Skąd się wzięły ciała w algebrze?

Witold WIĘSŁAW, Wrocław

0. Wstęp

Czy jest bardziej naturalne pojęcie w matematyce od pojęcia ciała?
Chyba nie !

Głównym przesłaniem matematyki jest sztuka liczenia, poczynając od najprostszych obiektów, jakimi są liczby.

Jeżeli na zbiorze elementów można bezkarnie wykonywać operacje dodawania, mnożenia, odejmowania i dzielenia (prócz dzielenia przez zero) w oparciu o zwykłe reguły działań (przemienność, łączność, rozdzielność mnożenia względem dodawania), to taki zbiór z działaniami zwykle nazywany jest *ciałem.*

Pojęcia ciała można się już doszukiwać u Euklidesa, który w X księdze *Elementów* wprowadza liczby postaci $x + y\sqrt{z}$.

Euler posługiwał się liczbami postaci $a + b\varepsilon$, gdzie a, b są liczbami wymiernymi, a ε jest pierwotnym pierwiastkiem z jedności stopnia 3. Dopiero jednak Gauss w *Disquisitiones Arithmeticae* posługuje się (nie nazwanym) pojęciem ciała. U Gaussa występują implicite nie tylko ciała liczb algebraicznych, lecz także ciało $\mathbf{F}_p$ reszt modulo p, jako szczególny przypadek pierścienia $\mathbf{Z}_n$ reszt modulo n.

Kummer w swoich badaniach nad Wielkim Twierdzeniem Fermata posługiwał się kombinacjami liniowymi o współczynnikach wymiernych potęg $1, \varepsilon, \varepsilon^2, \ldots$ pierwotnego pierwiastka z jedności ε stopnia n.

Galois, uogólniając konstrukcję Gaussa, rozważa skończone rozszerzenie ciała $\mathbf{F}_p$. Wprowadza m. in. analogon liczb zespolonych $x + iy$, gdzie $x, y \in \mathbf{F}_p$ ($p \not\equiv 1 \pmod 4$).

Kronecker posługiwał się ciałami funkcji wymiernych wielu zmiennych, nazywając je *Integritätsbereich.* Dopiero Dedekind podał precyzyjną definicję ciała liczbowego, a Weber – aksjomatyczną definicję ciała abstrakcyjnego. Definicja ta analizowana była przez innych matematyków takich, jak Dickson, Hancock, Huntington, Hurwitz, Wedderburn i inni.

Rozprawa Steinitza z 1910 roku zamyka wstępny okres budowania abstrakcyjnej teorii ciał. Zawiera już zarówno podstawowe pojęcia dotyczące ciał, jak też najważniejsze wyniki, niekiedy jednak bez pełnych dowodów.

1. Ciało C liczb zespolonych

W liście do Oldenburga z 1676/77 Leibniz wspomina już o rzeczywistej sumie liczb zespolonych sprzężonych.

De Moivre (*Miscell. anal.* 1730, str. 1) formułuje dla $\cos x = a$ i dowolnej liczby naturalnej m wzór zwany dziś jego imieniem:

$$2\cos mx = (a + \sqrt{a^2 - 1})^m + (a - \sqrt{a^2 - 1})^m.$$

Mimo, że Newton znał już szeregi potęgowe dla e^x, $\cos x$, $\sin x$, to jednak dopiero Euler docenił i zastosował twierdzenie Moivre'a oraz wyraził e^{ix} w postaci $\cos x + \sin x$ (*Introductio in Analysin Infinitorum*, 1748, tom 1, §138; Mém. de Berlin 1749, str. 265; por. też list Eulera do Goldbacha z 9 grudnia 1741). Wyrażenie iloczynu, ilorazu, potęgi, pierwiastka i logarytmu liczb zespolonych przez ich argumenty i moduły prócz Eulera podał także d'Alembert (Mém. de Berlin, 1746; str. 192; *Sur les vents* n° 78).

Argand wprowadza w 1806 liczby zespolone jako wektory na płaszczyźnie ([Arga 1], [Arga 2]). Na ten temat pisał także Français w 1813 [Fran]. Cauchy [Cauc] nie tylko stosuje metodę Arganda, lecz także podaje formalną konstrukcję liczb zespolonych jako pierścienia ilorazowego $\mathbf{R}[X]/(X^2 + 1)$.

Gauss w 1831 (Werke, tom 2, str. 169) rozważa punkty $x + iy$ tworzące *zweifach unendliche Mannigfaltigkeit, wie die Punkte einer Fläche.* Znacznie wcześniej, bo już 18 grudnia 1811 pisał Gauss do Bessela o analizie zespolonej:

Was soll man sich nun bei $\int \varphi x.dx$ *für* $x = a + bi$ *denken ?*

Konstrukcja Cauchy'ego ciała $\mathbf{C}$ jako pierścienia ilorazowego (Cauchy używał równoważnego sformułowania) prowadzi bezpośrednio do formalnej konstrukcji ciała $\mathbf{C}$ liczb zespolonych jako przestrzeni $\mathbf{R}^2$ z odpowiednio określonymi działaniami, czyli do wcześniejszej konstrukcji Hamiltona z 1837 roku [Hami]. Chronologicznie konstrukcja Hamiltona była pierwszą formalną definicją liczb zespolonych. Hamilton definiuje w $\mathbf{R}^2$ dwa działania:

odejmowanie

$$(b_1, b_2) - (a_1, a_2) = (b_1 - a_1, b_2 - a_2)$$

oraz mnożenie

$$(b_1, b_2)(a_1, a_2) = (b_1 a_1 - b_2 a_2, b_2 a_1 + b_1 a_2),$$

dowodząc, że w ten sposób otrzymuje się liczby zespolone.

Hamilton cytuje w tym miejscu *Cours d'Analyse* Cauchy'ego z 1821 roku (str. 176).
Wstęp Hamiltona do dzieła *Quaternions* jest dziś znacznie ciekawszy od samego dzieła. Hamilton opisuje tam kolejne próby zdefiniowania w analogiczny sposób, jak w $\mathbf{R}^2$, działań w $\mathbf{R}^3$ i uzasadnia, dlaczego to mu się nie udało. Następnie przechodzi do przestrzeni $\mathbf{R}^4$ i tu udaje mu się odpowiednia konstrukcja, znana dziś jako konstrukcja kwaternionów. Wynika stąd niezbicie, że odkrycie kwaternionów nie było przypadkiem, lecz że poprzedzone zostało gruntownymi poszukiwaniami i próbami przeniesienia znanych mu konstrukcji na przestrzenie wymiaru większego niż dwa.

Jedną z pierwszych prób zdefiniowania ciała można znaleźć w książce Hankela [Hank] z 1867; nie wywarła ona jednak – jak się wydaje – większego wpływu na ówczesnych matematyków.

Dokładniejszą historię liczb zespolonych można znaleźć w [Więś 4].

2. Pierwsze przykłady ciał

Jak już wspomnieliśmy we Wstępie, pierwsze przykłady ciał, choć nie nazwane, występują już u Eulera. Gauss w *Disquisitiones Arithmeticae* wprowadził i systematycznie badał ciała cyklotomiczne $Q(\varepsilon_n)$ (Rozdział VII, *O równaniach, od których zależy podział koła – Sectio septima, de aequationibus circuli sectiones definientibus*). Kolejno w ustępach 335, 336, 229 i 340 Gauss dowodzi, że jeżeli p jest liczbą pierwszą, to

$$x^{p-1} + x^{p-2} + \ldots + x + 1$$

jest wielomianem nieprzywiedlnym nad ciałem liczb wymiernych, a więc ciało cyklotomiczne $Q(\varepsilon_p)$ jest stopnia $p - 1$ nad Q.
We wcześniejszych rozdziałach, budując teorię kongruencji modulo n, Gauss rozważa przypadek, gdy n jest liczbą pierwszą, konstruując tym samym ciało $\mathbf{F}_p$ reszt modulo p.

Ciała cyklotomiczne pojawiły się w pierwszej połowie XIX wieku u Kroneckera i Kummera. Kronecker [Kron 2] w swojej pracy doktorskiej z 1845 napisanej pod kierunkiem Lejeune-Dirichleta bada systematycznie ciała $Q(\varepsilon_n)$. Natomiast dla Kummera [Kumm] ciało $Q(\varepsilon_p)$, p – liczba pierwsza, to podstawowy obiekt do badań nad Wielkim Twierdzeniem Fermata. Jednak w żadnej ze swoich prac nie używa specjalnej nazwy dla obiektu, którym się posługuje. Liczby, których używał nazywa Kummer po prostu: *n-ten Einheitswurzeln gebildeten complexen Zahlen.* W 1847 Kummer zauważa, że jeżeli λ jest liczbą pierwszą, $\alpha^\lambda = 1$, $\alpha \neq 1$, to każdy element ciała $Q(\alpha)$ ma postać

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_{\lambda-2}\alpha^{\lambda_2},$$

gdzie współczynniki są wymierne. Kummera interesuje jednak przede wszystkim pierścień $\mathbf{Z}[\alpha]$. Lamé w błędnym dowodzie Wielkiego Twierdzenia Fermata przyjął podświadomie, że $\mathbf{Z}[\alpha]$ jest pierścieniem z jednoznacznością rozkładu na czynniki pierwsze. Do wyniku tego przyznawał się Liouville aż do chwili, gdy okazało się, że jest to wynik fałszywy. Kummer, próbując uratować dowód Lamé, a właściwie ideę tego dowodu, stworzył liczby idealne, badając systematycznie ciała cyklotomiczne.

Dalszych przykładów ciał dostarczył Kronecker [Kron 1], zajmując się ciałami funkcji wymiernych zmiennych $\mathcal{R}'$, $\mathcal{R}''$, $\mathcal{R}'''$, ..., które oznaczał $(\mathcal{R}', \mathcal{R}'', \mathcal{R}''' \ldots)$ i nazywał *Rationalitäts-Bereich.*

Kronecker, naśladując w jakimś stopniu konstrukcję Galois ciał $GF(p^n)$, podał ogólną konstrukcję ciała, w którym dany wielomian nieprzywiedlny f o współczynnikach z ciała K ma pierwiastek. Konstruuje mianowicie pierścień ilorazowy $K[X]/(f)$, zauważając, że otrzymujemy ciało, w którym f ma pierwiastek. Na ten sam temat ukazała się w 1847 praca Cauchy'ego [Cauc]. Najważniejszym rezultatem tej pracy była konstrukcja ciała C liczb zespolonych jako pierścienia $\mathbf{R}[X]/(X^2+1)$, o czym już wspominaliśmy.

3. Pierwsze definicje ciała

Pojęcie ciała ukształtowało się w pracach Kummera, Kroneckera i Dedekinda. Jedną z pierwszych prób zdefiniowania ciała można znaleźć w książce Hankela [Hank]; nie wywarła ona jednak większego wpływu na rozwój teorii ciał.

Pierwszą definicję ciała podał Dedekind w X Suplemencie do wykładów Dirichleta z teorii liczb w 1871 [Dede 3].
Dedekind pisał tam:
Unter einem Körper wollen wir jedes System von unendlich vielen reellen oder komplexen Zahlen verstehen, welches in sich so abgeschlossen und vollständig ist, daß die Addition, Subtraktion, Multiplikation und Division von je zwei dieser Zahlen immer wieder eine Zahl desselben Systems hervorbringt.
Jak widać, mimo pełnej precyzji, definicja ta jest dość ograniczona.
W szczególności nie obejmuje ona obiektów już znanych, takich jak ciała Galois czy też ciała funkcji wymiernych, którymi posługiwał się Kronecker. Jest to całkowicie zrozumiałe – Dedekind zajmował się w tym czasie arytmetyką ciał liczbowych. Różnica pomiędzy definicją ciała u Dedekinda i Kroneckera polega na tym, że Dedekind używa aksjomatów, a Kronecker podaje postać elementów. Początkowo Dedekind rozpatrywał jedynie ciała przemienne. Później, w 1885 dopuścił w definicji nieprzemienność mnożenia, rozważając skończenie wymiarowe algebry z dzieleniem nad danym ciałem [Purk 1].

Tematyką tą zajmował się w tym czasie także Frobenius. Wykładowi idei Kroneckera poświęcona jest praca Hancocka [Hanc] z 1901.

4. Abstrakcyjne pojęcie ciała – aksjomatyzacja

Ogólną definicję ciała podał Weber w 1893 [Webe 1]. W jego dziele [Webe 2] prócz definicji ciała podana jest też definicja grupy i pierścienia w formie niewiele odbiegającej od definicji dziś używanych.

Weber [Webe 1] definiuje ciało jako zbiór z dwoma działaniami (*Zwei Arten der Compositionen*), dodawaniem i mnożeniem. Oba działania są przemienne, zbiór jest grupą względem dodawania, a ponadto

$\alpha)$ $\quad a(-b) = -ab,$

$\beta)$ $\quad a(b+c) = ab + ac,$

$\gamma)$ $\quad (-a)(-b) = ab,$

$\quad ab = ac$ implikuje $b = c$ lub $a = 0.$

Równanie $ab = c$ ma (jedyne) rozwiązanie dla $b \neq 0$.
Znamiennym jest, że nie żąda łączności mnożenia. Na str. 528 (loc. cit.) Weber

wskazuje na możliwość uogólnienia tego pojęcia:
Man könnte an verschiedene Erweiterungen des Körperbegriffs denken. Man könnte z. B. mehr als eine Ausnahme zulassen, so dass ein Product Null werden kann, auch wenn keiner seiner Factoren Null ist.
Definicja Webera trafiła do jego podręcznika ([Webe 2], tom 1, wyd. II, str. 491).

Początek XX stulecia przynosi ostateczne sformułowanie abstrakcyjnego pojęcia ciała. Stworzona przez Sylvestera w latach osiemdziesiątych XIX wieku szkoła algebraików w John Hopkins University, jak też szkoła Benjamina Peirce'a w Harvardzie [Par] prowadzą intensywne badania w zakresie algebry. Wyniki tych prac publikują w nowo założonym czasopiśmie *Transactions of the American Mathematical Society*. Wymieńmy tu kilku ważniejszych autorów: Dickson ([Dick 2], [Dick 3], [Dick 4]), Huntington ([Hunt 1]–[Hunt 3]), Wedderburn ([Wedd 1]) i inni.

A oto definicja Dicksona z 1903 roku ([Dick 2]).
A set of elements with two rules of combination denoted by $\circ$ and $\square$ is called a field if the following nine postulates hold:
1. if a and b belong to the set, then $a \circ b$ belongs to the set.
2. $a \circ b = b \circ a$, whenever $a \circ b$ and $b \circ a$ belong to the set.
3. $(a \circ b) \circ c = a \circ (b \circ c)$, whenever $a \circ b$, $b \circ c$, $(a \circ b) \circ c$, and $a \circ (b \circ c)$ belong to the set.
4. For any two elements a and b of the set, there exists in the set an element x such that $(a \circ x) \circ b = b$.
5. If a and b belong to the set, then $a \square b$ belongs to the set.
6. $a \square b = b \square a$, whwnever $a \square b$ and $b \square a$ belong to the set.
7. $(a \square b) \square c = a \square (b \square c)$, whenever $a \square b$, $b \square c$, $(a \square b) \square c$, and $a \square (b \square c)$ belong to the set.
8. For any two elements a and b of the set, such that * $c \square a \neq a$ for at least one element c of the set, there exists in the set an element x such that $(a \square x) \square b = b$.
9. $a \square (b \circ c) = (a \square b) \circ (a \square c)$, whenever $b \circ c$, $a \square c$, $a \square (b \circ c)$, and $(a \square b) \circ (a \square c)$ belong to the set.

---

* Another definition is obtained by replacing 8 by the postulate: For any two elements a, b, such that $c \circ a \neq c$ for at least one element c, there exists an element x such that $(a \square x) \square b = b$.

Nietrudno zauważyć, że działanie $\circ$ to dodawanie, a $\square$ – mnożenie w ciele. Jak widać, definicja ta różni się istotnie od definicji dziś stosowanych, nie tylko symboliką, ale i poszczególnymi aksjomatami. Dickson [Dick 2] podaje też uproszczoną aksjomatykę, definiując ciało, jak poprzednio, przy pomocy aksjomatów 1, 2, 3, 5, 6, 7, 9, zastępując 4 przez
"4′. There exists in the set an element z such that $z \circ b = b$ for every element b.",
a 8 przez
"8′. There exists in the set an element u such that $u \square b = b$ for every element b.",
a następnie dowodzi, że podane aksjomaty są niezależne.

Definicja Huntingtona [Hunt 1] jest prostsza, aniżeli definicja Dicksona. Huntington definiuje ciało następująco:
"A class in which the rules of combination $\oplus$ and $\odot$ are so defined as to satisfy any one of the eight sets of postulates given below shall be called a field (Körper)‡ with respect to $\oplus$ and $\odot$. (A field may be thought of, briefley, as any assemblage on which the rational operations of algebra can be performed.)"

"The simplest definition of a field is that supplied by the first set, which contains only seven postulates A1, A2, A3, M1, M2, M3, D."
"A1. If a, b and $a \oplus b$ belong to the class, then $a \oplus b = b \oplus a$.
A2. If $a, b, c, a \oplus b, b \oplus c$ and $a \oplus (b \oplus c)$ belong to the class, then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

A3. For every two elements a and b ($a = b$ or $a \neq b$) there is an element x such that $a \oplus x = b$."

"M1. If a, b and $b \odot a$ belong to the class, then $a \odot b = b \odot a$.

M2. If $a, b, c, a \odot b, b \odot c$ and $a \odot (b \odot c)$ belong to the class, then $(a \odot b) \odot c = a \odot (b \odot c)$.

M3. For every two elements a and b ($a = b$ or $a \neq b$) provided $a \oplus a \neq a$ and $b \oplus b \neq b$, there is an element y such that $a \odot y = b$.

"D. If $a, b, c, b \oplus c, a \odot b, a \odot c$ and $(a \odot b) \oplus (a \odot c)$ belong to the class, then $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$."

Huntington definiuje podobne warunki A1'-A4', M1'-M4', D', M_0, a następnie formułuje osiem różnych definicji ciała, zbliżonych do przytoczonej.
W późniejszej pracy [Hunt 2] Huntington podaje uproszczenie tej definicji. Definiuje ciało jako zbiór co najmniej dwuelementowy, z dwoma działaniami, dodawaniem i mnożeniem, takimi, że dodawanie jest łączne, przemienne, a równanie $a + x = b$ jest rozwiązalne dla dowolnych a, b mnożenie jest łączne, przemienne i dla dowolnych a, b takich, że $a + a \neq a$, równanie $ay = b$ ma rozwiązanie.

Jest to więc definicja, jaką i dziś można znaleźć w podręcznikach.

Wstępny etap rozwoju teorii ciał zamyka fundamentalna praca Steinitza [Stei] z 1910. Steinitz definiuje charakterystykę ciała (*die Charakteristik*), podciało proste (*die Primkörper*), rozszerzenie algebraiczne, przestępne, ciało doskonałe (*vollkommene*) i niedoskonałe (*unvollkommene*). Następnie przytacza za Kroneckerem pojęcie *ciała rozkładu wielomianu* i pojęcie *ciała algebraicznie domkniętego*. Zbiór S z działaniem binarnym nazywa *systemem kompozycyjnym*, a następnie definiuje *izomorfizm* takich systemów. Wprowadza pojęcie *pierścienia całkowitego (die Integritätsbereich)* i jego ciało ułamków. Opisuje pojedyncze rozszerzenia algebraiczne i przestępne ciał. Nieco wcześniej, bo już w 1871 Dedekind wprowadził pojęcie liniowej niezależności w ciałach. Dedekind nie cytuje *Ausdehnungslehre* Grassmanna, gdzie po raz pierwszy pojawiło się to pojęcie w ogólnej, choć niedoskonałej postaci. Praca Dedekinda [Dede 3] zawiera też pojęcie bazy ciała i stopnia rozszerzenia. W odnalezionym w latach siedemdziesiątych XX wieku rękopisie wykładów Dedekinda z roku akademickiego 1857/58 znajduje się, później zapomniane, twierdzenie o liniowej niezależności (nad K) automorfizmów ciała K[Purk 2]. Twierdzenie to odegrało dużą rolę w uproszczeniu teorii Galois, dokonanym przez Emila Artina w latach dwudziestych bieżącego stulecia. Steinitz w cytowanej pracy przytacza część wyników Dedekinda. Na ogół dowody Steinitza są prostsze niż u Dedekinda. Ponadto Steinitz definiuje rozszerzenia normalne. Definiuje też abstrakcyjne różniczkowanie pierścienia wielomianów $F[X]$ nad ciałem F. Ciało F nazywa doskonałym, jeżeli dla każdego wielomianu $f \in F[X]$, jeżeli f ma krotne pierwiastki w odpowiednim rozszerzeniu ciała F, to f jest przywiedlny nad F. Następnie dowodzi, że wszystkie ciała charakterystyki zero są doskonałe, a ciało F charakterystyki $p \neq 0$ jest doskonałe, wtedy i tylko wtedy, gdy dla każdego $a \in F$ jest $a^{1/p} \in F$.

Dowód twierdzenia Abela o elemencie pierwotnym, podany przez Steinitza, można dziś znaleźć w każdym podręczniku algebry: jeżeli α, β są elementami algebraicznymi nad ciałem K, to $K(\alpha, \beta) = K(\gamma)$, gdzie $\gamma = \alpha + \mu\beta$, a element $\mu \in K$ wybieramy tak, aby

$$\mu \neq \frac{\alpha_i - \alpha_j}{\beta_k - \beta_l}$$

dla dowolnych wskaźników i, j, k, l, gdzie $\alpha_1, \alpha_2, \ldots$ są pierwiastkami wielomianu minimalnego elementu α i podobnie dla β. Steinitz dowodzi, że algebraiczne domknięcie dowolnego ciała istnieje i jest jedyne. W końcowej części pracy definiuje algebraiczną zależność elementu od zbioru S, wprowadza wymiar przestępny ciała (*der Transzendenzgrad der Körper*) i dowodzi, że pojęcie to nie zależy od wyboru bazy przestępnej ciała. W dowodach twierdzeń o istnieniu algebraicznego domknięcia ciała i cytowanym twierdzeniu, że wymiar przestępny jest dobrze zdefiniowany, posługuje się indukcją pozaskończoną.

Definicję ciała zbliżoną do obecnie używanej oraz podstawowe własności ciał można znaleźć w pracy przeglądowej Wedderburna [Wedd 2] z 1923.

Książki, które ukazały się w połowie lat dwudziestych, cytują znaną nam definicję ciała. Np. Beck [Beck] definiuje ciało jako zbiór z dwoma działaniami, dodawaniem i mnożeniem nieco inaczej, niż dziś. Zbiór K nazywa się ciałem, jeżeli spełnione są następujące warunki:

"G1. Zu zwei Elementen A und B des Systems gibt es stets ein einziges Element $A+B$ des Systems.
G2. Es ist $A+(B+C)=(A+B)+C$.
G3. Aus $A+C=B+C$ folgt $A=B$.
G4. Die beiden Gleichungen $A+X=B$ und $Y+A=B$ lassen sich beide eindeutig im System auflösen.

Die Kommutativitat der "Addition" wird also nicht gefordert."

"H1. Zu zwei Elementen A und B des Systems gibt es stets ein einziges Element $A\cdot B$ im System.
H2. Es ist $A\cdot(B\cdot C)=(A\cdot B)\cdot C$.
H3. Aus $A\cdot C=B\cdot C$ folgt $A=B$, falls $C\neq 0$,
aus $C\cdot A=C\cdot B$ folgt $A=B$, falls $C\neq 0$.
H4. Für $B\neq 0$ sind die beiden Gleichungen $B\cdot X=A$ und $Y\cdot B=A$ eindeutig im System lösbar.
IX. Es ist $A\cdot B=B\cdot A$.
X. Es ist $A\cdot(B+C)=A\cdot B+A\cdot C$."

"Ein System von Element, welches den zehn Axiomen G1-4, H1-4, IX, X genügt, heiβt ein Körper."

Beck dowodzi (loc. cit. str. 174), że z podanej definicji wynika już przemienność dodawania.

5. Powstanie i rozwój teorii ciał skończonych

Jak zostało to już powiedziane we Wstępie, ciała reszt modulo p pojawiły się po raz pierwszy w *Disquisitiones Arithmeticae* Gaussa w 1801 w niejawnej postaci. Pierwsze konstrukcje ciał skończonych zawdzięczamy Galois [Galo]. Traktował je jako analogony liczb zespolonych. Między innymi rozważał ciała złożone z elementów postaci $a+ib$, gdzie $i^2=-1$; $a,b\in\mathbf{F}_p$ (rzecz jasna, $p\not\equiv 1 \pmod 4$). Wykład Galois jest bardzo elegancki.

Książka J. A. Serreta *Cours d'Algèbre supérieure*, której pierwsze wydanie ukazało się w 1849 zawiera już wiele informacji o ciałach skończonych [Więş 1]. Serret znalazł wzór na liczbę $N_n(p)$ unitarnych nieprzywiedlnych wielomianów stopnia n o współczynnikach z ciała $\mathbf{F}_p$ reszt modulo p:

$$N_n(p)=\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d},$$

gdzie μ jest funkcją Möbiusa (Serret nie używał funkcji Möbiusa). Ze wzoru tego, stosując rozwinięcie funkcji wykładniczej i logarytmicznej w szereg potęgowy, wyprowadził następujące oszacowanie

$$\frac{\varphi(n)}{n-1}\frac{p^n-p}{n}\leq N_n(p)\leq\frac{p^n-p}{n}.$$

Tematyka ciał skończonych przewinęła się przez prace C. G. J. Jacobiego, M. Lebesque'a w połowie XIX wieku, P. Pépina w drugiej połowie XIX wieku, żeby wymienić tylko kilku badaczy.

Kronecker i Mathieu widzieli już w 1858 ([Więş 3]), że grupa $PSL(2,\mathbf{F}_7)$ rzędu 168 jest prosta. Miało to znaczenie nie tylko dla teorii grup. Zwróciło też uwagę na rolę ciał skończonych w matematyce.

Jak pisze Huntington [Hunt 1]:

"The theorem, that every finite field is necesarily a Galois field of order of

a power of a prime was first proved by E. H. MOORE." ([Moor], str. 211; także [Dick 1], §18).

Książka Dicksona [Dick 1] z 1901 roku zawiera już systematyczny wykład teorii ciał skończonych. Badania swoje kontynuuje w późniejszych pracach (por. np. [Dick 5], [Dick 6]).

W 1905 ukazała się drukiem słynna praca Wedderburna [Wedd 1], w której udowodnił on, że każde ciało skończone jest przemienne (jeżeli w definicji ciała nie postulować przemienności mnożenia). Z twierdzenia tego wynika w szczególności, że *na każdej skończonej płaszczyźnie Desarguesa prawdziwe jest twierdzenie Pappusa.* Co ciekawsze, oryginalny dowód Wedderburna przetrwał do dziś w podręcznikach algebry.

Na początku XX wieku zaczęto klasyfikować ciała skończone. Bussey [Buss 1] wyznaczył w 1905 wszystkie ciała $q = p^n$ elementowe, dla których $q \leq 169$, a już w 1909 [Buss 2] rozszerzył swój wynik do $q \leq 1000$. Podobne wyniki uzyskał Neikirk [Neik].

Tematyka ciał skończonych stała się dziś bardzo ważna, m. in. dzięki licznym zastosowaniom, np. w teorii kodów korygujących błędy i, ogólniej, w informatyce.

6. Różne działania w tym samym ciele

Pierwsze przykłady działań w ciele, różnych od działań definiujących ciało, podał Huntington [Hunt 3] w 1905. Np. jeżeli K jest ciałem liczb zespolonych, to jest ono ciałem także względem działań zdefiniowanych następująco:

$$a \oplus b = a + b - h,$$
$$a \odot b = kab - hk(a+b) + h(1+hk),$$

gdzie h, k są ustalonymi liczbami, $k \neq 0$ (loc. cit., str. 225). Oczywiście K może być dowolnym ciałem.
Jak pisze Huntington (loc. cit., str. 226):
"This system (6), which includes the preceding system as special cases, was suggested to me by Professor C. L. BOUTON, who had noticed that the general formulae

$$a \oplus b = f[f^{-1}(a) + f^{-1}(b)],$$

and

$$a \odot b = f[f^{-1}(a) \times f^{-1}(b)],$$

in which f and its inverse f^{-1} are single-valued functions, provide a pair of operations which satisfy, in general, the postulates for a field with respect to $\oplus$ and $\odot$. In the present examples

$$f(x) = \frac{\alpha x + \beta}{\gamma x + \delta} \quad (\alpha\delta - \beta\gamma \neq 0)."$$

Tematyka ta powróciła w pracy Bella z 1930 roku [Bell 1], w której wprost, nie korzystając z wyżej opisanej konstrukcji, odcinek $(0,1)$ przekształcony został w ciało względem następujących działań:

$$\alpha \oplus \beta = \frac{1}{2} - \frac{1}{\pi}\operatorname{arctg}(\operatorname{ctg}\pi\alpha + \operatorname{ctg}\pi\beta)\ ,$$
$$\alpha \odot \beta = \frac{1}{2} - \frac{1}{\pi}\operatorname{arctg}(\operatorname{ctg}\pi\alpha \cdot \operatorname{ctg}\pi\beta)\ .$$

W ogólnej konstrukcji Boutona wystarczy zdefiniować

$$f(\alpha) = \frac{1}{2} + \frac{1}{\pi}\operatorname{arctg}\alpha.$$

Inną historyczną ciekawostką związaną z omawianym tematem jest jedna z pierwszych prac Wienera [Wien] z 1920 roku. W pracy tej Wiener definiuje ciało jako zbiór K z jedną operacją binarną @. Definicja Wienera jest zawiła i długa – nie będziemy więc jej przytaczać. Wiener definiuje nowe działania: dodawanie $\oplus$ i mnożenie $\odot$ za pomocą operacji @, a następnie dowodzi, że K jest ciałem względem tych działań. Np., jeżeli przyjąć $x \,@\, y = 1 - \frac{x}{y}$ w ciele $(K, +, \cdot)$, to

dodawanie i mnożenie można wyrazić w terminach operacji @. Na tym polega jego pomysł.

W końcowej części pracy Wiener zauważa, że w podobny sposób można zdefiniować algebrę zespoloną przy pomocy operacji $*$, przyjmując

$$x * y = 1 - \overline{x}(\overline{y})^{-1}.$$

Wiener stwierdza, że aksjomatyzacja taka jest możliwa, choć technicznie trudna.

Omawiana tematyka powróciła w latach sześćdziesiątych bieżącego stulecia, w nieco innym kontekście i sformułowaniu dalekim od teorii ciał.

Bibliografia

[Arga 1] J. R. Argand, *Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques*, 1806.

[Arga 2] –, –, *Annales de Mathematiques Pures et Appliquées* 4 (1813), 133–148.

[Balt] R. Baltzer, *Über die Einführung der complexen Zahlen*, Journal für die reine und angewandte Mathematik 94 (1883), 87–92.

[Beck] H. Beck, *Einführung in die Axiomatik der Algebra*, Walter de Gruyter, Berlin, 1926.

[Bell] E. T. Bell, *The real unit segment as a number field*, American Journal of Mathematics 52 (1930), 548–550.

[Bern 1] B. A. Bernstein, *The complete existential theory of Hurwitz's postulates for abelian groups and fields*, Bulletin of the American Mathematical Society 28 (1922), 397–399.

[Bern 2] *On the complete independence of Hurwitz's postulates for abelian groups and fields*, Annals of Mathematics, (2) ser., 23 (1923), 313–316.

[Bôch] M. Bôchner, *Simplification of Gauss's third proof that every algebraic equation has a root*, American Journal of Mathematics 17 (1895), 266–268.

[Buss 1] W. H. Bussey, *Galois field tables for* $p^n \leq 169$, Bulletin of the American Mathematical Society 12 (1905), 22–38.

[Buss 2] –, *Tables of Galois fields of order less than* 1,000, ibidem 16 (1909), 188–206.

[Cauc] A. L. Cauchy, *Mémoire sur une nouvelle théorie des imaginaires, et sur les racines symboliques des équations et de équivalences*, C. R. Acad. Sci. Paris 24 (1847), 1120 (Oeuvres de Cauchy 1° s., T. X, 312–323; No 369).

[Dede 1] R. Dedekind, *Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Prinzahl-Modulus*, Journal für die reine angewandte Mathematik 54 (1857), 1–26.

[Dede 2] –, *Beweis für die Irreductibilität der Kreistheilungs-Gleichungen*, ibidem 54 (1957), 27–30.

[Dede 3] –, *Über die Komposition der binären quadratischen Formen, Supplement X zur zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie*, Braunschweig 1871.

[Ded-Web] R. Dedekind, H. Weber, *Theorie der algebraischen Functionen einer Veränderlichen*, Journal für die reine und angewandte Mathematik 92 (1882), 181–250.

[Dick 1] L. E. Dickson, *Linear groups (with an exposition of the Galois field theory)*, B. G. Teubner, Leipzig, 1901.

[Dick 2] –, *Definition of a field by independent postulates*, Transactions of the American Mathematical Society 4 (1903), 13–20.

[Dick 3] –, *Definitions of a linear associative algebra by independent postulates*, ibidem 4 (1903), 21–30.

[Dick 4] –, *Definitions of a group and a field by independent postulates*, ibidem 6 (1905), 198–204.

[Dick 5] –, *On the theory of equations in a modular field*, Bulletin of the American Mathematical Society 13 (1906), 8–10.

[Dick 6] –, *Criteria for the irreducibility of functions in a finite field*, ibidem 13 (1906), 1–8.

[E–N–P] H. Edwards, O. Neumann, W. Purkert, *Dedekinds "Bunte Bemerkungen" zu Kronecker "Grundzüge"*, Archive for the History of Exact Sciences 27 (1982), No 1, 49–85.

[Fran] J. F. Français, *Nouveaux principes de géométrie de position, et interprétation géometrique des symboles imaginaires*, Annales de Mathématiques Pures et Appliquées 4 (1813), 61–71.

[Galo] E. Galois, *Ecrits et Mémoires Mathématiques*, Gauthier-Villars, Paris 1962.
[Gaus] C. F. Gauss, *Disquisitiones Arithmeticae*, Lipsiae 1801.
[Hami] W. R. Hamilton, *Preface to 'Lectures on Quaternions'*, Dublin 1853. (The Mathematical Papers of Sir William Rowan Hamilton, vol. III, Algebra; Edited for the Royal Irish Academy by H. Halberstam and R. E. Ingram, Cambridge University Press 1967, VI, 117–155).
[Hanc] H. Hancock, *Mémoire sur les systèmes modulaires de Kronecker*, Annales Scientifiques de l'École Normale Supérieure, Supplément au Tome XVIII, année 1901, 1–115.
[Hank] H. Hankel, *Theorie der complexen Zahlensysteme, insbesondere der gemeinen imaginären Zahlen und der Hamilton'schen Quaternionen nebst ihrer geometrischen Darstellung*, Leipzig, 1867.
[Hunt 1] E. V. Huntington, *Definitions of a field by sets of independent postulates*, Transactions of the American Mathematical Society 4 (1903), 31–37.
[Hunt 2] –, *Note on the definitions of abstract groups and fields by sets of independent postulates*, ibidem 6 (1905), 181–197.
[Hunt 3] –, *A set of postulates for ordinary complex algebra*, ibidem 6 (1905), 209–229.
[Hurw] W. A. Hurwitz, *Postulate sets for abelian groups and fields*, Annals of Mathematics, (2) ser., 15 (1913).
[Kron 1] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*,
Journal für die reine und angewandte Mathematik 92 (1882), 1–122.
[Kron 2] –, *De unitatibus complexis*, ibidem 93 (1882), 1–52.
[Kumm] E. Kummer, *Zur Theorie der complexen Zahlen*, ibidem 35 (1847), 319–325.
[Moor] E. H. Moore, *Mathematical Papers read at the Chicago Congress of 1893.*
[Neik] L. I. Neikirk, *A geometric representation of the Galois field*, Bulletin of the American Mathematical Society 14 (1908), 323–325.
[Pars] K. H. Parshall, *America's first school of mathematical research: James Joseph Sylvester at the John Hopkins University 1876–1883*, Archive for the History of Exact Sciences 38 (1988), No 2, 153–196.
[Purk 1] W. Purkert, *Zur Genesis des abstrakten Körperbegriffs*, NTM-Schriftenreihe Geschichte, Naturwissenschaften, Technik und Medizin, Leipzig 10 (1973), No 2, 8–20.
[Purk 2] –, *Ein Manuskript Dedekinds über Galois-Theorie*, ibidem 13 (1976), No 2, 1–16.
[Stei] E. Steinitz, *Algebraische Theorie der Körper*, Journal für die reine und angewandte Mathematik 137 (1910), 167–309.
[Webe 1] H. Weber, *Die allgemeine Grundlagen der Galois'schen Gleichungstheorie*, Mathematische Annalen 43 (1893), 521–549.
[Webe 2] –, *Lehrbuch der Algebra, 3 Bde*, Braunschweig, Druck und Verlag von Friedrich Vieweg und Sohn, 1895–1896; II wyd. 1898.
[Wedd 1] J. H. M. Wedderburn, *A theorem on finite algebras*, Transactions of the American Mathematical Society 6 (1905), 349–352.
[Wedd 2] –, *Algebraic fields*, Annals of Mathematics 24 (1923), 237–264.
[Wien] N. Wiener, *A set of postulates for fields*, Transactions of the American Mathematical Society 21 (1920), 237–246.
[Więś 1] W. Więsław, *O nauczaniu algebry w XIX i XX wieku*, (preprint, 1988), 23 strony.
[Więś 2] –, *Drogi i manowce początków algebry*, Matematyka, Społeczeństwo, Nauczanie 15 (VII 1995), 16–26.
[Więś 3] –, *Początki teorii grup skończonych*, Matematyka, Społeczeństwo, Nauczanie 16 (I 1996), 19–33.
[Więś 4] –, *Liczby i geometria*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1996.