne . . . 140
8.1. Przykłady zbiorów gładkich . . . 140
8.2. Pierścienie Dedekinda . . . 142
8.3. Grupa klas ideałów pierścienia Dedekinda . . . 144
8.4. Waluacje . . . 146
8.5. Rozszerzenia całkowite pierścieni Dedekinda . . . 149
8.6. Zbiory normalne i normalizacja . . . 151
8.7. Rozdmuchania i ściągnięcia . . . 154
8.8. Desingularyzacja, modele . . . 158
8.9. Formy różniczkowe na zbiorach algebraicznych . . . 159
8.10. Genus geometryczny zbioru gładkiego . . . 165
Zadania . . . 168
9. Wiązki wektorowe i dywizory . . . 171
9.1. Definicja wiązek wektorowych . . . 171
9.2. Snop przekrojów wiązki wektorowej . . . 173
9.3. Konstrukcje wiązek wektorowych . . . 174
9.4. Wiązka styczna i kostyczna . . . 177
9.5. Dywizory Cartiera . . . 178

9.6. Dywizory Weila 179
9.7. Dywizory na zbiorach gładkich 182
9.8. Przekształcenie wymierne wyznaczone przez dywizor 184
9.9. Dywizory na krzywych gładkich 186
10. Snopy i kohomologie 189
10.1. Snopy koherentne 189
10.2. Snopy grup 193
10.3. Snopy ilorazowe 196
10.4. Ciągi dokładne snopów 199
10.5. Snopy koherentne w geometrii analitycznej 203
10.6. Geometria formalna 207
10.7. Aksjomaty teorii kohomologii 209
10.8. Konstrukcja Čecha 211
10.9. Twierdzenie Riemanna–Rocha dla krzywych 213
10.10. Powierzchnie Riemanna 219
10.11. Teoria przecięć 220
Zadania 225
Bibliografia 227
Skorowidz symboli 230
Skorowidz pojęć 232

Przedmowa

Celem podręcznika jest zaznajomienie czytelnika z podstawowymi pojęciami geometrii algebraicznej. Może on służyć zarówno jako kompendium podstawowej wiedzy z tego przedmiotu, użyteczne dla każdego matematyka, jak i jako wstęp do dalszych studiów. Świadomość tego celu, przy naturalnym dążeniu autora do ograniczenia objętości książki do rozsądnych rozmiarów, spowodowała, że sporo tematów zostało potraktowanych informacyjnie, bez próby wniknięcia w ich istotę.

Przedstawiony tu wykład prowadzony jest w duchu książki Szafarewicza [40], która doczekała się licznych wydań i tłumaczeń. Program wykładu jest znacznym okrojeniem materiału zawartego w tym podręczniku i może być traktowany jako przygotowanie do systematycznej lektury tej książki. Inny, bardziej algebraiczny i formalny, punkt widzenia prezentowany jest w książce Robina Hartshorne'a *Algebraic geometry* [13]. Jest to z pewnością pozycja godna polecenia, ale trudna dla czytelnika, który dopiero poznaje podstawy tego przedmiotu. Na drugim krańcu lokują się bardzo elementarne wprowadzenia do geometrii algebraicznej Klausa Hulka *Elementary algebraic geometry* [16] oraz Milesa Reida *Undergraduate algebraic geometry* [35]. Materiał w nich zawarty jest bardzo skromny i nie wypełnia programu tego wykładu.

W trakcie wykładu będziemy korzystać z podstawowych pojęć algebraicznych, takich jak wielomian, ciało, grupa, pierścień, homomorfizm i ideał, oraz dotyczących ich twierdzeń zawartych w programach algebry studiów matematycznych. Odpowiednie definicje i twierdzenia można znaleźć na przykład w [6]. W razie wykorzystywania bardziej zaawansowanych narzędzi będziemy je dokładnie formułować oraz wskazywać źródła, w których można odszukać potrzebne dowody. Będzie to niekiedy [7], a nieomal wszystkie brakujące fakty algebraiczne można odnaleźć w monografii Balcerzyka i Józefiaka [2] oraz w książce Atiyaha i McDonalda [1].

Tok przedstawiania materiału w książce czasami ulega przyśpieszeniu i tekst jest skrócony. W tych miejscach użyty jest niekiedy *druk pochyły* – jako wskazówka i ostrzeżenie dla Czytelnika, że uzasadnienie danego fragmentu wymaga zastanowienia. Celem tych skrótów jest z jednej strony uchronienie tekstu przed rozwlekłością i nudą, a z drugiej pobudzenie Czytelnika do aktywnego uczestnictwa w poznawaniu przedstawianej teorii. Trudno jednak być konsekwentnym w przestrzeganiu tej umowy. Zapewne Czytelnik znajdzie takie fragmenty tekstu, których dokładne zrozumienie sprawi mu trudność, choć nie będą one w ten sposób wyróżnione.

Autor wyraża gorące podziękowanie prof. Adrianowi Langerowi za przejrzenie maszynopisu i cenne uwagi oraz recenzentowi tej książki, prof. Grzegorzowi Banaszakowi, za olbrzymi trud towarzyszący wykryciu dużej liczby pomyłek i przeoczeń w pierwotnej wersji tekstu oraz uwagi merytoryczne. Specjalne podziękowanie kieruję do redaktora książki, p. Jerzego Trzeciaka. Jego uwagi oraz zastrzeżenia dotyczyły nie tylko spraw redakcyjnych, ale i merytorycznych. Pozwoliły one na dokonanie zmian i uzupełnień, które przyczyniły się do ulepszenia tekstu w wielu miejscach.

Dziękuję też serdecznie prof. Pawłowi Strzeleckiemu, redaktorowi Księgozbioru Matematycznego, za mozolne działania, które doprowadziły do ukazania się tej książki drukiem.

Oznaczenia i ogólne założenia

- $\mathbb{C}$ – ciało liczb zespolonych, $\mathbb{R}$ – ciało liczb rzeczywistych, $\mathbb{Q}$ – ciało liczb wymiernych, $\mathbb{Z}$ – pierścień liczb całkowitych, $\mathbb{N}$ – zbiór liczb naturalnych $\{1, 2, \ldots\}$, $\mathbf{F}_q$ – ciało skończone o q elementach
- K – ustalone dla rozważań ciało podstawowe
- $K^* = K \setminus \{0\}$ – grupa multiplikatywna ciała K
- K^+ – grupa addytywna ciała K
- $\mathbb{A}_K^n$ – przestrzeń afiniczna, $\mathbb{P}_K^n$ – przestrzeń rzutowa (nad ciałem K)

Termin *pierścień* oznacza *pierścień przemienny z 1*. Zakładamy, że homomorfizmy pierścieni zachowują elementy 1. Dla pierścienia P przez *P-algebrę* rozumiemy pierścień R wraz z ustalonym homomorfizmem $P \to R$, a przez *P-homomorfizm* P-algebr wyznaczonych przez $\phi_1 : P \to R_1$ oraz $\phi_2 : P \to R_2$ rozumiemy taki homomorfizm $\psi : R_1 \to R_2$, że $\psi \circ \phi_1 = \phi_2$.

Jeśli P jest podpierścieniem pierścienia R oraz $a_1, \ldots, a_m \in R$, to symbol $P[a_1, \ldots, a_m]$ oznacza podpierścień w R generowany przez $P \cup \{a_1, \ldots, a_m\}$. Jeśli K jest podciałem ciała L oraz $a_1, \ldots, a_m \in L$, to $K(a_1, \ldots, a_m)$ oznacza podciało w L generowane przez $K \cup \{a_1, \ldots, a_m\}$.

Dla pierścienia P bez dzielników zera, $Q(P)$ oznacza ciało ułamków pierścienia P. Jeśli P jest pierścieniem oraz $a_1, \ldots, a_m \in P$, to $(a_1, \ldots, a_m)$ oznacza ideał w P generowany przez zbiór $\{a_1, \ldots, a_m\}$.

1 Afiniczne zbiory algebraiczne

W książce tej będziemy zakładać, że K jest ustalonym ciałem *algebraicznie domkniętym*, a więc takim, że każdy wielomian jednej zmiennej stopnia dodatniego o współczynnikach w K jest iloczynem wielomianów liniowych (tj. stopnia 1). Dla teorii przedstawianej w tej książce jest to założenie naturalne. Ponadto, ponieważ każde ciało ma (jednoznacznie wyznaczone z dokładnością do izomorfizmu) rozszerzenie algebraiczne, które jest ciałem algebraicznie domkniętym ([7, tw. 3.2, str. 181]), założenie to nie ogranicza zakresu rozważań.

Przykładami ciał algebraicznie domkniętych są:

- ciało liczb zespolonych $\mathbb{C}$,
- ciało liczb algebraicznych (złożone ze wszystkich takich liczb zespolonych, które są algebraiczne nad ciałem liczb wymiernych),
- dla dowolnej liczby pierwszej p, suma

  $$\bigcup \mathbf{F}_{p^{n!}}$$

  wstępującego ciągu ciał skończonych $\mathbf{F}_{p^{n!}}$ o $p^{n!}$ elementach.

Charakterystykę ciała K oznaczać będziemy przez $\mathrm{ch}(K)$.

Pierścień wielomianów n zmiennych $x_1, \dots, x_n$ o współczynnikach w K oznaczamy przez $K[x_1, \dots, x_n]$.

1.1. Definicja zbiorów afinicznych

Geometria algebraiczna (*afiniczna*) zajmuje się badaniem takich podzbiorów skończenie wymiarowych przestrzeni afinicznych, które są zbiorami rozwiązań układów równań wielomianowych.

Jeśli $n, r \in \mathbb{N}$ są liczbami naturalnymi, a $f_1, \ldots, f_r$ wielomianami o n niewiadomych $x_1, \ldots, x_n$, to zbiór rozwiązań układu równań

$$f_1 = 0, \ \ldots, \ f_r = 0$$

nazywamy *zbiorem algebraicznym* w K^n.

Jeśli $\mathbb{A}^n_K$ jest n-wymiarową przestrzenią afiniczną (nad ciałem K), to po ustaleniu w niej układu współrzędnych można utożsamić $\mathbb{A}^n_K$ z K^n. Rozważmy podzbiór w $\mathbb{A}^n_K$, określony w tych współrzędnych przez układ równań wielomianowych

$$f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_r(x_1, \ldots, x_n) = 0.$$

W dowolnym innym układzie współrzędnych afinicznych, związanym z poprzednim za pomocą (odwracalnej) liniowej zamiany zmiennych

$$x_i = b_i + \sum_{j=1}^{n} a_{ij} y_j,$$

gdzie $a_{ij}, b_i \in K$, zbiór ten jest określony przez równania

$$f_1\Big(b_1 + \sum_{j=1}^{n} a_{1j} y_j, \ldots, b_n + \sum_{j=1}^{n} a_{nj} y_j\Big) = 0,$$
$$\vdots$$
$$f_r\Big(b_1 + \sum_{j=1}^{n} a_{1j} y_j, \ldots, b_n + \sum_{j=1}^{n} a_{nj} y_j\Big) = 0;$$

są to nadal równania wielomianowe względem współrzędnych y_i. Pozwala to na rozważanie zbiorów algebraicznych w $\mathbb{A}^n_K$ bez odwoływania się do konkretnego układu współrzędnych.

Często mówimy „zbiór algebraiczny afiniczny” lub krótko „zbiór afiniczny” zamiast „podzbiór algebraiczny przestrzeni afinicznej”.

Przykłady

1 Zbiór pusty i cała przestrzeń $\mathbb{A}^n_K$ są podzbiorami algebraicznymi.

2 Każdy podzbiór skończony jest algebraiczny. Istotnie, podzbiór złożony z m punktów $(a_{1,1}, \ldots, a_{1,n}), \ldots, (a_{m,1}, \ldots, a_{m,n}) \in K^n$ jest zbiorem wszystkich rozwiązań układu równań

$$(x_{i_1} - a_{1,i_1}) \cdot \ldots \cdot (x_{i_m} - a_{m,i_m}) = 0,$$

gdzie $(i_1, \ldots, i_m)$ przebiega wszystkie m-elementowe ciągi złożone z liczb $1, \ldots, n$.

W $\mathbb{A}^1_K$ nie ma innych podzbiorów algebraicznych niż podane w dwu powyższych przykładach.

3 Z twierdzeń, które udowodnimy w dalszych rozdziałach, wyniknie, że każdy podzbiór algebraiczny w $\mathbb{A}^2_K$ jest albo skończony, albo opisany przez jedno równanie.

4 Podzbiorami algebraicznymi są wszystkie podprzestrzenie afiniczne. Istotnie, każda podprzestrzeń afiniczna w K^n może być opisana jako zbiór rozwiązań układu równań

$$f_1 = 0, \ \dots, \ f_r = 0,$$

gdzie wszystkie wielomiany f_i są liniowe, tzn. postaci $a_1x_1 + \cdots + a_nx_n + b$, gdzie $a_1, \dots, a_n, b \in K$. Odwrotnie, każdy układ równań liniowych określa podprzestrzeń afiniczną. Ta prostota równań nadaje podprzestrzeniom afinicznym wyróżnioną pozycję wśród wszystkich podzbiorów algebraicznych.

5 Wyróżnione miejsce wśród podzbiorów algebraicznych zajmują też podzbiory opisane jednym równaniem dodatniego stopnia. Takie podzbiory nazywamy *hiperpowierzchniami algebraicznymi.*

6 Jeśli zbiór algebraiczny jest określony jednym równaniem

$$f(x_1, \dots, x_n) = 0,$$

gdzie f jest (niezerowym) wielomianem liniowym, to można tak dobrać układ współrzędnych, by równanie to miało postać $x_1 = 0$.

Jeśli f jest wielomianem stopnia drugiego oraz $\mathrm{ch}(K) \neq 2$, to wiadomo z teorii form kwadratowych, że można tak dobrać układ współrzędnych, by równanie $f = 0$ sprowadzić do postaci

$$x_1^2 + \cdots + x_i^2 + a = 0, \quad \text{gdzie } a = 0 \text{ lub } 1 \text{ oraz } 1 \leq i \leq n,$$

albo

$$x_1^2 + \cdots + x_i^2 + x_n = 0, \quad \text{gdzie } 1 \leq i \leq n-1.$$

Wobec tego dla $\mathrm{ch}(K) \neq 2$, $n = 2$ otrzymujemy pięć typów zbiorów:

1. Jeśli $x_1^2 = 0$ (prosta),
2. $x_1^2 + 1 = 0$ (para prostych równoległych),
3. $x_1^2 + x_2^2 = 0$ (para prostych przecinających się),
4. $x_1^2 + x_2^2 + 1 = 0$ (hiperbola),
5. $x_1^2 + x_2 = 0$ (parabola).

7 Niech $V \subset K^n$ oraz $W \subset K^m$ będą podzbiorami algebraicznymi określonymi przez równania, odpowiednio,

$$f_1(x_1, \dots, x_n) = 0, \ \dots, \ f_r(x_1, \dots, x_n) = 0$$

oraz

$$g_1(x_1, \dots, x_m) = 0, \ \dots, \ g_s(x_1, \dots, x_m) = 0.$$

Po zamianie zmiennych $x_1, \dots, x_m$ na $y_1, \dots, y_m$ w wielomianach $g_1, \dots, g_s$, wielomiany f_i, $i = 1, \dots, r$, oraz g_j, $j = 1, \dots, s$, można w naturalny sposób traktować jako elementy pierścienia $K[x_1, \dots, x_n, y_1, \dots, y_m]$, a wtedy układ równań

$$\begin{aligned} f_1(x_1, \dots, x_n) = 0, \ \dots, \ f_r(x_1, \dots, x_n) = 0, \\ g_1(y_1, \dots, y_m) = 0, \ \dots, \ g_s(y_1, \dots, y_m) = 0, \end{aligned}$$

opisuje iloczyn kartezjański $V \times W$ w $K^n \times K^m = K^{n+m}$. Wobec tego iloczyn ten (czasami mówi się też „produkt") jest afinicznym zbiorem algebraicznym.

Sugerując się przypadkiem hiperpowierzchni opisywanych równaniami stopnia 1 i 2, można by się spodziewać. że rozwój teorii zbiorów algebraicznych będzie szedł w kierunku upraszczania, poprzez dobór odpowiednich współrzędnych, układów równań opisujących dany zbiór, aby ułatwić badanie jego własności. Okazuje się jednak, że powyższe przykłady w zasadzie wyczerpują przypadki, gdy takimi metodami można łatwo uzyskać postęp. Już dla wielomianów f stopnia 3, gdy $n = 2$, problem klasyfikacji i opisu własności zbiorów opisanych równaniem $f = 0$ jest nieporównanie trudniejszy, chociaż upraszczanie równań przez odpowiedni dobór współrzędnych jest w tym przypadku nadal owocne. W innych przypadkach ani nie ma metod upraszczania układów równań, ani badanie własności zbiorów rozwiązań układów równań o – jak by się wydawało – prostej postaci nie jest zadaniem łatwiejszym.

Chociaż w pewnych sytuacjach łatwo znaleźć rozwiązania szczególne, jednak nie znajdywanie rozwiązań, a badanie własności całego zbioru rozwiązań jest celem geometrii algebraicznej. Na przykład, gdy $n, r = 1$, $\mathrm{ch}(K) = 0$ i mamy do czynienia z równaniem $x^5 + x^4 + x^3 + x + 1 = 0$ lub $x^5 + 1 = 0$, w obu przypadkach zadowolimy się łatwym do wykazania stwierdzeniem, że zbiór rozwiązań składa się z pięciu różnych elementów, i nie będziemy się starać, by je dokładnie wyznaczyć, ani też badać ich położenia na prostej K^1.

Gdy $K = \mathbb{C}$ jest ciałem liczb zespolonych, wówczas własności zbioru rozwiązań, które mamy tu na myśli, to własności geometryczne i topologiczne, na przykład wymiar. Okazuje się, że własności te można wyrażać w terminach algebraicznych, a to pozwala na ich rozpatrywanie dla dowolnego ciała K.

Niektóre z podstawowych własności zbiorów algebraicznych wynikają już z faktu, że zbiór taki daje się opisać jako zbiór rozwiązań wielomianowego układu równań; już z tego powodu podzbiory algebraiczne są stosunkowo regularne. Bardziej specjalne własności danego zbioru algebraicznego wynikają ze specjalnych własności układu równań, które ten zbiór definiują, choć z reguły nie można liczyć na łatwe i bezpośrednie odczytywanie tych własności z postaci równań. Wiąże się to między innymi z faktem, że o ile układ równań wyznacza jednoznacznie swego geometrycznego partnera, jakim jest zbiór rozwiązań, to dla danego zbioru algebraicznego istnieje wiele układów równań, które ten zbiór określają. Postaramy się najpierw usunąć tę dowolność.

W tym celu zastanówmy się na wstępie nad tym, jakie zmiany układu równań nie zmieniają jego zbioru rozwiązań. Oczywiście uzupełnienie układu równań wyznaczającego zbiór algebraiczny V kolejnym równaniem postaci $f = 0$, gdzie f jest dowolnym wielomianem równym zero we wszystkich punktach zbioru V, nie zmienia zbioru rozwiązań. Prowadzi to do konkluzji, że z danym zbiorem algebraicznym V należy wiązać zbiór złożony z *wszystkich* wielomianów, które są równe zero na zbiorze V. Ten zbiór wielomianów jest ideałem i jest on już jednoznacznie wyznaczony przez dany zbiór algebraiczny. Ideał ten oznaczamy przez $\mathbf{I}(V)$.

Zauważmy, że jeśli $g^s \in \mathbf{I}(V)$ dla pewnej liczby naturalnej s, to $g \in \mathbf{I}(V)$. Ideały mające tę własność nazywamy *radykalnymi.*

Warto tu zaznaczyć, że dla dowolnego ideału I dowolnego pierścienia R (w tej książce rozważamy tylko pierścienie przemienne z 1) zbiór wszystkich takich elementów z R, których pewna potęga należy do I, jest ideałem. Ideał ten nazywamy *radykałem* ideału I. Łatwo wykazać, że radykał ideału jest już ideałem radykalnym.

Każdemu zbiorowi algebraicznemu V możemy zatem przyporządkować ideał radykalny $\mathbf{I}(V)$ w pierścieniu wielomianów $K[x_1, \ldots, x_n]$ oraz pierścień ilorazowy $K[x_1, \ldots, x_n]/\mathbf{I}(V)$, oznaczany przez $K[V]$. (Pierścień $K[V]$ będzie zdefiniowany jeszcze raz w §1.6, ale tam posłużymy się nieco inną, wygodniejszą dla dalszych rozważań, ale równoważną definicją.)

Jeśli zbiór V jest opisany przez układ równań

$$f_1 = 0, \ \ldots, \ f_r = 0,$$

to funkcje gf_i, $f_i + f_j$ (gdzie $g \in K[x_1, \ldots, x_n]$, $i, j = 1, \ldots, r$) lub ogólniej wszystkie funkcje postaci $g_1 f_1 + \cdots + g_r f_r$ dla $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ są równe zero na całym zbiorze V, a zatem należą do $\mathbf{I}(V)$. Inaczej mówiąc, $\mathbf{I}(V)$ zawiera ideał $(f_1, \ldots, f_r)$ generowany przez $f_1, \ldots, f_r$, a zatem również radykał tego ideału. Nasuwa się pytanie, czy jest temu radykałowi równy. Pozytywne odpowiedzi na to pytanie i na pytania pokrewne są wnioskami z twierdzeń Hilberta, podanych w następnych dwóch paragrafach.

1.2. Twierdzenie Hilberta o bazie

Twierdzenie 1.2.1 (Hilberta o bazie). *Każdy ideał pierścienia $K[x_1, \dots, x_n]$ ma skończony układ generatorów.*

W twierdzeniu tym ciało współczynników K może być dowolne (niekoniecznie algebraicznie domknięte).

Twierdzenie o bazie ma też inne, często użyteczne, równoważne sformułowania dotyczące rodzin ideałów w $K[x_1, \dots, x_n]$:

A. *Każda niepusta rodzina ideałów ma element maksymalny.*

B. *Każdy nieskończony rosnący ciąg ideałów stabilizuje się.*

Pierścienie, w których każdy ideał jest skończenie generowany, nazywamy *noetherowskimi.* Twierdzenia A oraz B są prawdziwe w każdym pierścieniu noetherowskim, i tylko w takich pierścieniach. Dowód tego stwierdzenia jest prosty ([7, tw. 2.6, rozdz. III] lub [1, stw. 6.1 i 6.2]) i pozostawiamy go Czytelnikowi jako ćwiczenie.

Pierścieniami noetherowskimi są wszystkie ciała. Twierdzenie o bazie wynika zatem przez indukcję z następującego rezultatu, który też można nazywać „twierdzeniem o bazie”:

Twierdzenie 1.2.2. *Jeśli pierścień R jest noetherowski, to pierścień $R[x]$ jest też noetherowski.*

Dowód. Załóżmy, że R jest pierścieniem noetherowskim oraz I jest ideałem pierścienia $R[x]$. Zbiór wszystkich współczynników przy najwyższych potęgach zmiennej x w wielomianach należących do I tworzy ideał w R. Oznaczmy go przez $\mathbf{N}(I)$.

Ponieważ pierścień R jest noetherowski, zatem $\mathbf{N}(I) = (a_1, \dots, a_s)$ dla pewnych $a_1, \dots, a_s \in R$. Niech wielomiany $f_1, \dots, f_s \in I$ mają przy najwyższych potęgach zmiennej x współczynniki $a_1, \dots, a_s$. Możemy założyć, że mają one taki sam stopień m. Wtedy dla każdego $h \in I$ możemy znaleźć takie wielomiany $g_1, \dots, g_s \in R[x]$, że wielomian $h - \sum g_i f_i$ ma stopień mniejszy od m. Wielomiany stopnia mniejszego od m należące do I tworzą R-podmoduł w skończenie generowanym R-module wszystkich wielomianów stopnia mniejszego od m. Ponieważ R jest pierścieniem noetherowskim, podmoduł ten jest też skończenie generowany (zob. lemat niżej). Jego generatory razem z $f_1, \dots, f_s$ tworzą układ generatorów ideału I, co kończy dowód.

Skorzystaliśmy z ważnego i użytecznego lematu ([7, tw. 8.3, rozdz. VI]):

Lemat. *Każdy podmoduł skończenie generowanego modułu nad pierścieniem noetherowskim jest skończenie generowany.*

1.3. Twierdzenie Hilberta o zerach

1.3.1. Sformułowania twierdzenia Hilberta o zerach

Twierdzenie 1.3.1 (Hilberta o zerach)**.** *Niech $V \subset K^n$ będzie zbiorem algebraicznym opisanym przez układ równań $f_1 = 0, \dots, f_r = 0$. Wtedy radykał ideału $(f_1, \dots, f_r)$ jest równy $\mathbf{I}(V)$.*

Twierdzenie to jest prawdziwe tylko dla ciał algebraicznie domkniętych.

Twierdzenie o zerach ma też wiele równoważnych sformułowań. Będziemy korzystać z następujących:

A. *Niech zbiór $V \subset K^n$ będzie określony przez układ równań $f_1 = 0, \dots, f_r = 0$. Jeśli $g \in K[x_1, \dots, x_n]$, to $g \in \mathbf{I}(V)$ wtedy i tylko wtedy, gdy pewna potęga wielomianu g należy do ideału $(f_1, \dots, f_r)$.*

B. *Każdy niesprzeczny układ równań $f_1 = 0, \dots, f_r = 0$ ma rozwiązanie w K^n.*

C. *Dla każdej skończenie generowanej K-algebry istnieje K-homomorfizm tej algebry na ciało K.*

D. *Niech $I \subset K[V]$ będzie ideałem. Część wspólna wszystkich takich ideałów maksymalnych $\mathbf{m}$ w $K[V]$, że $\mathbf{m} \supset I$ oraz $K[V]/\mathbf{m} = K$, jest równa radykałowi ideału I.*

Przypomnijmy, że układ równań $f_1 = 0, \dots, f_r = 0$ nazywamy *sprzecznym*, gdy wynika z niego sprzeczność $1 = 0$, tzn. gdy istnieją takie wielomiany $g_1, \dots, g_r$, że $g_1 f_1 + \cdots + g_r f_r = 1$, a zatem gdy mnożąc równania tego układu kolejno przez $g_1, \dots, g_r$ i dodając wyniki stronami, otrzymamy $1 = 0$.

Wyżej użyliśmy pojęcia K-algebry oraz K-homomorfizmu. Przypomnijmy, że *K-algebra* to pierścień R z ustalonym zanurzeniem (zachowującym element neutralny 1) $K \subset R$, natomiast *K-homomorfizm* K-algebr to homomorfizm pierścieni, który jest identycznością na wyróżnionych podpierścieniach K.

Równoważność powyższych sformułowań twierdzenia o zerach jest łatwa do wykazania. Pewnym wyjątkiem jest wynikanie wersji A z wersji B. Tu stosuje się następujący „trik Rabinowitscha”. Załóżmy, że prawdziwe jest stwierdzenie B i zachodzą założenia wersji A. Do naszego zestawu zmiennych $x_1, \dots, x_n$ dodajmy dodatkową zmienną y i rozpatrzmy układ równań

$$f_1 = 0, \ \dots, \ f_r = 0, \quad 1 - yg = 0.$$

Układ ten nie ma rozwiązań, bo jeśli $x_1 = a_1, \dots, x_n = a_n$, $y = b$ jest rozwiązaniem, to z założeń wersji A wynika, że $g(a_1, \dots, a_n) = 0$. Stąd $1 = 1 - bg(a_1, \dots, a_n) = 0$, a zatem $1 = 0$ i otrzymaliśmy sprzeczność (w ciele K

mamy $1 \neq 0$). Z B wynika więc, że układ ten jest sprzeczny, a zatem istnieją takie wielomiany $g_1, \dots, g_r, g_{r+1} \in K[x_1, \dots, x_n, y]$, że

$$g_1 f_1 + \cdots + g_r f_r + g_{r+1}(1 - yg) = 1.$$

Podstawmy w tej równości $1/g$ w miejsce y i pomnóżmy rezultat przez tak dużą potęgę wielomianu g, by pozbyć się mianowników. Otrzymamy równość postaci

$$(g^s g_1')f_1 + \cdots + (g^s g_r')f_r + (g^s g_{r+1}')(1 - 1) = g^s,$$

gdzie g_i' oznacza funkcję powstałą przez wstawienie do g_i ilorazu $1/g$ w miejsce zmiennej y. Ponieważ wiemy, że $g^s g_i' \in K[x_1, \dots, x_n]$, wynika stąd, że g^s należy do ideału $(f_1, \dots, f_r)$, co należało udowodnić.

Dowód twierdzenia o zerach szkicujemy poniżej.

1.3.2. Elementy i rozszerzenia całkowite

Zacznijmy od wprowadzenia pojęcia rozszerzenia całkowitego ([7, rozdz. VII]), które, niezależnie od zastosowań do dowodu twierdzenia o zerach, ma ogromne znaczenie w teorii liczb i w geometrii algebraicznej.

Niech P będzie pierścieniem, a R jego podpierścieniem. Mówimy, że element $a \in P$ jest *całkowity nad* R, gdy a jest pierwiastkiem pewnego wielomianu unormowanego $f \in R[x]$.

Zbiór wszystkich elementów całkowitych nad R w pierścieniu P tworzy podpierścień, zwany *domknięciem całkowitym* podpierścienia R w P. Pierścień P nazywamy *rozszerzeniem całkowitym* pierścienia R, gdy każdy element pierścienia P jest całkowity nad R.

Pierścień P bez dzielników zera nazywamy *całkowicie domkniętym* (lub *normalnym*), gdy pokrywa się ze swym domknięciem całkowitym w ciele ułamków $Q(P)$ pierścienia P.

W dalszym ciągu tego wykładu potrzebne nam będą następujące dwa rezultaty:

Lemat 1.3.1 (o podnoszeniu ideałów; [7, tw. 3.1, str. 262])**.** *Niech P będzie rozszerzeniem całkowitym pierścienia R i niech I będzie ideałem pierwszym w R. Wówczas istnieje taki ideał pierwszy I_1 w P, którego przecięcie z R jest równe I. Ideał I_1 jest maksymalny wtedy i tylko wtedy, gdy ideał I jest maksymalny.*

Lemat 1.3.2 (Noether o normalizacji)**.** *Niech $K[a_1, \dots, a_n]$ będzie skończenie generowaną algebrą bez dzielników zera. Algebra ta ma podalgebrę $K[b_1, \dots, b_s]$, izomorficzną z algebrą wielomianów s zmiennych, o tej własności, że rozszerzenie*

$$K[a_1, \dots, a_n] \supset K[b_1, \dots, b_s]$$

jest całkowite, a rozszerzenie ciał ułamków

$$K(a_1, \ldots, a_n) \supset K(b_1, \ldots, b_s)$$

jest rozdzielcze.

Dowód lematu (w nieco ogólniejszej wersji) można znaleźć w [46, Theorem 8, Ch. V, str. 266–267], a dowód pierwszej części – w [7, tw. 2.1, str. 260].

Następny lemat dotyczący rozszerzeń całkowitych nie będzie nam potrzebny w tym paragrafie, ale będzie wykorzystywany w dalszych częściach książki.

Lemat 1.3.3. *Niech R będzie całkowicie domkniętym pierścieniem noetherowskim. Niech $L \supset Q(R)$ będzie skończonym rozszerzeniem rozdzielczym ciała ułamków pierścienia R. Wtedy domknięcie całkowite pierścienia R w L jest R-modułem skończenie generowanym.*

Dowód tego rezultatu można znaleźć na przykład w [7, str. 257].

1.3.3. Dowody twierdzenia Hilberta o zerach

Będziemy dowodzić wersji C. Niech $\phi : K[b_1, \ldots, b_s] \to K$ będzie dowolnym K-homomorfizmem, gdzie $K[b_1, \ldots, b_s] \subset K[a_1, \ldots, a_n]$ jak w lemacie o normalizacji. Niech $I \subset K[b_1, \ldots, b_s]$ będzie jądrem tego homomorfizmu i niech $I_1 \subset K[a_1, \ldots, a_n]$ będzie jak w lemacie o podnoszeniu ideałów. Wobec tego I oraz I_1 są ideałami maksymalnymi. Rozważmy

$$K[a_1, \ldots, a_n] \to K[a_1, \ldots, a_n]/I_1.$$

Wystarczy udowodnić, że $K[a_1, \ldots, a_n]/I_1 = K$ – ale to jest oczywiste, bo ten iloraz jest ciałem, którego każdy element jest algebraiczny nad K.

Inny dowód twierdzenia Hilberta o zerach można znaleźć w [1], jeszcze inny dowód zostanie podany w §1.12. A jeszcze inny (należący do N. Bourbakiego), i to twierdzenia ogólniejszego, opisany jest w zadaniach na końcu tego rozdziału.

1.4. Ideał podzbioru afinicznego

Jako łatwy wniosek z twierdzenia o bazie i twierdzenia o zerach otrzymujemy wzajemnie jednoznaczną odpowiedniość między podzbiorami algebraicznymi w K^n a ideałami radykalnymi w $K[x_1, \ldots, x_n]$. Dokładniej:

Każdemu podzbiorowi (algebraicznemu) $V \subset K^n$ odpowiada ideał radykalny $\mathbf{I}(V)$ złożony z tych wszystkich wielomianów $f \in K[x_1,\dots,x_r]$, które są równe zero na V. Każdemu ideałowi (radykalnemu) I odpowiada podzbiór algebraiczny $\mathbf{V}(I)$ złożony z tych punktów $(a_1,\dots,a_n) \in K^n$, dla których $f(a_1,\dots,a_n) = 0$ dla każdego $f \in I$. Podzbiór ten jest opisany przez układ

$$f_1 = 0,\ \dots,\ f_r = 0,$$

gdzie $f_1,\dots,f_r$ tworzą układ generatorów ideału I.

Zdefiniowane tak przyporządkowania są dobrze określone, odpowiednio, dla dowolnych ideałów i podzbiorów, a na ideałach radykalnych i zbiorach algebraicznych opisują przekształcenia wzajemnie odwrotne.

Przekształcenia te mają szereg łatwych do udowodnienia własności:

1. $\mathbf{V}(I_1 I_2) = \mathbf{V}(I_1) \cup \mathbf{V}(I_2)$.
2. $\mathbf{V}(\bigcup I_l) = \bigcap \mathbf{V}(I_l)$.
3. $I_1 \subset I_2 \Rightarrow \mathbf{V}(I_1) \supset \mathbf{V}(I_2)$.
4. $V_1 \subset V_2 \Rightarrow \mathbf{I}(V_1) \supset \mathbf{I}(V_2)$.
5. $\mathbf{V}(I_1 + I_2) = \mathbf{V}(I_1) \cap \mathbf{V}(I_2)$.
6. $\mathbf{V}(I_1 \cap I_2) = \mathbf{V}(I_1 I_2) = \mathbf{V}(I_1) \cup \mathbf{V}(I_2)$.
7. $\mathbf{V}(\mathbf{I}(\mathbf{V}(J))) = \mathbf{V}(J)$ dla każdego ideału J.
8. $\mathbf{I}(\mathbf{V}(\mathbf{I}(W))) = \mathbf{I}(W)$ dla każdego podzbioru W.

Wyżej związaliśmy z każdym zbiorem algebraicznym V ideał $\mathbf{I}(V)$. Na dalszych stronach tej książki będziemy badać, w jaki sposób własności ideału $\mathbf{I}(V)$ związane są z geometrycznymi własnościami zbioru V. Warto sobie jednak zdawać sprawę z tego, że odczytywanie własności tego ideału z własności układów równań określających zbiór V jest na ogół bardzo złożone obliczeniowo. Wiemy co prawda, że jeśli zbiór V jest opisany przez układ równań

$$f_1 = 0, \dots,\ f_r = 0,$$

to $\mathbf{I}(V)$ jest radykałem ideału $(f_1,\dots,f_r)$, ale już samo sprawdzenie przynależności do tego radykału nie daje się opisać przez efektywny (tzn. wymagający wielomianowego czasu) algorytm ([22, 5.4]). Oczywiście zdarzają się łatwe przypadki.

Jest tak na przykład wtedy, gdy dla ideału $I \subset K[x_1,\dots,x_n]$ ideał $\mathbf{M}(I)$ generowany przez najwyższe (ze względu na jakieś, na przykład leksykograficzne, uporządkowanie) jednomiany występujące w wielomianach należących do I, jest generowany przez najwyższe jednomiany występujące w danym układzie generatorów tego ideału. Taki układ generatorów ideału nazywamy jego *bazą Gröbnera.* Okazuje się, że jeśli dana jest baza Gröbnera ideału, to problem przynależności wielomianu do tego ideału jest już algorytmicznie łatwy (opiera się na „dzieleniu z resztą” przez wielomiany wchodzące w skład bazy). Istnieje też koncepcyjnie prosty, ale wymagający czasu potęgowego, algorytm (Buchbergera) znajdowania bazy Gröbnera, gdy dana jest baza dowolna (zob. na przykład [5]).

Wobec tego odwołując się w przyszłości do własności ideałów $\mathbf{I}(V)$, powinniśmy sobie zdawać sprawę z tego, że efektywne odczytanie tych własności z postaci równań określających zbiór V jest na ogól trudne. Z tym większym zainteresowaniem możemy odnotowywać te wyjątkowe przypadki, w których udaje się tego dokonać.

Na dalszych stronach tej książki nie będziemy się zajmować problemami obliczeniowymi związanymi z tematami, o których tu mowa, chociaż stanowią one interesujący kierunek badań.

Jeszcze tylko jedna uwaga. Numeryczne znajdywanie szczególnych rozwiązań układów równań wielomianowych jest zadaniem stosunkowo prostym. W związku z tym można łatwo naszkicować fragmenty zbioru rozwiązań (zapewnia to na przykład program *Mathematica*) i wywnioskować na tej podstawie, jakie są przypuszczalne i przybliżone jego własności. Natomiast trudne jest na ogół, na podstawie równań, opisanie nie przypuszczalnych, ale niewątpliwych własności całego zbioru.

1.5. Topologia Zariskiego

Z podanych w poprzednim paragrafie równości 1 i 2 wynika, że suma dwóch, a zatem i dowolnej skończonej liczby zbiorów algebraicznych oraz iloczyn dowolnej liczby takich zbiorów są też zbiorami algebraicznymi. Ponieważ zbiór pusty i cała przestrzeń K^n są podzbiorami algebraicznymi, możemy przyjąć rodzinę zbiorów algebraicznych jako rodzinę wszystkich podzbiorów domkniętych pewnej topologii na K^n. Topologia ta nosi nazwę *topologii Zariskiego*.

Warto zauważyć, że z wyjątkiem trywialnego przypadku $n = 0$ nie jest to topologia Hausdorffa, a topologia na $K^n = K^{n-s} \times K^s$, gdzie s jest dowolną liczbą naturalną mniejszą od n, nie jest topologią produktową (Tichonowa).

W rzeczywistości topologie na K^s, gdzie s jest liczbą naturalną mniejszą od n, oraz na K^{n-s}, nie wyznaczają jeszcze topologii na K^n, a wobec tego topologia na K^n wnosi nowe (w porównaniu z K^s, $s < n$) informacje dotyczące własności ciała K.

W tym kontekście interesujące jest twierdzenie Hrushovskiego–Zilbera ([15]), które głosi, że ciało K jest jednoznacznie wyznaczone przez nieskończony ciąg przestrzeni topologicznych $K^1, K^2, K^3, \ldots$ (oraz ich naturalnych przekształceń rzutowania, zanurzeń i przekształceń diagonalnych).

Topologia Zariskiego na K^n wyznacza topologię indukowaną na każdym podzbiorze $V \subset K^n$. Tę topologię będziemy nazywać *topologią Zariskiego na* V.

Jeśli $V \subset K^n$ jest afinicznym zbiorem algebraicznym, a $f \in K[x_1, \dots, x_n]$, $f \neq 0$, to zbiór

$$V_f := \{a \in V;\ f(a) \neq 0\}$$

jest podzbiorem otwartym (jako dopełnienie zbioru domkniętego $\{a \in V;\ f(a) = 0\}$).

Okazuje się, że każdy podzbiór otwarty $U \subset V$ jest sumą zbiorów postaci V_f, a zatem zbiory tej postaci stanowią bazę topologii Zariskiego.

Istotnie, ponieważ zbiór $U \subset V$ jest otwarty, jego dopełnienie $V \setminus U$ jest podzbiorem domkniętym w V, a więc w K^n. Istnieje zatem taki układ równań wielomianowych $f_1 = 0, \dots, f_r = 0$, który go opisuje. Wobec tego punkt $a \in V \subset K^n$ nie należy do $V \setminus U$, a zatem należy do U, wtedy i tylko wtedy, gdy nie spełnia któregoś równania $f_i = 0$, a więc gdy należy do pewnego zbioru V_{f_i}. Stąd $U = V_{f_1} \cup \dots \cup V_{f_r}$, co należało wykazać.

Ponieważ każdy wstępujący nieskończony ciąg ideałów w $K[x_1, \dots, x_n]$ jest od pewnego miejsca stały, zatem każdy nieskończony zstępujący ciąg podzbiorów algebraicznych zawartych w K^n jest od pewnego miejsca stały. Wobec tego dla dowolnego zbioru algebraicznego $V \subset K^n$, w przestrzeni topologicznej V, *każdy zstępujący ciąg podzbiorów domkniętych jest od pewnego miejsca stały*. Przestrzenie topologiczne o tej własności nazywamy *przestrzeniami noetherowskimi.*

Zanotujmy tu jeszcze, że:

— *Podzbiory otwarte afinicznych zbiorów algebraicznych są quasi-zwarte,*

tzn. z każdego pokrycia podzbioru otwartego zbioru afinicznego podzbiorami otwartymi można wybrać pokrycie skończone. Aby się o tym przekonać, wystarczy udowodnić rezultat dualny:

— *Jeśli część wspólna pewnej rodziny zbiorów domkniętych jest równa W, to istnieje taka skończona podrodzina tej rodziny, której część wspólna jest też równa W.*

Wynika to z faktu, że zstępujący ciąg zbiorów domkniętych jest od pewnego miejsca stały.

W przypadku $K = \mathbb{C}$ w przestrzeni $\mathbb{C}^n$ mamy jeszcze inną znaną nam dobrze topologię, zwaną *topologią naturalną. Każdy zbiór domknięty w topologii Zariskiego w $\mathbb{C}^n$ jest domknięty w topologii naturalnej, ale nie na odwrót* (gdy $n > 0$).

Mogłoby się wydawać, że topologia Zariskiego jest tak uboga, że nie może być używana do odczytywania głębszych geometrycznych własności zespolonych zbiorów algebraicznych, wyposażonych w bogatszą topologię naturalną, indukowaną przez naturalną topologię w $\mathbb{C}^n$. Mniemanie to nie jest jednak uzasadnione: okazuje się, że do badania pewnych własności geometrycznych podzbiorów w $\mathbb{C}^n$ wystarcza znajomość zbiorów otwartych w topologii Zariskiego. Badania takie można przy tym przenieść na zbiory algebraiczne nad dowolnym ciałem. Wprowadzenie topologii Zariskiego nie tylko umożliwia korzystanie z języka topologii, ale pozwala na rozpatrywanie zbioru algebraicznego jako ciekawego obiektu topologicznego.

1.6. Pierścień funkcji regularnych i jego spektrum

Każdemu wielomianowi $f \in K[x_1, \dots, x_n]$ odpowiada funkcja $K^n \to K$. Tak otrzymane funkcje nazywamy *funkcjami wielomianowymi* lub *regularnymi* na K^n.

Niech $V \subset K^n$ będzie podzbiorem algebraicznym. Każdą funkcję regularną na K^n można ograniczyć do V. Tak otrzymane funkcje $V \to K$ nazywamy *funkcjami regularnymi* na V. Funkcjami regularnymi są na przykład funkcje stałe o wartościach w K. W zbiorze wszystkich funkcji regularnych na V wprowadza się naturalne działania dodawania i mnożenia,

$$(f + g)(v) = f(v) + g(v), \quad (f \cdot g)(v) = f(v) \cdot g(v),$$

w tym mnożenia przez funkcje stałe o wartościach w K,

$$(af)(v) = af(v),$$

dla $v \in V$. W ten sposób funkcje regularne na V tworzą K-algebrę. Oznaczamy ją przez $K[V]$.

Przyporządkowując każdej funkcji $f \in K[x_1, \dots, x_n]$ jej obcięcie do V, otrzymujemy homomorfizm

$$K[x_1, \dots, x_n] \to K[V]$$

o jądrze $\mathbf{I}(V)$. Wobec tego

$$K[V] \simeq K[x_1, \dots, x_n]/\mathbf{I}(V).$$

Z tych definicji wynika, że:

- *Algebra $K[V]$ jest skończenie generowana i nie ma elementów nilpotentnych* (gdyż ideał $\mathbf{I}(V)$ jest radykalny) oraz że:

— *Każda skończenie generowana K-algebra bez elementów nilpotentnych może występować w tej roli.*

To ostatnie stwierdzenie jest wnioskiem z twierdzenia Hilberta o zerach.

$K[V \times W]$ jest iloczynem tensorowym $K[V] \otimes_K K[W]$ (co można przyjąć za definicję iloczynu tensorowego K-algebr $K[V]$ oraz $K[W]$) ([7, str. 240–241]).

Funkcje współrzędnych $x_1, \dots, x_n$ (po ograniczeniu do V) są generatorami K-algebry $K[V]$. Podzbiór $V \subset K^n$ jest wyznaczony przez $K[V]$ i ten wybór generatorów. Dokładniej, punkty zbioru V można utożsamiać z K-homomorfizmami $K[V] \to K$, gdyż z jednej strony każdy punkt $a \in V$ wyznacza homomorfizm ewaluacji ϕ_a, określony przez $\phi_a(f) = f(a)$; z drugiej strony każdy K-homomorfizm $\varphi : K[V] \to K$ wyznacza punkt

$$a = (\varphi(x_1), \dots, \varphi(x_n)) \in V.$$

Warto tu jeszcze dodać, że każdy K-homomorfizm $K[V] \to K$ jest jednoznacznie wyznaczony przez swe jądro – ideał maksymalny w $K[V]$. A ponieważ z twierdzenia Hilberta o zerach wynika, że każdy ideał maksymalny w $K[V]$ jest jądrem pewnego K-homomorfizmu $K[V] \to K$, zatem:

— *Punkty zbioru algebraicznego V można identyfikować z K-homomorfizmami $K[V] \to K$ oraz z ideałami maksymalnymi w $K[V]$.*

Oznaczmy przez $\mathrm{Spec_m}(K[V])$ zbiór wszystkich ideałów maksymalnych w $K[V]$. Zbiór ten nazywamy *spektrum maksymalnym* pierścienia $K[V]$. Z powyższego wynika, że możemy napisać $V = \mathrm{Spec_m}(K[V])$. Nadaje to zbiorowi V samoistny byt, niezależny od zanurzenia w K^n.

Zanurzenie $V \subset K^n$ jest określone przez wybór n generatorów K-algebry $K[V]$. Inny wybór daje inne zanurzenie V w przestrzeń afiniczną. Zbiór V możemy wobec tego realizować jako różne podzbiory algebraiczne w przestrzeniach afinicznych.

Tę myśl będziemy kontynuować na następnych wykładach. Na razie tylko zauważmy, że identyfikując zbiór V z $\mathrm{Spec_m}(K[V])$, możemy wprowadzić w zbiorze $\mathrm{Spec_m}(K[V])$ topologię Zariskiego; możemy ją też określić bezpośrednio, przyjmując, że domknięciem podzbioru $A \subset \mathrm{Spec_m}(K[V])$ jest zbiór wszystkich ideałów maksymalnych w $K[V]$ zawierających $\bigcap_{\mathbf{m} \in A} \mathbf{m}$.

Pójdźmy jeszcze o krok dalej i dla dowolnego pierścienia R rozważmy zbiór $\mathrm{Spec}(R)$ złożony z wszystkich ideałów pierwszych pierścienia R. Zbiór ten nazywamy *spektrum* pierścienia R.

Można w nim określić topologię (zwaną też *topologią Zariskiego*), przyjmując, że domknięciem podzbioru $A \subset \mathrm{Spec}(R)$ jest zbiór wszystkich ideałów pierwszych w R zawierających $\bigcap_{\mathbf{p}\in A}\mathbf{p}$. *Bazą zbiorów otwartych dla tej topologii jest rodzina wszystkich zbiorów postaci*

$$\operatorname{Spec}(R)_f = \{\mathbf{p} \in \operatorname{Spec}(R);\ f \notin \mathbf{p}\}.$$

Przyporządkujmy każdemu podzbiorowi domkniętemu $V \subset \operatorname{Spec}(R)$ ideał $\mathbf{I}(V)$ określony jako przecięcie $\bigcap_{\mathbf{p}\in V}\mathbf{p}$. Wówczas $\mathbf{I}(V)$ *jest ideałem radykalnym i na tej drodze uzyskujemy wzajemnie jednoznaczną odpowiedniość między ideałami radykalnymi w R oraz podzbiorami domkniętymi w* $\operatorname{Spec}(R)$.

Dowód tego rezultatu przypominającego twierdzenie Hilberta o zerach jest jednak znacznie łatwiejszy od dowodu jego pierwowzoru, bo wynika wprost z następującego prostego twierdzenia:

— *Każdy ideał radykalny jest częścią wspólną wszystkich ideałów pierwszych, które go zawierają* [1, stw. 1.14].

Przypomnijmy natomiast, iż twierdzenie Hilberta mówi, że jeśli ciało K jest algebraicznie domknięte, to każdy ideał radykalny w skończenie generowanej algebrze $K[a_1,\dots,a_n]$ jest częścią wspólną takich ideałów maksymalnych $\mathbf{m} \subset K[a_1,\dots,a_n]$, że $K[a_1,\dots,a_n]/\mathbf{m} = K$.

Jeśli R jest pierścieniem noetherowskim, to zbiór $\operatorname{Spec}(R)$ z topologią Zariskiego jest przestrzenią noetherowską.

Dla $R = K[V]$ *zbiór* $\operatorname{Spec}_{\mathrm{m}}(K[V])$ *jest podprzestrzenią gęstą w* $\operatorname{Spec}(K[V])$, a nawet *zbiór tych punktów z* $\operatorname{Spec}_{\mathrm{m}}(K[V])$, *które należą do ustalonego podzbioru domkniętego w* $\operatorname{Spec}(K[V])$, *jest gęsty w tym podzbiorze.* Wobec tego istnieje naturalna, wzajemnie jednoznaczna i zachowująca inkluzję odpowiedniość między rodzinami zbiorów domkniętych w $\operatorname{Spec}_{\mathrm{m}}(R)$ i $\operatorname{Spec}(R)$. Tak więc przestrzenie topologiczne $\operatorname{Spec}_{\mathrm{m}}(R)$ oraz $\operatorname{Spec}(R)$ różnią się zasobami punktów, a nie własnościami rodziny zbiorów domkniętych. Dowody tych faktów wymagają skorzystania z twierdzenia Hilberta o zerach.

1.7. Zbiory nierozkładalne

Zbiór algebraiczny nazywamy *rozkładalnym*, gdy można go przedstawić jako sumę dwóch podzbiorów algebraicznych, z których każdy jest od niego różny. Zbiór jest *nierozkładalny*, gdy nie daje się tak przedstawić.

Twierdzenie 1.7.1. *Każdy zbiór algebraiczny można przedstawić jako skończoną sumę zbiorów nierozkładalnych. Takie przedstawienie nieskracalne jest tylko jedno.*

Dowód. Rozważmy rodzinę $\mathcal{R}$ wszystkich zbiorów algebraicznych, których *nie można* tak przedstawić. Gdyby rodzina ta nie była pusta, istniałby w niej element minimalny (bo w rodzinie odpowiadających im ideałów radykalnych istniałby element maksymalny, na mocy twierdzenia o bazie). Element ten nie byłby nierozkładalny, bo takie dają się przedstawić jako suma nierozkładalnych; dawałby się więc przedstawić jako suma podzbiorów algebraicznych istotnie mniejszych. Te mniejsze zbiory nie należałyby do $\mathcal{R}$, bo są istotnie mniejsze od minimalnego elementu tej rodziny. Byłyby zatem przedstawialne jako skończone sumy zbiorów nierozkładalnych. Wobec tego i ich sumę można by w tej postaci przedstawić. Otrzymaliśmy sprzeczność z założeniem, że ta suma należy do $\mathcal{R}$. Kończy to dowód pierwszej części twierdzenia.

Dowód, że takie przedstawienie nieskracalne jest tylko jedno ([7, tw. 3.4, rozdz. VIII]), pozostawimy Czytelnikowi jako proste ćwiczenie, wyjaśniając jedynie, że przedstawienie nieskracalne to takie, w którym nie można pominąć żadnego składnika; oznacza to, że żaden składnik nie jest zawarty w sumie pozostałych, a tym bardziej w żadnym z pozostałych składników.

Jeśli $V = V_1 \cup \cdots \cup V_r$ jest nieskracalnym przedstawieniem zbioru V w postaci sumy zbiorów nierozkładalnych, to zbiory V_i, gdzie $i = 1, \ldots, r$, nazywamy *składowymi nierozkładalnymi* zbioru V.

Twierdzenie 1.7.2. *Zbiór algebraiczny V jest nierozkładalny wtedy i tylko wtedy gdy ideał $\mathbf{I}(V)$ jest pierwszy.*

Dowód. Załóżmy, że zbiór V jest rozkładalny, i niech $V = W_1 \cup W_2$ będzie rozkładem na dwa zbiory algebraiczne, z których każdy jest różny od V. Istnieją zatem punkty $a_1 \in W_2 \setminus W_1$ oraz $a_2 \in W_1 \setminus W_2$. Ponieważ $a_1 \notin W_1$, istnieje taki wielomian f_1, który jest równy zero na W_1, ale $f_1(a_1) \neq 0$. Podobnie istnieje wielomian f_2, który jest równy zero na W_2, ale $f_2(a_2) \neq 0$. Wobec tego iloczyn $f_1 f_2$ jest równy zero na $W_1 \cup W_2 = V$, czyli $f_1 f_2 \in \mathbf{I}(V)$, ale żaden z czynników nie jest równy zero na całym zbiorze V, więc żaden nie należy do $\mathbf{I}(V)$. Oznacza to, że ideał $\mathbf{I}(V)$ nie jest pierwszy.

Rozumowanie to można odwrócić, co prowadzi do wniosku, że jeśli ideał $\mathbf{I}(V)$ nie jest pierwszy, to zbiór V jest rozkładalny.

Przecięcie ideałów pierwszych jest zawsze ideałem radykalnym (była już o tym mowa w poprzednim paragrafie). Udowodnimy, że każdy ideał radykalny jest takim przecięciem.

Wniosek 1.7.1. *Każdy ideał radykalny w pierścieniu $K[x_1, \ldots, x_n]$ można przedstawić jako część wspólną ideałów pierwszych. Takie nieskracalne przedstawienie jest tylko jedno.*

Dowód. Dany ideał radykalny I wyznacza zbiór algebraiczny $\mathbf{V}(I)$. Zbiór ten można przedstawić (i to tylko na jeden sposób) jako nieskracalną sumę zbiorów nierozkładalnych

$$\mathbf{V}(I) = V_1 \cup \cdots \cup V_r.$$

Stąd, na mocy własności 1–4 z §1.4, otrzymujemy

$$I = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(V_1) \cap \cdots \cap \mathbf{I}(V_r).$$

Ponieważ na mocy twierdzenia ideały $\mathbf{I}(V_i)$ są pierwsze, udowodniliśmy, że każdy ideał radykalny jest przecięciem skończonej liczby ideałów pierwszych. Jednoznaczność takiego nieskracalnego przedstawienia wynika stąd, że jeśli

$$I = I_1 \cap \cdots \cap I_r$$

jest nieskracalnym przedstawieniem jako przecięcie ideałów pierwszych, to z własności 1–4 wynika, że $\mathbf{V}(I) = \mathbf{V}(I_1) \cup \cdots \cup \mathbf{V}(I_r)$ jest nieskracalnym (a zatem wyznaczonym jednoznacznie) przedstawieniem zbioru $\mathbf{V}(I)$.

Przykłady

1 Jeśli wielomiany $f_1, f_2 \in K[x_1, \ldots, x_n]$ są nierozkładalne, to podzbiory V_1, V_2 określone, odpowiednio, równaniami $f_1 = 0$, $f_2 = 0$ są nierozkładalne, Ponadto $\mathbf{I}(V_1) = (f_1)$ oraz $\mathbf{I}(V_2) = (f_2)$. Równanie $f_1 f_2 = 0$ określa zbiór $V = V_1 \cup V_2$ i jeśli wielomiany f_1 oraz f_2 nie są stowarzyszone, to zbiór V jest rozkładalny oraz $\mathbf{I}(V) = (f_1 f_2)$. Aby to udowodnić, trzeba wykorzystać fakt, że $K[x_1, \ldots, x_n]$ jest pierścieniem z własnością jednoznaczności rozkładu, co wynika z twierdzenia Gaussa ([7, tw. 9.1, str. 151]).

2 Zachowajmy oznaczenia z poprzedniego przykładu. Zbiór $V_1 \cap V_2$ jest określony układem równań $f_1 = 0$, $f_2 = 0$. Wobec tego $\mathbf{I}(V_1 \cap V_2)$ jest radykałem ideału (f_1, f_2) i na ogół jest od niego istotnie większy. Jako przykład, dla $n = 2$, można wziąć $f_1 = x_1^5 - x_2$, $f_2 = x_2$. Wtedy radykał ideału $(x_1^5 - x_2, x_2)$ jest równy (x_1, x_2), ale $x_1 \notin (x_1^5 - x_2, x_2)$.

3 Zbiór V określony w k^3 równaniem

$$x_1^3 + x_1^2 x_2^3 + x_1^2 x_3^4 = 0$$

jest rozkładalny. Jest on sumą dwóch podzbiorów nierozkładalnych określonych równaniami $x_1 = 0$ oraz $x_1 + x_2^3 + x_3^4 = 0$.

Korzystając z topologii Zariskiego, definicję zbioru nierozkładalnego można sformułować w języku topologicznym:

— *Zbiór domknięty nazywamy nierozkładalnym, gdy nie jest sumą dwóch swoich właściwych* (*tzn. różnych od całego zbioru*) *podzbiorów domkniętych.*

Wówczas *sformułowanie i dowód twierdzenia o rozkładzie zbioru domkniętego na sumę zbiorów nierozkładalnych można uogólnić na dowolne przestrzenie noetherowskie.*

Często będziemy korzystać z następującego, łatwego do udowodnienia rezultatu, wypowiedzianego już w tym topologicznym języku:

Następujące warunki nakładane na dany zbiór domknięty Y są równoważne:

1. *zbiór Y jest nierozkładalny,*
2. *każdy niepusty podzbiór otwarty $U \subset Y$ jest gęsty w Y,*
3. *przecięcie $U_1 \cap U_2$ dowolnych dwóch niepustych podzbiorów otwartych $U_1, U_2 \subset Y$ jest niepuste,*
4. *jeśli $U \subset Y$ jest niepustym podzbiorem otwartym, a $W \subset Y$ podzbiorem domkniętym różnym od V, to różnica $U \setminus W$ jest niepusta,*
5. *zbiór Y zawiera podzbiór gęsty* (*który jako przestrzeń topologiczna jest*) *nierozkładalny.*

Czasami zamiast mówić, że zbiór jest nierozkładalny, mówimy, że jest on *nieprzywiedlny* lub *nieredukowalny*, lub że jest *rozmaitością algebraiczną.*

Jeśli R jest pierścieniem noetherowskim, to przestrzeń $\operatorname{Spec}(R)$ jest noetherowska; otrzymujemy zatem następujące twierdzenie:

Twierdzenie 1.7.3. *Niech R będzie pierścieniem noetherowskim.*

(A) *Każdy zbiór domknięty w* $\operatorname{Spec}(R)$ *można jednoznacznie przedstawić w postaci skończonej sumy domkniętych zbiorów nierozkładalnych.*

(B) *Każdy ideał radykalny w R można jednoznacznie przedstawić jako część wspólną skończonej liczby ideałów pierwszych.*

Twierdzenie o przedstawieniu ideału radykalnego jako części wspólnej ideałów pierwszych jest fragmentem pewnej szerszej teorii, którą niżej przedstawiamy w wielkim skrócie.

Zacznijmy od tego, że gdy rozpatrywany pierścień jest pierścieniem liczb całkowitych, powyższy rezultat o przedstawieniu ideałów radykalnych odpowiada twierdzeniu o rozkładzie liczb całkowitych bezkwadratowych na iloczyn liczb pierwszych. By to zauważyć, należy zastąpić liczby całkowite przez generowane przez nie ideały.

Idąc dalej tym tropem, dostrzegamy, że twierdzeniu o rozkładzie dowolnych liczb całkowitych na iloczyn potęg różnych liczb pierwszych odpowiada twierdzenie o przedstawieniu dowolnego ideału w $\mathbb{Z}$ jako przecięcia potęg ideałów pierwszych.

To zastąpienie w rozumowaniach elementów (liczb całkowitych) przez generowane przez nie ideały i formułowanie twierdzeń w języku ideałów okazało się bardzo istotne do uogólnienia teorii rozkładu w pierścieniu $\mathbb{Z}$ na dowolne pierścienie noetherowskie.

Uogólnienie takie nosi nazwę *teorii Laskera–Noether* ([2, rozdz. II, §3, str. 54–64] lub [1, rozdz. IV i VII]).

Zakładamy, że rozpatrywane niżej pierścienie R są noetherowskie. Na wstępie tej teorii dowodzi się, że te ideały $I \subset R$, które są nierozkładalne, tzn. których nie można przedstawić jako przecięcie ideałów istotnie większych, spełniają następujący warunek:

— *Jeśli $x, y \in R$ oraz $xy \in I$ i $x \notin I$, to $y^m \in I$ dla pewnej liczby naturalnej m.*

Ideały takie nazywamy *prymarnymi. Radykał ideału prymarnego jest ideałem pierwszym. Każdy ideał prymarny jest zatem zawarty w pewnym ideale pierwszym i zawiera pewną potęgę tego ideału.* Są to substytuty potęg ideałów pierwszych.

Bez trudu można udowodnić, że każdy ideał jest częścią wspólną skończonego zbioru ideałów nierozkładalnych, a zatem prymarnych. Rozkład taki nazywa się nieskracalnym, gdy nie da się w nim pominąć żadnego czynnika oraz ideały pierwsze związane z tymi czynnikami są różne. Ponieważ *część wspólna ideałów prymarnych o tym samym radykale jest ideałem prymarnym*, łatwo udowodnić, że *każdy ideał ma taki nieskracalny rozkład.*

Główne twierdzenie teorii Laskera–Noether mówi, że radykały czynników prymarnych występujących w nieskracalnym rozkładzie ideału I są przez ten ideał wyznaczone jednoznacznie. Radykały te nazywamy *ideałami stowarzyszonymi* z I; wśród nich wyróżniamy te, które są minimalne, i nazywamy je *izolowanymi*, pozostałe zaś nazywamy *zanurzonymi.*

Każdy ideał minimalny w rodzinie ideałów pierwszych zawierających ideał I jest ideałem izolowanym i odwrotnie. Dowodzi się, że jednoznacznie wyznaczone są też te czynniki prymarne, których radykały są izolowane. Gdy ideał I jest radykalny, wszystkie czynniki prymarne występujące w rozkładzie są izolowanymi ideałami pierwszymi, rozkład jest jednoznaczny i otrzymujemy znany nam już wynik.

Przedstawienia w postaci części wspólnej ideałów prymarnych mają również ideały główne. Czynniki występujące w takim rozkładzie ideału głównego nie muszą już być ideałami głównymi, a zatem nie są wyznaczone przez elementy istniejące już w rozpatrywanym pierścieniu. Inaczej mówiąc, czynniki te istnieją tylko w „świecie idealnym”, i dlatego właśnie nazwano je *ideałami.*

Na ogół ani ideał prymarny nie jest potęgą ideału pierwszego, ani potęga ideału pierwszego nie jest ideałem prymarnym, ale oba te stwierdzenia są prawdziwe, gdy rozpatrywany pierścień jest pierścieniem liczb całkowitych dowolnego skończonego rozszerzenia $L \supset \mathbb{Q}$ ciała liczb wymiernych (tzn. domknięciem całkowitym pierścienia $\mathbb{Z}$ w L). Ma to podstawowe znaczenie w algebraicznej teorii liczb, gdzie teoria rozkładu ideałów miała swe historyczne źródła.

1.8. Funkcje wymierne

Gdy zbiór $V \subset K^n$ jest nierozkładalny, pierścień $K[V]$ nie ma dzielników zera, gdyż ideał $\mathbf{I}(V)$ jest wtedy ideałem pierwszym oraz wiemy, że

$$K[V] \simeq K[x_1, \dots, x_n]/\mathbf{I}(V).$$

Możemy więc utworzyć ciało ułamków pierścienia $K[V]$, które oznaczamy przez $K(V)$ i nazywamy *ciałem funkcji wymiernych* zbioru V; każdy element tego ciała jest *funkcją wymierną* na V.

Nazwanie elementów zbioru $K(V)$ funkcjami bierze się stąd, że:

— *Każdy element $f/g \in K(V)$, gdzie $f, g \in K[V]$, wyznacza funkcję określoną na pewnym niepustym otwartym (a więc gęstym) podzbiorze $U \subset V$ o wartościach w K.*

Funkcja ta jest *określona w punkcie $a \in V$*, gdy istnieje takie przedstawienie elementu f/g w postaci ułamka f_1/g_1, gdzie $f_1, g_1 \in K[V]$, że $g_1(a) \neq 0$. W tej sytuacji *iloraz $f_1(a)/g_1(a)$ nie zależy od wyboru mianownika g_1* i przyjmujemy go jako wartość funkcji f/g w punkcie a. Funkcja ta jest zatem nieokreślona jedynie we wspólnych zerach wszystkich mianowników g_1 ułamków f_1/g_1 równych f/g.

Jeśli mamy jakąkolwiek funkcję $h : U \to K$ powstałą z funkcji wymiernej przez ograniczenie zbioru jej punktów określoności do niepustego zbioru otwartego $U \subset V$, to będziemy ją uważać za reprezentanta tej funkcji wymiernej (lub nawet za tę funkcję). Taka umowa nie prowadzi do sprzeczności, gdyż:

— *Jeśli funkcje wymierne f_1/g_1 oraz f_2/g_2 mają te same wartości na pewnym niepustym podzbiorze otwartym $U \subset V$, to są równe.*

Istotnie, różnica $f_1/g_1 - f_2/g_2 = (f_1g_2 - f_2g_1)/g_1g_2$ jest równa zero na U, a zatem $f_1/g_1 - f_2/g_2$ jest funkcją regularną na V równą zero na niepustym podzbiorze otwartym $U \setminus \{a \in V;\ g_1(a)g_2(a) = 0\}$. Wobec tego *funkcja regularna $f_1g_2 - f_2g_1$ jest równa* 0, czyli $f_1/g_1 = f_2/g_2$. Korzystaliśmy powyżej z ciągłości funkcji regularnych w topologii Zariskiego oraz z własności 2–5 zbiorów nierozkładalnych podanych w §1.4, nie przywołując ich explicite.

Zauważmy, że $K[V] \subset K(V)$ i każda funkcja $f \in K[V]$ jest funkcją wymierną określoną na całym zbiorze V. Jest i na odwrót:

Twierdzenie 1.8.1. *Jeśli funkcja wymierna $f/g \in K(V)$, gdzie $f, g \in K[V]$, jest wszędzie określona, to $f/g = h/1$, gdzie $h \in K[V]$, tj. $f/g \in K[V]$.*

Dowód. Rozważmy zbiór wszystkich mianowników g_1 występujących w przedstawieniach ułamka f/g w postaci f_1/g_1, gdzie $f_1, g_1 \in K[V]$. Trzeba wykazać, że 1 należy do tego zbioru. Dorzućmy do tego zbioru element 0, otrzymując zbiór, który oznaczmy przez J. Wtedy J jest ideałem w $K[V]$. Istotnie, jeśli $g_1 \in J$ i $f_1/g_1 = f/g$, to dla każdego $h \in K[V]$ różnego od zera, $hf_1/hg_1 = f/g$, czyli $hg_1 \in J$. Jeśli $f_1/g_1 = f_2/g_2 = f/g$, to albo $g_1 + g_2 = 0$, albo $(f_1 + f_2)/(g_1 + g_2) = f/g$, a zatem w obu przypadkach $g_1 + g_2 \in J$.

W V nie ma punktu, w którym wszystkie funkcje należące do ideału J są równe zero, bo f/g jest określone na całym V. Z twierdzenia Hilberta o zerach wynika, że $J = K[V]$, a zatem $1 \in J$. Wobec tego 1 jest mianownikiem i dowód jest zakończony.

Pojęcie funkcji wymiernej można bez trudu rozszerzyć na dowolne, niekoniecznie nierozkładalne, zbiory algebraiczne. Jeśli $V = V_1 \cup \cdots \cup V_s$ jest nieskracalnym przedstawieniem zbioru algebraicznego w postaci sumy zbiorów nierozkładalnych, to zamiast ciała ułamków pierścienia funkcji regularnych należy wziąć sumę prostą $\bigoplus_{i=1}^{s} K(V_i)$ ciał funkcji wymiernych dla składowych V_i. Sumę tę oznaczamy przez $K(V)$ i nazywamy K-algebrą funkcji wymiernych na V. Każdy element tej sumy możemy interpretować jako funkcję określoną na pewnym niepustym gęstym podzbiorze otwartym zbioru V.

Uwaga. Można udowodnić, że $K(V)$ jest równe lokalizacji K-algebry $K[V]$ względem systemu multiplikatywnego złożonego z tych wszystkich elementów w $K[V]$, które nie są dzielnikami zera.

Jeśli funkcja wymierna jest określona we wszystkich punktach podzbioru otwartego $U \subset V$, to jej obcięcie do U nazywamy *funkcją regularną* na U.

Następujący przykład pokazuje, że funkcja wymierna na zbiorze rozkładalnym może być regularna na każdej składowej tego zbioru, ale nie być regularna na tym zbiorze.

Przykład. Niech V będzie podzbiorem płaszczyzny opisanym równaniem $x_1x_2 = 0$. Jest to zbiór rozkładalny będący sumą dwóch prostych $x_1 = 0$ oraz $x_2 = 0$. Na zbiorze V możemy rozważyć funkcję, która na jednej z tych prostych (z pominięciem punktu $(0,0)$) jest równa 0, a na drugiej (też z pominięciem $(0,0)$) jest równa 1. Jest to funkcja wymierna, regularna na każdej z tych prostych, ale nieregularna na V, gdyż ma punkt nieokreśloności w $(0,0)$.

Korzystając z faktu, że każda funkcja regularna jest ciągła w topologii Zariskiego, można łatwo udowodnić, że *każda funkcja wymierna jest ciągła na zbiorze punktów, w których jest określona.*

Metoda użyta w dowodzie twierdzenia 1.8.1 pozwala udowodnić następujące jego uogólnienie:

Twierdzenie 1.8.2. *Niech V będzie dowolnym nierozkładalnym zbiorem algebraicznym i niech $f \in K[V] \setminus \{0\}$. Wtedy każdy element należący do*

$$K[V]_f = \{h \in K(V);\ h = g/f^m,\ m \in \mathbb{Z},\ g \in K[V]\}$$

wyznacza pewną funkcję regularną na $V_f = \{x \in V;\ f(x) \neq 0\}$. Na odwrót, *każda funkcja regularna na V_f jest wyznaczona przez pewien element g/f^m algebry $K[V]_f$. Otrzymujemy w ten sposób izomorfizm K-algebry funkcji regularnych na V_f oraz algebry $K[V]_f$.*

Dowód tego rezultatu powierzamy Czytelnikowi jako zadanie.

1.9. Snop funkcji regularnych

Niech V będzie afinicznym zbiorem algebraicznym, a $U \subset V$ jego niepustym podzbiorem otwartym. Oznaczmy przez $\mathcal{O}_V(U)$ zbiór wszystkich funkcji wymiernych określonych we wszystkich punktach zbioru U, czyli regularnych na U. Zbiór ten jest pierścieniem względem zwykłych działań dodawania i mnożenia funkcji o wartościach w K. Ponadto funkcje stałe o wartościach z K należą do $\mathcal{O}_V(U)$, czyli $K \subset \mathcal{O}_V(U)$, i wobec tego $\mathcal{O}_V(U)$ jest K-algebrą. Wygodnie jest dodatkowo przyjąć, że $\mathcal{O}_V(\emptyset)$ jest K-algebrą zerową.

Ponadto, jeśli U_1, U_2 są podzbiorami otwartymi i $U_1 \subset U_2$, to ograniczając funkcje określone na U_2 do U_1, otrzymamy homomorfizm

$$\mathcal{O}_V(U_2) \to \mathcal{O}_V(U_1).$$

Tak określone odwzorowanie $\mathcal{O}_V$, które zbiorom otwartym przyporządkowuje algebry funkcji regularnych, a inkluzjom zbiorów otwartych homomorfizmy obcięć funkcji do mniejszych zbiorów, nazywamy *snopem funkcji regularnych* na V.

Z twierdzenia 1.8.2 wynika, że dla $f \in K[V] \setminus \{0\}$,

$$\mathcal{O}_V(V_f) = K[V]_f.$$

Ponadto, z twierdzenia Hilberta o zerach oraz z twierdzenia 1.8.2 wynika, że:

- *Jeśli $V_g \subset V_f$ dla pewnych $f, g \in K[V] \setminus \{0\}$, to dla pewnego $v \in K[V]$ oraz liczby naturalnej m mamy $g^m = vf$ i istnieje naturalne przekształcenie $K[V_f] = K[V]_f \to K[V]_g = K[V_g]$ określone przez*

$$a/f^s \mapsto av^s/g^{sm}.$$

Snop funkcji regularnych jest przykładem ogólnego pojęcia snopa funkcji. Niech X będzie przestrzenią topologiczną, a L dowolnym ciałem. Wtedy przyporządkowanie $\mathcal{O}_X$, które każdemu podzbiorowi otwartemu $U \subset X$ przyporządkowuje pewien zbiór $\mathcal{O}_X(U)$ złożony z funkcji $U \to L$, nazywamy *snopem funkcji* o wartościach w L, jeśli

- dla każdego otwartego $U \subset X$ zbiór funkcji $\mathcal{O}_X(U)$ jest zamknięty względem dodawania i mnożenia funkcji oraz zawiera wszystkie funkcje stałe o wartościach w L, a wiec jest L-algebrą,
- jeśli $V \subset U \subset X$ są zbiorami otwartymi, to ograniczenie $f|V$ funkcji $f \in \mathcal{O}_X(U)$ do zbioru V należy do $\mathcal{O}_X(V)$,
- jeśli $f : U \to L$ i istnieje takie pokrycie otwarte $\{V_i\}_{i \in I}$ zbioru U, że dla każdego $i \in I$ mamy $f|V_i \in \mathcal{O}_X(V_i)$, to $f \in \mathcal{O}_X(U)$.

Sprawdzenie, że ten ostatni warunek jest spełniony przez funkcje wymierne, jest bardzo proste. Wystarczy zauważyć, że jeśli X jest zbiorem nierozkładalnym, to każdy niepusty podzbiór otwarty jest gęsty i dwie funkcje wymierne równe na tym zbiorze są równe. Ogólny przypadek można łatwo sprowadzić do powyższego.

Innym przykładem snopa funkcji jest *snop funkcji różniczkowalnych* (*gładkich*) na rozmaitości różniczkowej. W tym przypadku zamiast funkcji wymiernych określonych na podzbiorach otwartych bierzemy funkcje różniczkowalne.

1.10. Morfizmy zbiorów afinicznych

Każde przekształcenie ϕ określone na zbiorze algebraicznym V o wartościach w zbiorze algebraicznym $W \subset K^m$ wyznaczone jest przez układ złożony z m funkcji $\phi_i : V \to K$, gdzie $i = 1, \dots, m$, określających współrzędne obrazu, tj.

$$\phi(a) = (\phi_1(a), \dots, \phi_m(a))$$

dla każdego $a \in V$. Jeśli funkcje ϕ_i są regularne, tj. $\phi_i \in K[V]$ dla $i = 1, \dots, m$, to tak zdefiniowane przekształcenie ϕ nazywamy *morfizmem* zbioru V w zbiór W i piszemy $\phi : V \to W$.

Łatwo zauważyć, że:

- *przekształcenie identycznościowe zbioru algebraicznego jest morfizmem;*
- *złożenie morfizmów* (*jeśli jest określone*) *jest morfizmem.*

Wobec tego afiniczne zbiory algebraiczne i ich morfizmy tworzą kategorię. Nazywamy ją *kategorią afinicznych zbiorów algebraicznych.*

Morfizm mający przekształcenie odwrotne, które w dodatku jest morfizmem, nazywamy *izomorfizmem.* Dwa zbiory algebraiczne V i W nazywamy *izomorficznymi*, gdy istnieje izomorfizm $V \to W$. Izomorfizm zbioru algebraicznego na siebie nazywamy *automorfizmem.*

Odnotujmy, że przekształcenie identycznościowe jest izomorfizmem. Złożenie izomorfizmów jest izomorfizmem i przekształcenie odwrotne do izomorfizmu jest izomorfizmem. Wobec tego wszystkie automorfizmy ustalonego zbioru algebraicznego tworzą grupę przekształceń. Inkluzja podzbiorów algebraicznych $V \subset W \subset K^n$ jest morfizmem. Zanotujmy jeszcze, że:

— *Morfizmy są przekształceniami ciągłymi* (*w topologii Zariskiego*).

Wynika stąd, że:

— *Jeśli* $\phi : V \to W$ *jest morfizmem oraz zbiór* V *jest nierozkładalny, to zbiór* $\overline{\phi(V)}$ *jest nierozkładalny.*

Przykłady i komentarze

1 Przekształcenia afiniczne przestrzeni afinicznych są morfizmami. Izomorfizmy (automorfizmy) afiniczne są izomorfizmami (automorfizmami).

2 Każda funkcja regularna $f : V \to K = K^1$ jest morfizmem.

3 Ograniczenie morfizmu do podzbioru algebraicznego jest morfizmem,

4 Rzutowanie $V \times W \to V$ jest morfizmem.

5 Jeśli $\phi_i : V_i \to W_i$, $i = 1, 2$, są morfizmami, to

$$\phi_1 \times \phi_2 : V_1 \times V_2 \to W_1 \times W_2$$

też jest morfizmem.

6 Wykres $\Gamma(\phi)$ morfizmu $\phi : V \to W$ jest podzbiorem algebraicznym w $V \times W$. Rzutowanie $\Gamma(\phi) \to V$ jest izomorfizmem. Morfizmem odwrotnym $V \to \Gamma(\phi)$ jest przekształcenie $x \mapsto (x, \phi(x))$. Wobec tego wykresy funkcji regularnych $f : K^n \to K$ są zbiorami algebraicznymi izomorficznymi z K^n. Na przykład zbiór $H \subset K^3$ określony równaniem

$$x_1^3 + x_1 x_2^5 + x_2^4 - x_3 = 0$$

jest izomorficzny z K^2 i izomorfizmem jest rzut H na dwie pierwsze osie.

7 Wszystkie automorfizmy $\phi : K^1 \to K^1$ są postaci $\phi(x_1) = cx_1 + d$, gdzie $c, d \in K$, $c \neq 0$, a zatem są przekształceniami afinicznymi.

8 Przekształcenia $\phi : K^2 \to K^2$ określone wzorem

$$\phi(x_1, x_2) = (ax_1 + b, cx_2 + f(x_1)),$$

gdzie $ac \neq 0$, $f(x_1) \in K[x_1]$, są automorfizmami. Automorfizmy takie nazywamy *trójkątnymi.* Jeśli $\deg(f(x_1)) > 1$, to automorfizm ϕ nie jest afiniczny, wobec tego automorfizm płaszczyzny na siebie nie musi być automorfizmem afinicznym. Można udowodnić, że każdy automorfizm $K^2 \to K^2$ jest złożeniem automorfizmów afinicznych oraz automorfizmów trójkątnych [19], [24].

9 Z definicji morfizmu wynika, że przekształcenie $\phi : K^2 \to K^2$ określone wzorem

$$\phi(x_1, x_2) = (\phi_1(x_1, x_2), \phi_2(x_1, x_2)),$$

gdzie $\phi_1, \phi_2 \in K[x_1, x_2]$, jest morfizmem. Jeśli jest to automorfizm, to wyznacznik Jacobiego

$$\frac{\partial \phi_1}{\partial x_1} \cdot \frac{\partial \phi_2}{\partial x_2} - \frac{\partial \phi_1}{\partial x_2} \cdot \frac{\partial \phi_2}{\partial x_1}$$

tego przekształcenia jest wielomianem wszędzie różnym od zera, a zatem jest różnym od zera wielomianem stałym. Nie wiadomo, czy ma miejsce implikacja odwrotna, a przypuszczenie, że tak jest, nosi nazwę *hipotezy jakobianowej.* Ustalenie, czy ta hipoteza jest prawdziwa, uważane jest za bardzo trudny problem.

10 Rozstrzygnięcie, czy dane dwa zbiory afiniczne są, czy nie są izomorficzne, może być skomplikowane. Na przykład pytanie, czy zbiór $V \subset K^4$ opisany równaniem $x_1 + x_1x_2 + x_3^3 + x_4^2 = 0$ jest izomorficzny z K^3, przez parę lat pozostawało bez odpowiedzi. Okazało się, że zbiory te nie są izomorficzne, ale dowód tego faktu jest długi i trudny ([28]). Dotychczas nie wiadomo, czy zbiór $V \times K^1$ jest izomorficzny z K^4.

11 Załóżmy, że $\mathrm{ch}(K) \neq 2$. Automorfizm $\phi : V \to V$ nazywamy *symetrią*, gdy $\phi \circ \phi = \mathrm{id}$. Jeśli $\phi(a) = a$, to mówimy, że a jest *punktem stałym.* Wiadomo (udowodnimy to w tej książce), że zbiór wszystkich punktów stałych symetrii $K^n \to K^n$ jest niepustym podzbiorem algebraicznym, ale nie wiadomo, czy ten podzbiór jest, dla każdej symetrii, izomorficzny z przestrzenią afiniczną K^s dla pewnego s spełniającego warunek $0 \leq s \leq n$. Wiadomo jedynie, że jest tak, gdy $n = 1, 2$. Rezultat ten i jego uogólnienia można znaleźć na przykład w [41] oraz [20].

12 Jeśli $\mathrm{ch}(K) = p$, gdzie p jest liczbą pierwszą, to morfizm (zwany *morfizmem Frobeniusa*) $\psi : K^n \to K^n$ określony wzorem $\psi(x_1, \ldots, x_n) = (x_1^p, \ldots, x_n^p)$ jest przekształceniem wzajemnie jednoznacznym, ale nie jest izomorfizmem.

Jeśli $\mathrm{ch}(K) = 0$, to każdy różnowartościowy morfizm zbioru algebraicznego w siebie jest automorfizmem (*twierdzenie Axa–Borela* [9]).

13 Niech równania $f_1 = 0, \dots, f_r = 0$ opisują podzbiór algebraiczny $V \subset K^n$. Wtedy przekształcenie $\phi : K^n \to K^{(n+1)r}$ określone wzorem

$$\phi(x_1, \dots, x_n) = (f_1, \dots, f_r, x_1 f_1, x_2 f_1, \dots, x_n f_1, \dots, x_1 f_r, x_2 f_r, \dots, x_n f_r)$$

jest morfizmem. Przy tym ϕ ściąga zbiór V do punktu $(0, \dots, 0)$ oraz obcięcie $\phi|(K^n \setminus V)$ jest różnowartościowe.

14 Niech $\phi : K^2 \to K^2$ będzie dane wzorem $\phi(x_1, x_2) = (x_1, x_1 x_2)$. Wtedy ϕ ściąga prostą $x_1 = 0$ do punktu. Obrazem $\phi(K^2) \subset K^2$ jest w tym przypadku płaszczyzna K^2 z pominięciem wszystkich punktów osi x_2 oprócz punktu $(0, 0)$. Wobec tego $\phi(K^2)$ nie jest ani podzbiorem otwartym, ani domkniętym.

Ponieważ funkcje regularne są morfizmami oraz złożenie morfizmów jest morfizmem, zatem każdy morfizm $\phi : V \to W$ wyznacza przekształcenie $K[W] \to K[V]$, które funkcji regularnej $f \in K[W]$ przyporządkowuje złożenie $f \circ \phi$. Jest to, jak łatwo sprawdzić, K-homomorfizm algebr. Homomorfizm ten oznaczamy przez ϕ^*.

Ale i odwrotnie, dla każdego homomorfizmu $\alpha : K[W] \to K[V]$ istnieje dokładnie jeden taki morfizm $\phi : V \to W$, że $\phi^* = \alpha$. Żeby się o tym przekonać, ustalmy włożenie $W \subset K^m$ i wyznaczony przez to włożenie układ generatorów $(t_1, \dots, t_m)$ algebry $K[W]$ odpowiadający funkcjom $x_1, \dots, x_m$ przyporządkowującym punktom z K^m ich współrzędne. Wówczas elementy $\alpha(t_1), \dots, \alpha(t_m)$ są funkcjami regularnymi na V. Niech przekształcenie $\phi : V \to W$ będzie określone wzorem

$$\phi(x) = (\alpha(t_1)(x), \dots, \alpha(t_m)(x)).$$

Wtedy $\phi^* = \alpha$.

Jeśli interpretujemy punkty zbioru algebraicznego jako K-homomorfizmy $K[V] \to K$ (§1.6), to opisane wyżej przyporządkowanie K-homomorfizmowi $\alpha : K[W] \to K[V]$ morfizmu $\phi : V \to W$ jest jeszcze prostsze: punktowi reprezentowanemu przez homomorfizm $K[V] \to K$ morfizm ϕ przyporządkowuje punkt odpowiadający złożeniu α z tym homomorfizmem.

Ponieważ każda skończenie generowana algebra bez elementów nilpotentnych jest postaci $K[V]$ dla pewnego zbioru V, oznacza to, że istnieje pełna odpowiedniość miedzy obiektami geometrycznymi, jakimi są zbiory algebraiczne i ich morfizmy, a obiektami algebraicznymi, jakimi są skończenie generowane K-algebry (bez elementów nilpotentnych) i ich K-homomorfizmy.

Geometryczne własności morfizmu $\phi : V \to W$ mają swe odbicie w algebraicznych własnościach homomorfizmu ϕ^* i odwrotnie. Zanotujmy niektóre z nich (ich sprawdzenie pozostawiamy Czytelnikowi):

- $\mathrm{id}^* = \mathrm{id}$.
- $(\phi_1 \circ \phi_2)^* = \phi_2^* \circ \phi_1^*$.

- *ϕ jest izomorfizmem zbiorów algebraicznych wtedy i tylko wtedy, gdy ϕ^* jest K-izomorfizmem algebr.*

Wniosek 1.10.1. *Zbiory algebraiczne V i W są izomorficzne wtedy i tylko wtedy, gdy K-algebry $K[V]$ oraz $K[W]$ są izomorficzne.*

A oto dalsze własności morfizmów:

- *$\phi(V)$ jest podzbiorem gęstym w W wtedy i tylko wtedy, gdy ϕ^* jest monomorfizmem.*
- *ϕ^* jest epimorfizmem wtedy i tylko wtedy, gdy ϕ jest izomorfizmem na podzbiór domknięty.*
- *Jeśli $\phi : V \to W$ jest morfizmem oraz $\phi(V) = W$, to ϕ^* jest włożeniem i wobec tego $K[W]$ można traktować jak podpierścień w $K[V]$.*

Przy umowie przyjętej w ostatnim punkcie oraz przy interpretacji punktów z V jako K-homomorfizmów $K[V] \to K$, a punktów z W jako K-homomorfizmów $K[W] \to K$, przekształcenie ϕ przyporządkowuje punktowi z V, tj. homomorfizmowi $K[V] \to K$, punkt z W utożsamiany z obcięciem tego homomorfizmu do podpierścienia $K[V]$. Ta algebraiczna interpretacja wartości morfizmu jest bardzo przydatna w dowodach twierdzeń. Przekonamy się o tym już w następnym paragrafie.

Przyporządkowując jak wyżej każdemu zbiorowi algebraicznemu V jego K-algebrę $K[V]$, a każdemu morfizmowi ϕ K-homomorfizm ϕ^*, otrzymujemy funktor kontrawariantny z kategorii zbiorów algebraicznych w kategorię K-algebr. Wyznaczyliśmy też taki funktor kontrawariantny z kategorii skończenie generowanych K-algebr bez elementów nilpotentnych w kategorię zbiorów algebraicznych, że złożenie obu funktorów w dowolnej kolejności nie zmienia klasy izomorfizmu obiektu. W języku teorii kategorii oznacza to, że każda z tych kategorii jest równoważna kategorii dualnej do drugiej.

1.11. Iloczyny zbiorów afinicznych

Niech V, W będą afinicznymi zbiorami algebraicznymi. Wtedy łatwo sprawdzić, że *rzutowania $\pi_1 : V \times W \to W$ oraz $\pi_2 : V \times W \to W$ są morfizmami*

$$\begin{tikzcd} & V \times W \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ V & & W \end{tikzcd}$$

i iloczyny zbiorów afinicznych (wraz z tymi dwoma morfizmami rzutowania) mają następującą *własność uniwersalną*:

$(*)$ *Dla każdej pary morfizmów $\phi_1 : Z \to V$, $\phi_2 : Z \to W$*

$$\begin{tikzcd} V & & W \\ & Z \arrow[ul, "\phi_1"] \arrow[ur, "\phi_2"'] & \end{tikzcd}$$

istnieje dokładnie jeden taki morfizm $\kappa : Z \to V \times W$ (oznaczany często przez $\phi_1 \times \phi_2$), że $\pi_1 \circ \kappa = \phi_1$ oraz $\pi_2 \circ \kappa = \phi_2$.

$$\begin{tikzcd} & V \times W \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ V & & W \\ & Z \arrow[ul, "\phi_1"] \arrow[ur, "\phi_2"'] \arrow[uu, "\kappa"] & \end{tikzcd}$$

Twierdzenie 1.11.1. *Jeśli V i W są zbiorami nierozkładalnymi, to iloczyn $V \times W$ jest też nierozkładalny.*

Dowód. Załóżmy, że V, W są nierozkładalne, i niech $V \times W = Z_1 \cup Z_2$, gdzie Z_1, Z_2 są domknięte. Dla ustalonego $w \in W$ rozpatrzmy podzbiór $V_w \subset V$ złożony z tych punktów $v \in V$, że $(v, w) \in Z_1$. Podzbiór ten jest domknięty (rozważ $(V \times \{w\}) \cap Z_1$). Wobec tego domknięta jest też część wspólna

$$\bigcap V_w,$$

gdzie w przebiega cały zbiór W. Ta część wspólna składa się z wszystkich takich punktów $v \in V$, że $\{v\} \times W \subset Z_1$. Podobnie podzbiorem domkniętym jest zbiór tych punktów $v \in V$, że $\{v\} \times W \subset Z_2$. Ponieważ zbiór W jest nierozkładalny, zatem dla każdego $v \in V$ ($\{v\} \times W$ jest nierozkładalny i wobec tego) albo $\{v\} \times W \subset Z_1$, albo $\{v\} \times W \subset Z_2$. Suma tych dwóch podzbiorów domkniętych jest więc równa V. Ponieważ zbiór V jest nierozkładalny, jeden z podzbiorów jest równy całemu V, a stąd $Z_1 = V \times W$ lub $Z_2 = V \times W$, co kończy dowód.

Jeśli V, W, S są afinicznymi zbiorami algebraicznymi, a

$$\tau_1 : V \to S, \qquad \tau_2 : W \to S$$

są morfizmami, to definiujemy

$$V \times_S W := \{(v, w) \in V \times W;\ \tau_1(v) = \tau_2(w)\}.$$

Łatwo udowodnić, że jest to podzbiór domknięty w $V \times W$.

Gdy S jest zbiorem jednopunktowym, wtedy $V \times_S W = V \times W$. W ogólnym przypadku zbiór $V \times_S W$ wraz z rzutowaniami π_1, π_2 na osie V i W:

$$\begin{tikzcd}
& V \times_S W \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
V \arrow[dr, "\tau_1"'] & & W \arrow[dl, "\tau_2"] \\
& S &
\end{tikzcd}$$

ma następującą własność uniwersalną, analogiczną do $(*)$:

$(**)$ *dla każdego morfizmu* $\lambda : Z \to S$ *i pary morfizmów* $\phi_1 : Z \to V$, $\phi_2 : Z \to W$ *takich, że*

$$\lambda = \tau_1 \circ \phi_1, \quad \lambda = \tau_2 \circ \phi_2$$

$$\begin{tikzcd}
V \arrow[ddr, "\tau_1"'] & & W \arrow[ddl, "\tau_2"] \\
& Z \arrow[ul, "\phi_1"'] \arrow[ur, "\phi_2"] \arrow[d, "\lambda"] & \\
& S &
\end{tikzcd}$$

istnieje dokładnie jeden morfizm $\kappa : Z \to V \times_S W$ (*oznaczany przez* $\phi_1 \times_S \phi_2$) *o tej własności, że*

$$\pi_1 \circ \kappa = \phi_1, \quad \pi_2 \circ \kappa = \phi_2.$$

$$\begin{tikzcd}
& V \times_S W \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
V \arrow[ddr, "\tau_1"'] & & W \arrow[ddl, "\tau_2"] \\
& Z \arrow[uu, "\kappa"] \arrow[ul, "\phi_1"] \arrow[ur, "\phi_2"'] \arrow[d, "\lambda"] & \\
& S &
\end{tikzcd}$$

Własność ta określa $V \times_S W$ (wraz z rzutowaniami) jednoznacznie z dokładnością do izomorfizmu, a wobec tego można ją przyjąć za definicję iloczynu $V \times_S W$.

W tym miejscu Czytelnik może czuć się zniechęcony rozważaniami formalnymi, i autor nie ma chwilowo nic do powiedzenia na swą obronę. W przyszłości okaże się jednak, że uogólnione pojęcie iloczynu $\times_S$ będzie nieodzowne dla rozwinięcia teorii, a w definicji tego pojęcia najprościej będzie powołać się na własność uniwersalną $(**)$.

Czytelnik obeznany z teorią kategorii bez trudu rozpoznaje w $(*)$ i $(**)$ definicje iloczynu ([7, rozdz. I, §17]) w odpowiednich kategoriach zbiorów afinicznych oraz morfizmów w ustalony zbiór afiniczny.

1.12. Twierdzenie Chevalleya o obrazie

Przykład 14 w §1.10 pokazuje, że obraz zbioru algebraicznego przy morfizmie może nie być podzbiorem algebraicznym. Obrazy zbiorów algebraicznych są jednak dosyć regularne. Wynika to z następującego ważnego i użytecznego wyniku:

Twierdzenie 1.12.1 (Chevalleya o obrazie)**.** *Niech $\phi : V \to W$ będzie morfizmem zbiorów afinicznych i niech $\overline{\phi(V)} = W$. Wtedy $\phi(V)$ zawiera niepusty podzbiór otwarty w W.*

Jeśli warunek $\overline{\phi(V)} = W$ nie jest spełniony, to należy w miejsce W przyjąć $\overline{\phi(V)}$. Wówczas założenia powyższego twierdzenia będą spełnione, zatem $\phi(V)$ zawiera niepusty podzbiór otwarty zbioru $\overline{\phi(V)}$.

Dowód twierdzenia Chevalleya opiera się na następującym rozumowaniu. Zauważmy najpierw, że *wystarczy ograniczyć się do przypadku, gdy zbiór V jest nierozkładalny*. Ponadto *morfizm $\phi : V \to W$ wyznacza zanurzenie $K[W] \hookrightarrow K[V]$*.

Następnie, korzystając z interpretacji punktu zbioru algebraicznego jako K-homomorfizmu pierścienia funkcji regularnych na V w K, stwierdzamy, że *punkt $w \in W$ leży w $\phi(V)$ wtedy i tylko wtedy, gdy homomorfizm $K[W] \to K$ wyznaczony przez w daje się rozszerzyć do homomorfizmu $K[V] \to K$.*

Będziemy się starali znaleźć zbiór otwarty postaci W_c, gdzie $c \in K[W]$, $c \neq 0$, zawarty w $\phi(V)$. W tym celu wystarcza wskazać taki element $c \in K[W] \setminus \{0\}$, że każdy K-homomorfizm $\kappa : K[W] \to K$ taki, że $\kappa(c) \neq 0$, daje się przedłużyć do $K[V] \to K$. Wobec tego wystarczy udowodnić następujący rezultat:

Twierdzenie 1.12.2 (o rozszerzaniu homomorfizmów)**.** *Niech R_1 będzie pierścieniem bez dzielników zera i niech $R_0 \subset R_1$ będzie takim podpierścieniem, że $R_1 = R_0[b_1, \ldots, b_s]$ dla pewnych $b_1, \ldots, b_s \in R_1$. Wówczas istnieje taki różny od* *zera element $c \in R_0$, że każdy homomorfizm $\kappa : R_0 \to L$, gdzie L jest dowolnym ciałem, spełniający warunek $\kappa(c) \neq 0$ rozszerza się do homomorfizmu $R_1 \to \overline{L}$, gdzie $\overline{L}$ jest domknięciem algebraicznym ciała L.*

Ten rezultat wynika łatwo (przez indukcję względem s) z następującego lematu:

Lemat 1.12.1. *Niech R_1 będzie pierścieniem bez dzielników zera, a $R_0 \subset R_1$ podpierścieniem. Niech $R_1 = R_0[b]$ dla pewnego $b \in R_1$. Niech $d \in R_1 \setminus \{0\}$. Wtedy istnieje taki element $c \in R_0 \setminus \{0\}$, że każdy homomorfizm $\kappa : R_0 \to L$, dla którego $\kappa(c) \neq 0$, rozszerza się do homomorfizmu $\overline{\kappa} : R_1 \to \overline{L}$ spełniającego warunek $\overline{\kappa}(d) \neq 0$.*

Dowód lematu. Ponieważ $d \in R_1 = R_0[b]$, zatem istnieje taki wielomian $g(x) \in R_0[x]$, że $g(b) = d$. Niech $g(x) = e_t x^t + e_{t-1}x^{t-1} + \cdots + e_0$. Można założyć, że $e_t \neq 0$, bo $d \neq 0$.

Jeśli b jest elementem przestępnym nad ciałem ułamków $Q(R_0)$ pierścienia R_0, to możemy rozszerzyć homomorfizm κ na $R_1 = R[b]$, przypisując elementowi b dowolną wartość $a \in \overline{L}$. Jeśli przy tym $\kappa(e_t) \neq 0$, to tę wartość a można dobrać tak, by

$$\begin{aligned}\overline{\kappa}(d) &= \overline{\kappa}(e_t b^t + e_{t-1}b^{t-1} + \cdots + e_0)\\ &= \kappa(e_t)a^t + \kappa(e_{t-1})a^{t-1} + \cdots + \kappa(e_0) \neq 0.\end{aligned}$$

Wobec tego jako c należy wziąć e_t.

Jeśli element b nie jest przestępny, to wybierzmy wielomian $f(x) \in R_0[x]$ niezerowy najniższego stopnia, którego b jest pierwiastkiem. Wówczas $\deg(f) > 0$. Niech $c_1 \neq 0$ będzie współczynnikiem przy najwyższej potędze x występującej w f. Wykażemy najpierw, że:

- *Każdy homomorfizm $\kappa : R_0 \to L$, dla którego $\kappa(c_1) \neq 0$, można rozszerzyć do homomorfizmu $\overline{\kappa} : R_0[b] \to \overline{L}$.*

Niech I_b będzie jądrem homomorfizmu $R_0[x] \to R_0[b] = R_1$, przy którym $x \mapsto b$, i niech $\mathbf{m}$ będzie ideałem w $R_0[x]$ generowanym przez $\ker(\kappa)$. Wystarczy wykazać, że $I_b + \mathbf{m}$ jest ideałem właściwym w $R_0[x]$, gdyż *każdy ideał maksymalny zawierający $I_b + \mathbf{m}$ wyznacza pewien homomorfizm $R_0[b] \to \overline{L}$ będący przedłużeniem homomorfizmu κ*. Korzystamy tu z założenia, że element b jest algebraiczny nad R_0 oraz $\kappa(c_1) \neq 0$, skąd wnosimy, że obraz elementu b będzie elementem algebraicznym nad $\kappa(R_0) \subset L$, a zatem będzie należał do $\overline{L}$.

Załóżmy zatem, że $1 \in I_b + \mathbf{m}$, a więc że w pierścieniu $R_0[x]$ mamy równość $1 = i + m$ dla pewnych $i \in I_b$, $m \in \mathbf{m}$. Podstawiając w tej równości b w miejsce x, otrzymamy $m(b) = 1$. Wobec tego b jest pierwiastkiem wielomianu $m - 1$. Ponieważ f jest wielomianem najniższego stopnia, którego b jest pierwiastkiem, zatem wielomian $m-1$ jest podzielny przez f w pierścieniu $Q(R_0)[x]$. Wobec tego dla pewnej liczby naturalnej s wielomian $c_1^s(m-1)$ jest podzielny przez f w $R_0[x]$, a więc

$$c_1^s(m-1) = f_1 f$$

dla pewnego $f_1 \in R_0[x]$. Weźmy teraz wartość homomorfizmu κ rozszerzonego na $R_0[x] \to L[x]$ (a oznaczonego w dalszym ciągu przez κ) dla wielomianów stojących po obu stronach tej równości. Otrzymamy $\kappa(c_1)^s(\kappa(m)-1) = \kappa(f_1)\kappa(f)$, a ponieważ $\kappa(m) = 0$, zatem

$$-\kappa(c_1)^s = \kappa(f_1)\kappa(f).$$

Otrzymaliśmy sprzeczność, bo po lewej stronie stoi różny od zera element ciała L, a po prawej iloczyn dwóch wielomianów, z których jeden (a mianowicie $\kappa(f)$) *jest wielomianem dodatniego stopnia*.

Aby zakończyć dowód lematu, załóżmy, że homomorfizm $\kappa : R_0 \to L$ daje się rozszerzyć do $\overline{\kappa} : R_1 = R_0[b] \to \overline{L}$. Chcemy ponadto, by $\overline{\kappa}(d) \neq 0$. Wiemy, że $d = g(b) \neq 0$ (zob. początek dowodu), zatem w $Q(R_0)[x]$ wielomian g nie jest podzielny przez f, a ponieważ f jest nierozkładalny, zatem wielomiany f, g są względnie pierwsze w $Q(R_0)[x]$. Wobec tego istnieją w $R_0[x]$ takie wielomiany F, G, że $Ff + Gg = c_2 \in R$, $c_2 \neq 0$. Jeśli $c = c_1c_2$, to $c \neq 0$. Jeśli $\kappa : R_0 \to L$ jest takim homomorfizmem, że $\kappa(c) \neq 0$, to κ można rozszerzyć do $\overline{\kappa} : R_0[b] \to \overline{L}$, bo $\kappa(c_1) \neq 0$. Ponadto, po podstawieniu b w miejsce x w $Ff + Gg = c_2$ otrzymamy $G(b)g(b) = c_2$. Wobec tego

$$\overline{\kappa}(G(b))\overline{\kappa}(d) = \overline{\kappa}(G(b))\overline{\kappa}(g(b)) = \overline{\kappa}(c_2) \neq 0,$$

a zatem $\overline{\kappa}(d) \neq 0$. Wynika stąd, że jako c wystarczy wziąć c_1c_2, i dowód został zakończony.

Z tego lematu wynika twierdzenie o rozszerzaniu, a zatem kończy to już dowód twierdzenia Chevalleya.

Twierdzenie Chevalleya można też sformułować w następujący sposób:

Twierdzenie 1.12.3. *Obraz zbioru algebraicznego V przy morfizmie $\phi : V \to W$ jest skończoną sumą podzbiorów lokalnie domkniętych, tzn. podzbiorów postaci $X \setminus Z$, gdzie X oraz Z są podzbiorami domkniętymi w W.*

Podzbiory, które są skończonymi sumami zbiorów lokalnie domkniętych, nazywane są często *zbiorami konstruowalnymi*.

Dowód twierdzenia Chevalleya w tej nowej wersji jest bardzo łatwy, jeśli ma się do dyspozycji twierdzenie Chevalleya w wersji poprzedniej oraz podstawowe twierdzenia teorii wymiaru, dlatego zaproponowany zostanie jako zadanie w rozdziale poświęconym tej teorii.

Twierdzenie Hilberta o zerach w wersji C (zob. §1.3.1) jest prostym wnioskiem z twierdzenia o rozszerzaniu homomorfizmów. Jeśli bowiem $R_0 = K$ oraz $R_1 = K[a_1, \dots, a_s]$ jest K-algebrą, to z twierdzenia o rozszerzaniu homomorfizmów zastosowanego do izomorfizmu identycznościowego $R_0 = K \to K$ wynika istnienie K-homomorfizmu $K[a_1, \dots, a_n] \to K$. Ponieważ w dowodzie twierdzenia o rozszerzaniu homomorfizmów wykorzystywaliśmy jedynie proste fakty dotyczące podzielności wielomianów, a nie korzystaliśmy nigdzie z twierdzenia Hilberta o zerach, zatem uzyskaliśmy jeszcze jeden dowód tego twierdzenia.

Z twierdzenia o rozszerzaniu homomorfizmów wynika też następujący rezultat użyteczny w arytmetyce i algebraicznej teorii liczb.

Twierdzenie 1.12.4. *Niech $R = \mathbb{Z}[a_1, \dots, a_s]$ będzie pierścieniem skończenie generowanym, a $\mathbf{m}$ jego ideałem maksymalnym. Wtedy ciało $R/\mathbf{m}$ jest skończone. Ponadto jeśli p jest daną liczbą pierwszą, to ideał $\mathbf{m}$ można wybrać tak, by* $\mathrm{ch}(R/\mathbf{m}) \neq p$.

Dowód. Należy udowodnić, że skończenie generowane (jako pierścień) ciało $L = \mathbb{Z}[a_1, \dots, a_s]/\mathbf{m}$ jest skończone. Ciało L zawiera obraz homomorficzny R_0 pierścienia $\mathbb{Z}$ i możemy stosować twierdzenie o rozszerzaniu do przypadku $R_0 \subset L$. Wobec tego istnieje taki element $c \in R_0 \setminus \{0\}$, że każdy homomorfizm κ odwzorowujący R_0 w jakiekolwiek ciało L_1 i spełniający warunek $\kappa(c) \neq 0$ daje się rozszerzyć do homomorfizmu ciała L w skończone rozszerzenie ciała L_1. Ponieważ dla każdego takiego c istnieje homomorfizm κ pierścienia R_0 na ciało skończone, spełniający warunek $\kappa(c) \neq 0$, zatem istnieje homomorfizm ciała L w skończone rozszerzenie ciała skończonego, a wobec tego L jest ciałem skończonym. Ostatnie zdanie twierdzenia jest oczywiste.

1.13. Przekształcenia wymierne

Każdy morfizm $V \to W \subset K^m$ jest wyznaczony przez podanie funkcji regularnych $f_1, \dots, f_m \in K[V]$ określających kolejne współrzędne obrazu. Jeżeli odstąpimy od wymagania, by funkcje te były regularne, ale przyjmiemy jedynie, że są to funkcje wymierne określone na podzbiorach gęstych w V, to otrzymamy przekształcenie określone jedynie na podzbiorze otwartym gęstym w V. Tak określone przekształcenia nazywamy *przekształceniami wymiernymi* zbioru V w zbiór W.

Jeśli zbiory V, W są nierozkładalne i obraz przekształcenia wymiernego $\phi : V \to W$ jest gęsty w W, to złożenie $f \circ \phi$, gdzie $f \in K(W)$, należy do $K(V)$. Wobec tego ϕ wyznacza przekształcenie $K(W) \to K(V)$ oznaczane przez ϕ^*. Podobnie jak w przypadku morfizmów (na podzbiór gęsty) przekształcenie to jest zanurzeniem.

Przekształcenie wymierne ϕ zbioru V w zbiór W nazywamy *biwymiernym*, jeśli istnieje dla niego przekształcenie wymierne odwrotne, tzn. takie przekształcenie wymierne zbioru W w V, że złożenia tych dwóch przekształceń są przekształceniami identycznościowymi (wszędzie tam, gdzie są określone). Łatwo wykazać, że przekształcenie wymierne ϕ jest biwymierne wtedy i tylko wtedy, gdy ϕ^* jest izomorfizmem.

Zbiory algebraiczne nazywamy *biwymiernie równoważnymi*, gdy istnieje między nimi przekształcenie biwymierne, a to ma miejsce wtedy i tylko wtedy, gdy ich ciała funkcji wymiernych są izomorficzne (nad K).

Jeśli zbiór V jest rozkładalny, to przez przekształcenie wymierne tego zbioru rozumiemy każdy układ przekształceń wymiernych określonych na składowych nierozkładalnych tego zbioru.

Przekształcenia wymierne można też zdefiniować jako morfizmy określone na gęstych podzbiorach otwartych, przy czym dwa takie morfizmy uważamy za tożsame, gdy są równe tam, gdzie są oba określone. Taka definicja jest równoważna definicji podanej poprzednio.

Twierdzenie 1.13.1. *Jeżeli V_1, V_2 są biwymiernie równoważnymi zbiorami afinicznymi, to istnieją takie niepuste podzbiory otwarte $U_1 \subset V_1$ oraz $U_2 \subset V_2$, które są izomorficzne.*

Dowód. Na mocy założenia istnieją przekształcenia wymierne $\phi_1 : V_1 \to V_2$ oraz $\phi_2 : V_2 \to V_1$, których złożenia są identycznościami. Niech przekształcenie ϕ_1 będzie określone na $U_1' \subset V_1$, a ϕ_2 – na $U_2' \subset V_2$. Wówczas $\phi_1 \circ \phi_2$ jest identycznością na $U_2' \cap \phi_2^{-1}(U_1')$, podobnie $\phi_2 \circ \phi_1$ jest identycznością na $U_1' \cap \phi_1^{-1}(U_2')$. Wobec tego ϕ_1 oraz ϕ_2 określają izomorfizm między $U_1 = \phi_1^{-1} \circ \phi_2^{-1}(U_1')$ a $U_2 = \phi_2^{-1} \circ \phi_1^{-1}(U_2')$, co kończy dowód.

Powyższe twierdzenie nadaje pojęciu biwymiernej równoważności jasny sens geometryczny.

Zbiory biwymiernie równoważne przestrzeniom afinicznym K^n nazywamy *zbiorami wymiernymi.*

Nietrudno udowodnić, że:

- *Każdy nierozkładalny zbiór algebraiczny jest biwymiernie równoważny hiperpowierzchni (tzn. podzbiorowi $V \subset K^n$ określonemu tylko jednym równaniem).*

Rezultat ten wynika z lematu Noether o normalizacji 1.3.2 oraz z następującego twierdzenia Abela (zob. [7, tw. 5.6, str. 186]):

- *Każde skończone rozdzielcze rozszerzenie ciał jest generowane przez jeden element.*

Istotnie, z tych dwóch rezultatów wynika, że każde skończenie generowane rozszerzenie $K \subset K(a_1, \ldots, a_r)$ może być przedstawione jako

$$K \subset K(x_1, \ldots, x_s, a),$$

gdzie elementy $x_1, \ldots, x_s$ są algebraicznie niezależne, natomiast a jest elementem algebraicznym nad $K(x_1, \ldots, x_s)$. Jeśli teraz

$$g(x_{s+1}) \in K[x_1, \ldots, x_s][x_{s+1}] = K[x_1, \ldots, x_s, x_{s+1}]$$

jest wielomianem nierozkładalnym w $K[x_1, \ldots, x_s, x_{s+1}]$, którego a jest pierwiastkiem, to równanie $g = 0$, gdzie niewiadomymi są $x_1, \ldots, x_{s+1}$, opisuje w K^{s+1} hiperpłaszczyznę, której ciałem funkcji wymiernych jest

$$K(x_1, \ldots, x_s, a) = K(a_1, \ldots, a_r),$$

i to kończy dowód.

Sprawdzenie, czy dane dwa zbiory algebraiczne są biwymiernie równoważne, może być zadaniem bardzo trudnym.

Przykłady

1 Prosta afiniczna K^1 oraz hiperbola dana równaniem $x_1x_2 = 1$ są biwymiernie równoważne. Rzutowanie hiperboli na oś x_1 jest biwymierne, jego odwrotnością jest przekształcenie wymierne prostej K^1 w hiperbolę określone przez $x_1 \mapsto (x_1, 1/x_1)$.

2 Niech $\mathrm{ch}(K) \neq 2$. Naszkicujemy dowód faktu, że zbiór algebraiczny V w K^n opisany równaniem $x_1^2 + x_2^2 + \cdots + x_n^2 = 1$ jest wymierny. Niech H będzie hiperpłaszczyzną w K^n o równaniu $x_n = 0$. Niech $v_0 = (0, \ldots, 0, 1) \in V$. Określmy przekształcenie π zdefiniowane na pewnym podzbiorze zbioru V w H w następujący sposób. Punktowi $v \in V$ różnemu od v_0 przyporządkowujemy punkt przecięcia prostej przechodzącej przez punkty v_0 oraz v z hiperpłaszczyzną H (jeśli ta prosta przecina H). Można wykazać, że jest to przekształcenie biwymierne.

3 Niech $\mathrm{ch}(K) \neq 3$. Naszkicujemy dowód rezultatu mówiącego, że zbiór algebraiczny $V \subset k^3$ opisany równaniem $x_1^3 + x_2^3 + x_3^3 = 1$ jest wymierny. Zbiór V zawiera dwie proste skośne L_1, L_2 opisane przez dwa układy równań: $x_3 = 1$, $x_1 + x_2 = 0$ oraz $x_3 = \epsilon$, $\epsilon x_1 + x_2 = 0$, gdzie ϵ jest pierwiastkiem trzeciego stopnia z 1 różnym od 1. Niech, dla każdego $v \in V \setminus (L_1 \cup L_2)$, $L(v)$ oznacza prostą będącą przecięciem płaszczyzn rozpiętych odpowiednio na $L_1 \cup \{v\}$ oraz na $L_2 \cup \{v\}$. Niech teraz H będzie płaszczyzną, która nie zawiera ani L_1, ani L_2. Przekształcenie, które przyporządkowuje punktowi $v \in V$ punkt przecięcia tak określonej prostej $L(v)$ z H, jest przekształceniem biwymiernym zbioru V w H.

4 *Stożkową afiniczną* nazywamy zbiór algebraiczny $V \subset K^2$ opisany równaniem $f = 0$ stopnia 2, przy czym zakładamy, że w żadnym punkcie zbioru V wielomiany $\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}$ nie są jednocześnie równe zero. Jeśli $\mathrm{ch}(k) \neq 2$, to dobierając odpowiednio układ współrzędnych, można równaniu temu nadać postać $x_1x_2 - 1 = 0$ lub $x_1^2 + x_2 = 0$. Ciała funkcji wymiernych dwóch ostatnich zbiorów są generowane przez x_1, zatem wszystkie stożkowe są biwymiernie równoważne z K^1, a więc wymierne.

5 *Afiniczną krzywą eliptyczną* nazywamy zbiór algebraiczny $V \subset K^2$ opisany równaniem $f = 0$ stopnia 3, przy czym zakładamy, że w żadnym punkcie zbioru V wielomiany $\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}$ nie są jednocześnie równe zero. Jeśli $\mathrm{ch}(K) \neq 2, 3$, to, można udowodnić, że każda krzywa eliptyczna jest biwymiernie równoważna krzywej danej równaniem $x_2^2 = x_1^3 + ax_1 + b$, gdzie wielomian $x_1^3 + ax_1 + b$ nie ma pierwiastków wielokrotnych. Afiniczne krzywe eliptyczne nie są wymierne i na ogół dwie takie krzywe nie są biwymiernie równoważne. Na przykład krzywe eliptyczne określone równaniami $x_1^2 = x_2^3 + x_2 + a$, $x_1^2 = x_2^3 + x_2 + b$, gdzie $a^2 \neq b^2, ab \neq 0$, nie są biwymiernie równoważne (zakładamy, że $\mathrm{ch}(K) \neq 2, 3$).

6 Przez kilkadziesiąt lat nie było wiadomo, czy zbiory $V_3, V_4 \subset K^4$ określone odpowiednio równaniami $x_1^4 + x_2^4 + x_3^4 + x_4^4 = 1$ oraz $x_1^3 + x_2^3 + x_3^3 + x_4^3 = 1$ są wymierne. Okazało się, że jeśli $\mathrm{ch}(K) = 0$, to *nie są* [10], [18].

7 Zbiór algebraiczny V nazywamy *uniwymiernym*, gdy jest nierozkładalny i pewne algebraiczne rozszerzenie ciała funkcji wymiernych $K(V)$ jest K-izomorficzne z $K(x_1, \ldots, x_n)$, gdzie $x_1, \ldots, x_n$ są zmiennymi. Twierdzenie Lürotha ([7, str. 287]) mówi, że jeśli w powyższej definicji $n = 1$, to uniwymierność jest równoważna wymierności zbioru. Jest tak też dla $n = 2$, o ile $\mathrm{ch}(K) = 0$ (twierdzenie Castelnuovo, [7, str. 288]). Zbiory algebraiczne V_3, V_4 opisane w poprzednim przykładzie są uniwymierne (w tym przypadku $n = 3$) i do czasu znalezienia dowodu, że nie są to zbiory wymierne, sądzono, że uniwymierność jest zawsze równoważna wymierności.

1.14. Przestrzenie ze snopami funkcji

Niech V będzie afinicznym zbiorem algebraicznym. Dla podzbioru otwartego $U \subset V$ umówiliśmy się, że $\mathcal{O}_V(U)$ oznacza algebrę funkcji regularnych na U, tzn. funkcji wymiernych określonych we wszystkich punktach zbioru U.

Określone tak przyporządkowanie $U \mapsto \mathcal{O}_V(U)$ jest, jak już wiemy, snopem funkcji.

Wiemy też, że $\phi : V \to W$ jest morfizmem wtedy i tylko wtedy, gdy dla każdej funkcji regularnej $f : W \to K$ złożenie $f \circ \phi$ jest funkcją regularną na V. Ze względu na późniejsze zastosowania warto ten rezultat zmodyfikować:

Jeśli V, W są zbiorami algebraicznymi oraz $\phi : V \to W$ jest morfizmem, to dla każdego podzbioru otwartego $U \subset W$ oraz funkcji $f \in \mathcal{O}_W(U)$ złożenie $f \circ \phi$ należy do $\mathcal{O}_V(\phi^{-1}(U))$. Wyznaczone tak przyporządkowanie wyznacza homomorfizm algebr

$$\mathcal{O}_W(U) \to \mathcal{O}_V(\phi^{-1}(U)).$$

Odwrotnie, jeśli $\phi : V \to W$ jest takim przekształceniem ciągłym zbiorów algebraicznych, że dla każdego podzbioru otwartego $U \subset W$ i funkcji regularnej $f : U \to K$ złożenie $f \circ \phi$ jest funkcją regularną na $\phi^{-1}(U)$, to ϕ jest morfizmem.

Z rezultatu tego wynika, że dla wyznaczenia morfizmów (w tym izomorfizmów) afinicznego zbioru algebraicznego $V \subset K^n$ wystarcza podanie przestrzeni topologicznej V oraz snopa $\mathcal{O}_V$. Wobec tego nic nie stoi na przeszkodzie, by rozumieć afiniczny zbiór algebraiczny jako parę $(V, \mathcal{O}_V)$. Para ta wyznacza bowiem zbiór afiniczny z dokładnością do izomorfizmu i pozwala na wyznaczenie morfizmów tego zbioru. Takie rozumienie afinicznego zbioru algebraicznego doprowadzi nas później do ważnych uogólnień, jakimi są ogólne zbiory algebraiczne.

Na razie zauważmy, że jeśli $U \subset V$ jest podzbiorem otwartym, to snop funkcji $\mathcal{O}_V$, po ograniczeniu do tych podzbiorów otwartych, które są zawarte w U, wyznacza snop funkcji na U. Wobec tego można również określić pojęcie *morfizmu dowolnych podzbiorów otwartych* afinicznych zbiorów algebraicznych, przyjmując powyższą własność morfizmu jako definicję. *Pozwala to na wygodną równoważną definicję przekształcenia wymiernego jako morfizmu określonego na otwartym podzbiorze gęstym.*

Ze względu na inne analogiczne sytuacje, z którymi można się spotkać w geometrii, warto wprowadzić język, który będzie służyć do opisu takich sytuacji i ich uogólnień. W tym celu rozważać będziemy przestrzenie topologiczne X wraz z ustalonym snopem funkcji $\mathcal{O}_X$ (o wartościach w ustalonym ciele K). Jeśli dane są dwie takie przestrzenie X_1, X_2 ze snopami $\mathcal{O}_{X_1}$, $\mathcal{O}_{X_2}$ oraz takie przekształcenie ciągłe $\phi : X_1 \to X_2$, że dla każdego podzbioru otwartego $U \subset X_2$ oraz funkcji $f \in \mathcal{O}_{X_2}(U)$ złożenie $f \circ \phi$ należy do $\mathcal{O}_{X_1}(\phi^{-1}(U))$, to mówimy, że ϕ jest morfizmem pary $(X_1, \mathcal{O}_{X_1})$ w parę $(X_2, \mathcal{O}_{X_2})$. Morfizm ϕ nazywamy izomorfizmem, gdy jest przekształceniem wzajemnie jednoznacznym oraz ϕ^{-1} jest też morfizmem.

Warto tu jeszcze zauważyć, że jeśli dana jest para $(X, \mathcal{O}_X)$, a $U \subset X$ jest podzbiorem otwartym, to możemy na U określić snop funkcji, przyjmując $\mathcal{O}_X(W)$ jako wartość tego snopa dla każdego zbioru otwartego $W \subset U$. Tak otrzymany snop oznaczamy przez $\mathcal{O}_X|U$ i nazywamy *ograniczeniem* (lub *obcięciem*) *snopa* $\mathcal{O}_X$ do U. Włożenie $U \to X$ jest wówczas morfizmem $(U, \mathcal{O}_X|U)$ w $(X, \mathcal{O}_X)$.

Klasa wszystkich par $(X, \mathcal{O}_X)$ wraz z takimi morfizmami tworzy kategorię. Natomiast pary $(V, \mathcal{O}_V)$, gdzie V jest afinicznym zbiorem algebraicznym, a $\mathcal{O}_V$ snopem funkcji regularnych, wraz z morfizmami zbiorów algebraicznych, tworzą pełną podkategorię tej kategorii. Z podobną sytuacją mamy do czynienia w geometrii różniczkowej, gdy wygodnie jest identyfikować gładką podrozmaitość różniczkową $X \subset \mathbb{R}^n$ z parą $(X, \mathcal{O}_X)$, gdzie $\mathcal{O}_X$ jest snopem rzeczywistych funkcji gładkich.

Przykład. Niech $\mathrm{ch}(K) \neq 2, 3$. Niech $f = x(x-1)(x-2)(x-3)$. Zbiór $V \subset K^1$ określony równaniem $f = 0$ składa się z czterech punktów $0, 1, 2, 3$. Pierścień $K[V] = K[x]/(f)$ jest izomorficzny z sumą prostą $K \oplus K \oplus K \oplus K$. Każda z osi odpowiada jednemu z czterech punktów tego zbioru, w tym sensie, że wartość funkcji $f \in K[V]$ w tym punkcie jest równa współrzędnej funkcji $f \in K \oplus K \oplus K \oplus K$ na tej osi. Każdy podzbiór tego czteroelementowego zbioru jest otwarty i każda funkcja o wartościach w K jest regularna. Snop $\mathcal{O}_V$ pokrywa się ze snopem wszystkich funkcji o wartościach w K. Ten zbiór algebraiczny jest zatem izomorficzny z dowolnym innym zbiorem algebraicznym złożonym z czterech punktów. Ogólniej:

Dowolne dwa skończone równoliczne zbiory algebraiczne są izomorficzne.

1.15. Podzbiory analityczne przestrzeni zespolonych

W przypadku dowolnego ciała K funkcje wielomianowe i ich ilorazy – funkcje wymierne – można traktować jako odpowiedniki, czy też zamienniki, funkcji różniczkowalnych. Istotnie, każdy wielomian, i ogólniej każdą funkcję wymierną, można formalnie różniczkować; z drugiej strony, brak naturalnej szerszej klasy funkcji, które można by rozważać na przestrzeniach afinicznych nad dowolnym ciałem, a tym bardziej brak szerszej klasy funkcji, które można by różniczkować.

W przypadku $K = \mathbb{C}$ naturalne jest jednak rozważanie, oprócz wielomianów, również wszystkich funkcji różniczkowalnych (w sensie zespolonym). Funkcje takie nazywa się holomorficznymi. Dokładniej, jeśli $W \subset \mathbb{C}^n$ jest podzbiorem otwartym w topologii naturalnej, to funkcję $W \to \mathbb{C}$ nazywamy *holomorficzną*, gdy dla każdego $w \in W$ funkcja ta jest różniczkowalna w sensie zespolonym lub równoważnie gdy jest rozwijalna w szereg potęgowy zbieżny w pewnym otoczeniu tego punktu.

Gdy w definicji zbioru algebraicznego zastąpimy funkcje wielomianowe przez holomorficzne, otrzymamy następujące określenie: podzbiór $V \subset \mathbb{C}^n$ nazywamy *zbiorem analitycznym*, jeśli dla każdego punktu $a \in V$ istnieje takie otoczenie W_a oraz układ $h_1, \ldots, h_r$ funkcji holomorficznych na W_a, że

$$W_a \cap V = \{z \in W_a;\ h_1(z) = 0, \ldots, h_r(z) = 0\}.$$

Dla zbioru analitycznego $V \subset \mathbb{C}^n$ oraz podzbioru otwartego $U \subset V$ funkcję $f : U \to \mathbb{C}$ nazywamy *holomorficzną* (na U), jeśli dla każdego $a \in U$ istnieje takie otoczenie W w $\mathbb{C}^n$ oraz funkcja holomorficzna h na W, że $f|(W \cap U) = h|(W \cap U)$.

Jeśli dla podzbioru analitycznego $V \subset \mathbb{C}^n$ i podzbioru otwartego $U \subset V$ określimy $\mathcal{O}_V(U)$ jako zbiór wszystkich funkcji holomorficznych na U, to otrzymamy snop funkcji na V. Tak jak w przypadku algebraicznym, za zbiór analityczny będziemy uważać parę $(V, \mathcal{O}_V)$.

Waga tych pojęć dla geometrii algebraicznej wynika stąd, że każdy zbiór algebraiczny $V \subset \mathbb{C}^n$ jest zbiorem analitycznym, a do badania zbiorów analitycznych możemy stosować metody analityczne.

1.16. Snopy, schematy afiniczne

W poprzednich paragrafach związaliśmy z każdą K-algebrą skończenie generowaną i bez elementów nilpotentnych, gdzie K jest ciałem algebraicznie domkniętym, pewną strukturę geometryczną – przestrzeń topologiczną ze snopem funkcji o wartościach w K. Ta struktura geometryczna może być przedstawiona jako podzbiór przestrzeni K^n ze snopem funkcji wyznaczonych przez funkcje wymierne. Jest jednak parę ważnych powodów, dla których ograniczenie rozważań do powyższej klasy K-algebr jest zbyt krępujące:

Po pierwsze, rozpatrzmy przypadek $\mathrm{ch}(K) \neq 2$ i bardzo prosty morfizm $\phi : K^1 \to K^1$, określony wzorem $\phi(t) = t^2$. Przeciwobraz $\phi^{-1}(a)$ punktu $a \in K^1$ jest opisany równaniem $x^2 - a = 0$. Gdy $a \neq 0$, przeciwobraz ten składa się z dwóch różnych punktów i odpowiada mu K-algebra $K[x]/(x^2 - a)$. Jeśli jednak $a = 0$, to przeciwobraz jest opisany równaniem $x^2 = 0$, składa się więc z jednego punktu, ale „krotności 2". Celowe wydaje się uwzględnienie tego faktu i przypisanie temu przeciwobrazowi K-algebry $K[x]/(x^2)$, która zawiera elementy nilpotentne.

Po drugie, przecięcie $V_1 \cap V_2$ podzbiorów algebraicznych $V_1, V_2 \subset K^n$ opisane jest przez ideał $\mathbf{I}(V_1) + \mathbf{I}(V_2)$, który na ogół nie jest radykalny, a wobec tego algebra $K[x_1, \ldots, x_n]/(\mathbf{I}(V_1) + \mathbf{I}(V_2))$ może zawierać elementy nilpotentne. Gdybyśmy się jednak umówili, że temu przecięciu przyporządkowujemy zawsze K-algebrę $K[x_1, \ldots, x_n]/(\mathbf{I}(V_1) + \mathbf{I}(V_2))$, to moglibyśmy uwzględnić charakter tego przecięcia („stopień styczności").

Po trzecie, każdemu morfizmowi $V \to W$ odpowiada homomorfizm $K[W] \to K[V]$, a zatem pierścień $K[V]$ staje się $K[W]$-algebrą. Gdybyśmy mieli definicje i twierdzenia dotyczące struktur geometrycznych przypisanych algebrom *nad pierścieniami*, to mielibyśmy teorię opisującą zarówno zbiory afiniczne, jak i ich morfizmy.

Po czwarte, wprowadzone wyżej założenia nie pozwalają na wzajemnie jednoznaczne wiązanie struktur geometrycznych z układami równań wielomianowych określonych nad dowolnymi pierścieniami (np. $\mathbb{Z}$), a nawet nad ciałami, które nie są algebraicznie domknięte (np. $\mathbb{Q}$ i $\mathbb{R}$).

Odpowiedź na te wyzwania daje stworzona przez Grothendiecka teoria schematów w swym afinicznym fragmencie. Jej podstawowe definicje podajemy niżej.

Zacznijmy od definicji snopa o wartościach w pierścieniach. Otóż *snopem pierścieni* nad przestrzenią topologiczną X nazywamy przyporządkowanie $\mathcal{O}$ każdemu zbiorowi otwartemu $U \subset X$ pewnego pierścienia $\mathcal{O}(U)$ (jego elementy nazywamy *przekrojami snopa* $\mathcal{O}$ nad U), a każdej parze zbiorów otwartych $U \supset T$ *homomorfizmu obcięcia przekrojów* $r_{U,T} : \mathcal{O}(U) \to \mathcal{O}(T)$, o następujących własnościach:

1. dla każdego zbioru otwartego U mamy $r_{U,U} = \mathrm{id}_{\mathcal{O}(U)}$,
2. dla każdej trójki zbiorów otwartych $U \supset T \supset Z$ mamy $r_{T,Z} \circ r_{U,T} = r_{U,Z}$,
3. jeśli $\{U_i\}_{i \in I}$ jest pokryciem otwartym zbioru otwartego $U \subset X$ oraz dla każdego $i \in I$ wybrany jest przekrój $s_i \in \mathcal{O}(U)$ taki, że dla $i, j \in I$ obcięcia przekrojów s_i, s_j do $U_i \cap U_j$ są równe, to istnieje dokładnie jeden taki przekrój $s \in \mathcal{O}(U)$, którego obcięcie do każdego U_i jest równe s_i.

Zapewne Czytelnik zauważa, że w analogiczny sposób można definiować *snopy zbiorów, snopy grup, snopy grup abelowych* itd. Dalej sporadycznie będziemy z tych pojęć korzystać, a w ostatnim rozdziale książki rozpatrzymy dokładniej przypadek snopów grup abelowych.

Jeśli $\mathcal{O}$ jest snopem pierścieni nad przestrzenią topologiczną X oraz $x \in X$, to *źdźbłem* snopa $\mathcal{O}$ w punkcie x nazywamy zbiór $\mathcal{O}_x$ klas równoważności przekrojów snopa $\mathcal{O}$ na otoczeniach punktu x, przy czym dwa takie przekroje uważamy za równoważne, gdy ich obcięcia do pewnego otoczenia punktu x są równe. Ponieważ przekroje snopa pierścieni nad ustalonym zbiorem otwartym tworzą pierścień, łatwo zauważyć, że taką samą strukturę ma też każde źdźbło takiego snopa. Definicja źdźbła przenosi się bez trudu na snopy zbiorów, snopy grup itd. i w tych sytuacjach źdźbła mają również taką strukturę, jak przekroje.

Podstawowymi przykładami snopów pierścieni są snopy funkcji, o których była wyżej mowa. W szczególności gdy $\mathcal{O}$ jest snopem funkcji regularnych na zbiorze afinicznym V, źdźbło $\mathcal{O}_{v,V}$ snopa $\mathcal{O}$ w punkcie $v \in V$ jest pierścieniem lokalnym, tzn. zawiera tylko jeden ideał maksymalny. Jest nim podzbiór złożony z tych funkcji wymiernych na V, które są równe 0 w punkcie v.

Jeśli mamy teraz dwie pary $(X, \mathcal{O}_X)$, $(Y, \mathcal{O}_Y)$ złożone z przestrzeni topologicznych oraz snopów pierścieni, to morfizm snopów $\phi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ określamy, podając przekształcenie ciągłe (oznaczane też przez) $\phi : X \to Y$ oraz dla każdego podzbioru otwartego $U \subset Y$ homomorfizm pierścieni

$$\phi_U : \mathcal{O}_Y(U) \to \mathcal{O}_X(\phi^{-1}(U))$$

przemienny z obcięciami. Znowu podstawowych przykładów takich morfizmów dostarczają morfizmy afinicznych zbiorów algebraicznych. Analogicznie możemy określić morfizmy innych typów snopów: snopów zbiorów, grup itd.

Niech teraz R będzie dowolnym pierścieniem (przemiennym z 1). Niech $\mathrm{Spec}(R)$ będzie zbiorem wszystkich ideałów pierwszych pierścienia R z topologią Zariskiego. Wiemy już, że bazą zbiorów otwartych dla tej topologii jest rodzina wszystkich zbiorów postaci $\mathrm{Spec}(R)_f = \{\mathbf{p} \in \mathrm{Spec}(R); f \notin \mathbf{p}\}$ (str. 25).

Na $\mathrm{Spec}(R)$ *można określić snop pierścieni* $\mathcal{O} = \mathcal{O}_{\mathrm{Spec}(R)}$ *tak, by spełniony był warunek*

$$\mathcal{O}(\mathrm{Spec}(R)_f) = R_f,$$

gdzie R_f *oznacza pierścień ułamków postaci* r/f^m *dla* $r \in R$, $m \in \mathbb{N}$, *oraz by homomorfizmy obcięcia dla* $\mathrm{Spec}(R)_g \subset \mathrm{Spec}(R)_f$ *były naturalnymi homomorfizmami* $\kappa_{f,g} : R_f \to R_g$. *Istnienie tych naturalnych homomorfizmów wynika stąd, że jeśli* $\mathrm{Spec}(R)_g \subset \mathrm{Spec}(R)_f$, *to* $g^m = af^m$ *dla pewnych* $a \in R$ *oraz* $m \in \mathbb{N}$ (por. twierdzenie 1.8.2).

Dowód tego rezultatu nie jest trudny, ale mozolny. Najpierw trzeba wykazać, że przyporządkowanie

$$\mathrm{Spec}(R)_f \mapsto R_f \quad \text{oraz} \quad (\mathrm{Spec}(R)_g \subset \mathrm{Spec}(R)_f) \mapsto (\kappa_{f,g} : R_f \to R_g)$$

spełnia warunki definicji snopa w obrębie zbiorów postaci $\mathrm{Spec}(R)_f$. Najbardziej kłopotliwe jest sprawdzenie warunku trzeciego. Należy zauważyć, że w obrębie zbiorów tej postaci warunek ten jest sensowny, bo część wspólna zbiorów postaci $\mathrm{Spec}(R)_f$ jest też tej postaci. Następnie trzeba skorzystać z metody użytej w dowodzie twierdzeń 1.8.1 oraz 1.8.2. Dowód kończy następujący lemat, użyteczny w teorii snopów (nie tylko pierścieni):

Lemat 1.16.1. *Niech X będzie dowolną przestrzenią topologiczną, a $\{V_t\}_{t\in T}$ jej bazą zamkniętą względem skończonych przecięć. Każde przekształcenie, które zbiorom należącym do tej bazy przyporządkowuje pierścienie (lub zbiory, grupy itd.), a inkluzjom zbiorów należących do tej bazy – homomorfizmy przyporządkowanych pierścieni (odpowiednio: zbiorów, grup itd.) w taki sposób, że w tym obrębie spełnione są warunki definicji snopa, można jednoznacznie rozszerzyć do snopa.*

Idea dowodu lematu jest jasna. Dowolnemu zbiorowi otwartemu $U \subset X$ przyporządkowujemy pierścień zgodnych rodzin przekrojów dla pokryć zbioru U przez zbiory otwarte należące do $\{V_t\}_{t\in T}$, przy czym dwie takie zgodne rodziny uważamy za równe, gdy ich przekroje po obcięciu do pewnych podzbiorów z $\{V_t\}_{t\in T}$ tworzących pokrycie zbioru U są równe. Określenie homomorfizmów obcięć jest też oczywiste: jeśli $U_1 \supset U_2$, to przekroje tworzące zgodną rodzinę na U_1 należy obciąć do przecięć z U_2, otrzymując zgodną rodzinę na U_2.

Źdźbłem tego snopa w punkcie $\mathbf{p} \in \mathrm{Spec}(R)$ *jest pierścień lokalny* $R_{\mathbf{p}}$, tzn. pierścień ułamków postaci r_1/r_2, gdzie $r_1 \in R$, $r_2 \in R \setminus \mathbf{p}$ (zob. [1, Przykłady, 1, str. 50]).

Parę $(\mathrm{Spec}(R), \mathcal{O}_{\mathrm{Spec}(R)})$ nazywamy *schematem afinicznym* (pierścienia R).

Punktem wyjścia do sformułowania definicji morfizmów schematów afinicznych jest ogólna definicja morfizmów przestrzeni ze snopami pierścieni. Jednak nie wszystkie takie morfizmy chcemy zaakceptować w szczególnej sytuacji schematów afinicznych.

Otóż każdy ogólny morfizm $\phi : (X_1, \mathcal{O}_1) \to (X_2, \mathcal{O}_2)$ wyznacza homomorfizm źdźbeł $\mathcal{O}_{x_1} \to \mathcal{O}_{x_2}$ dla $x_2 = \phi(x_1)$. W przypadku schematów afinicznych źdźbła te są pierścieniami lokalnymi i dodatkowo postulujemy, by przy tym homomorfizmie obraz ideału maksymalnego pierścienia lokalnego $\mathcal{O}_{x_1}$ był zawarty w ideale maksymalnym pierścienia $\mathcal{O}_{x_2}$. Okazuje się, że przy tym ograniczeniu morfizmy schematów afinicznych $\phi : (X_1, \mathcal{O}_1) \to (X_2, \mathcal{O}_2)$, gdzie $X_i = \mathrm{Spec}(R_i)$, $i = 1, 2$, są jednoznacznie wyznaczone przez homomorfizmy przekrojów globalnych $R_2 = \mathcal{O}_2(X_2) \to \mathcal{O}_1(X_1) = R_1$.

W ujęciu Grothendiecka podstawowymi obiektami teorii schematów afinicznych nie są jednak odpowiadające pierścieniom schematy afiniczne i ich morfizmy, ale morfizmy schematów afinicznych w ustalony schemat S (odpowiadający ustalonemu pierścieniowi R_0) oraz ich morfizmy. Takie morfizmy nazywamy *S-schematami.*

Algebraicznym odpowiednikiem tej kategorii geometrycznej jest kategoria algebr nad ustalonym pierścieniem R_0. Gdy w szczególności jako S weźmiemy $\mathrm{Spec}(K)$, otrzymamy kategorię schematów odpowiadających K-algebrom. Wśród nich najbliższe naszym zainteresowaniom są schematy odpowiadające algebrom skończenie generowanym (nad K). Dla takich algebr $R = K[a_1, \dots, a_s]$

schemat $\mathrm{Spec}(R)$ oraz zbiór $\mathrm{Spec_m}(R)$ niosą tę samą treść matematyczną, gdyż każdy zbiór otwarty $U \subset \mathrm{Spec}(R)$ jest jednoznacznie wyznaczony przez swe przecięcie z $\mathrm{Spec_m}(R)$.

Jeśli algebra R nie ma elementów nilpotentnych, to $\mathrm{Spec_m}(R)$ z tym obciętym snopem jest afinicznym zbiorem algebraicznym. Wobec tego jeśli R jest skończenie generowaną K-algebrą bez elementów nilpotentnych, to $\mathrm{Spec}(R)$ ze swym snopem pierścieni wyznacza i jest wyznaczone przez pewien zbiór afiniczny ze snopem funkcji regularnych. Jeśli jednak w R są elementy nilpotentne, to w dalszym ciągu $\mathrm{Spec}(R)$ wraz ze swym snopem pierścieni jest pewnym obiektem geometrycznym, który można badać podobnymi metodami jak zbiory afiniczne.

Uwaga. Może się wydawać, że rozszerzenie naszych rozważań na dowolne pierścienie i przyporządkowanie im struktury geometrycznej, jaką jest spektrum, nie może być owocne, gdyż od samego początku podstawą naszych rezultatów było twierdzenie Hilberta o zerach, prawdziwe jedynie dla skończenie generowanych algebr nad ciałem algebraicznie domkniętym.

Wrażenie to jest jednak fałszywe. Rzecz w tym, że kluczowa dla naszych rozważań wersja D twierdzenia Hilberta o zerach mówi, że dla każdego ideału I rozpatrywanego tam pierścienia, część wspólna wszystkich ideałów odpowiadajacych punktom zbioru algebraicznego wyznaczonego przez ideał I jest równa radykałowi ideału I. Otóż dla spektrów analogiczne twierdzenie też jest prawdziwe, bo część wspólna wszystkich ideałów odpowiadających punktom podzbioru w spektrum wyznaczonego przez ten ideał to część wspólna wszystkich ideałów pierwszych zawierających ideał I, a zatem radykał ideału I ([1, stw. 1.14, str. 18] lub [2, wniosek (1.1.5), str. 12]). Zresztą wspominaliśmy już o tym poprzednio.

Dla każdej pary schematów, ogólniej: dla każdej pary morfizmów w ustalony schemat S, powiedzmy $\tau_1 : V \to S$, $\tau_2 : W \to S$, można określić ich *iloczyn* $V \times_S W$ jako morfizm w S wraz z dwoma rzutowaniami π_1, π_2, który ma własność uniwersalną $(**)$ wprowadzoną w §1.11.

Odwoływanie się tu do definicji iloczynu zbiorów afinicznych jako iloczynu kartezjańskiego okazuje się w teorii schematów bezsensowne i dopiero teraz widać sens przyjęcia własności uniwersalnej za definicję. Można udowodnić

Twierdzenie 1.16.1. *Dla dowolnych dwóch S-schematów X_1, X_2 istnieje ich iloczyn $X_1 \times_S X_2$.*

Aby to wykazać, należy wziąć spektrum iloczynu tensorowego algebr wyznaczających te S-schematy.

Dla dowolnego pierścienia R elementy nilpotentne w R tworzą ideał $N(R)$. Iloraz $R_{\mathrm{red}} = R/N(R)$ nazywamy *redukcją* pierścienia R, a jego schemat afiniczny $\mathrm{Spec}(R_{\mathrm{red}})$ nazywamy *redukcją* schematu $\mathrm{Spec}(R)$ i oznaczamy przez $\mathrm{Spec}(R)_{\mathrm{red}}$. Schemat nazywamy *zredukowanym*, gdy jest identyczny ze swą redukcją. Kanoniczny homomorfizm $R \to R_{\mathrm{red}}$ wyznacza morfizm schematów $\mathrm{Spec}(R_{\mathrm{red}}) \to \mathrm{Spec}(R)$.

Morfizm redukcji ma własność uniwersalną (względem wszystkich morfizmów schematów zredukowanych w $\mathrm{Spec}(R)$).

Pojęcie schematu wiąże z każdym pierścieniem przestrzeń topologiczną ze snopem pierścieni. W przypadku klasycznej geometrii algebraicznej jest to związek K-algebr skończenie generowanych bez elementów nilpotentnych oraz afinicznych zbiorów algebraicznych. Tu podstawowym obiektem naszych zainteresowań są geometryczne własności zbiorów algebraicznych, a metoda badawcza polega na interpretowaniu tych własności w terminach własności algebr i sprowadzaniu problemów geometrycznych do algebry.

Teoria schematów pozwala jednak również na działalność odwrotną – badanie dowolnych pierścieni przez sprowadzanie problemów algebraicznych do problemów dotyczących przyporządkowanych im struktur geometrycznych (schematów). Możliwości te wpłynęły bardzo istotnie na rozwój teorii liczb i wyróżnienie działu zwanego geometrią arytmetyczną. Podstawowymi algebraicznymi obiektami badań są tu skończenie generowane $\mathbb{Z}$-algebry (w tym pierścienie elementów całkowitych w skończonych rozszerzeniach $K \supset \mathbb{Q}$) oraz obiekty geometryczne, jakimi są schematy tych algebr.

W dalszym ciągu książki będziemy rozwijać przede wszystkim teorię zbiorów algebraicznych. Jednak od czasu do czasu będziemy też wspominać o wersjach i paralelach arytmetycznych, mieszczących się w ogólnej teorii schematów.

Przyporządkowanie każdemu pierścieniowi R jego spektrum $(\mathrm{Spec}(R), \mathcal{O}_{\mathrm{Spec}(R)})$, a każdemu homomorfizmowi pierścieni $\phi : R_1 \to R_2$ morfizmu

$$\phi^* : (\mathrm{Spec}(R_2), \mathcal{O}_{\mathrm{Spec}(R_2)}) \to (\mathrm{Spec}(R_1), \mathcal{O}_{\mathrm{Spec}(R_1)})$$

jest funktorem kontrawariantnym. Funktor ten określa równoważność kategorii dualnej do kategorii pierścieni oraz kategorii spektrów pierścieni. Wobec tego możemy zdefiniować kategorię spektrów pierścieni jako kategorię dualną do kategorii pierścieni, pozostawiając na boku kwestię geometrycznych interpretacji obiektów i morfizmów tej kategorii, ale przyjmując, że kategoria ta, jako kategoria do dualna do kategorii algebraicznej, ma charakter geometryczny. W ten sposób otrzymujemy parę wzajemnie dualnych kategorii. W jednej z nich dostrzegamy charakter algebraiczny, a w drugiej – geometryczny.

Kategoria pierścieni, o której tu mowa, to kategoria pierścieni przemiennych z jedynką, a zatem pełna podkategoria znacznie obszerniejszej kategorii wszystkich (także nieprzemiennych) pierścieni z 1. Nic nie stoi na przeszkodzie, by rozważać jej kategorię dualną i traktować jej obiekty oraz morfizmy tak, jak gdyby miały charakter geometryczny, oraz ten charakter ujawniać i opisywać. Takie obiekty nazywane są *algebraicznymi zbiorami kwantowymi*. Idee te w ostatnich dziesięcioleciach zafascynowały wielu wybitnych matematyków i doprowadziły do powstania i rozwoju nowej gałęzi matematyki, zwanej *geometrią algebraiczną nieprzemienną*.

Istnieje też wersja topologiczna tej teorii (w odróżnieniu od powyższej, geometryczno-algebraicznej). W tej wersji rozważa się najpierw kategorię zwartych przestrzeni topologicznych i dualną do niej kategorię przemiennych C^*-algebr z 1. Każdej przestrzeni zwartej odpowiada tu C^*-algebra (z 1) wszystkich zespolonych funkcji ciągłych określonych na tej przestrzeni (z normą wyznaczoną przez kres górny modułów wartości i operacją $*$ sprzężenia zespolonego). Następnie kategorię przemiennych C^*-algebr z 1 traktuje się jako podkategorię kategorii wszystkich (na ogół nieprzemiennych) C^*-algebr i kategorię dualną do tej kategorii traktuje się jako geometryczną kategorię przestrzeni kwantowych. Użycie słowa „kwantowy” wiąże się z pewnymi nadziejami, jakie kiedyś łączono z zastosowaniami fizycznymi tych teorii.

Zadania

1 Niech $K \subset L \subset K(a_1, \ldots, a_n)$ będzie wieżą rozszerzeń ciał. Udowodnij, że ciało L jest skończenie generowane nad K.

2 Niech R będzie podpierścieniem ciała L i niech $\alpha : R \to K$ będzie homomorfizmem w algebraicznie domknięte ciało K. Niech $a \in L \setminus \{0\}$. Udowodnij, że α można rozszerzyć do homomorfizmu $R[a] \to K$ lub do homomorfizmu $R[a^{-1}] \to K$. Wskazówka: Najpierw udowodnij, że można założyć, iż pierścień R jest lokalny, a jego ideałem maksymalnym jest $\ker \alpha$. Potem wykaż, że jeśli homomorfizmu α nie można przedłużyć na $R[a]$, to element a^{-1} jest calkowity nad R.

3 Pierścień R nazywamy *pierścieniem Jacobsona*, gdy każdy jego ideał pierwszy jest częścią wspólną ideałów maksymalnych. Udowodnij, że jeśli R jest pierścieniem Jacobsona, to każdy pierścień skończenie generowany nad R jest też pierścieniem Jacobsona.

4 Udowodnij, że jeśli R jest pierścieniem Jacobsona oraz pierścień

$$R[a_1, \ldots, a_r] \supset R$$

jest ciałem, to R jest ciałem, a $R[a_1, \ldots, a_r] \supset R$ jest rozszerzeniem algebraicznym. Wyprowadź stąd twierdzenie Hilberta o zerach.

5 Niech $V \subset K^n$ będzie zbiorem afinicznym i niech $f \in K[V] \setminus \{0\}$. Udowodnij, że zbiór V_f jest (izomorficzny ze) zbiorem afinicznym.

6 Przyjmij, że $\mathrm{ch}(K) \neq 2, 3$. Dla jakich wartości parametru $a \in K$ istnieje niestały morfizm $\phi : K^1 \to C_a$, gdzie zbiór $C_a \subset K^2$ jest opisany równaniem $x_1^2 - x_2^3 - a = 0$? Następnie przyjmij $K = \mathbb{C}$ i narysuj na płaszczyźnie $\mathbb{R}^2$ część rzeczywistą krzywych C_0 oraz C_1.

7 Niech $\phi : K^1 \to K^n$. Udowodnij, że $\phi(K^1) = \overline{\phi(K^1)}$.

8 Wykaż, że morfizm $\phi : K^1 \to K^2$ określony wzorem

$$\phi(x) = (x(x-1), x^2(x-1))$$

zlepia punkty $0, 1$, a na pozostałych jest różnowartościowy i przekształca prostą K^1 na krzywą o równaniu $x_1^3 - x_2^2 + x_1 x_2 = 0$. Przyjmij $K = \mathbb{C}$ i narysuj na płaszczyźnie $\mathbb{R}^2$ część rzeczywistą tej krzywej.

9 Znajdź taki morfizm $\phi : K^2 \to W$, że ϕ jest izomorfizmem na właściwy podzbiór otwarty w W.

10 Czy istnieje morfizm hiperboli $x_1 x_2 = 1$ na K^1? Czy istnieje morfizm prostej K^1 na hiperbolę? Czy istnieje morfizm zbioru V opisanego równaniem $x_1^2 x^2 + x_3 x_4 = 1$ na K^1? Znajdź podzbiór domknięty w K^2, którego obraz przy rzutowaniu na oś x_1 jest równy całej tej prostej bez czterech punktów.

11 Znajdź taki morfizm $\phi : K^2 \to K^4$, który przekształca hiperbolę $x_1 x_2 = 1$ w punkt $(0, 0, 0, 0)$, ale na dopełnieniu tej hiperboli jest przekształceniem różnowartościowym.

12 Znajdź taki morfizm $K^2 \to K^6$, który zlepia dwa punkty $(0, 0), (0, 1)$, a na pozostałych punktach jest różnowartościowy.

13 Czy produkt dwóch hiperbol zawiera podzbiór domknięty izomorficzny z prostą K^1?