§ 22. Разширения на полета

В този и следващия параграф ще разглеждаме само числови полета, т. е. подполета на полето на комплексните числа $\mathbb{C}$.

Нека F е поле. Ще казваме, че едно число $\alpha \in \mathbb{C}$ е *алгебричен елемент над* F, ако α е корен на ненулев полином с коефициенти от F. Ненулевия полином от най-ниска степен, на който α е корен и който е унитарен (със старши коефициент 1) ще наричаме *минимален полином на* α *над* F (по-долу ще видим, че всеки алгебричен елемент притежава единствен минимален полином). Най-често минималния полином на α над F ще бележим с f_α. Степента на f_α ще наричаме *степен на алгебричност на* α *над* F и ще я бележим с $\deg_F \alpha$. Ще казваме, че два алгебрични над F елемента са *спрегнати над* F, ако минималните им полиноми над F съвпадат. Ако едно число α не е алгебрично над F, ще казваме, че то е *трансцендентно над* F. (По-долу ще стане ясно, че досадното повторение на израза "над F" в горните определения е съществено.)

П р и м е р и. 1. Ако F е поле и α е число, то $\alpha \in F \iff \deg_F \alpha = 1$. В този случай $f_\alpha(x) = x - \alpha \in F[x]$.

2. Числото $\sqrt{2}$ е алгебрично над $\mathbb{Q}$ и минималният полином на $\sqrt{2}$ над $\mathbb{Q}$ е $f(x) = x^2 - 2$. Така $\deg_{\mathbb{Q}} \sqrt{2} = 2$. В същото време $\sqrt{2}$ е алгебрично и над $\mathbb{R}$, но минималният му полином над $\mathbb{R}$ е $f(x) = x - \sqrt{2}$ и $\deg_{\mathbb{R}} \sqrt{2} = 1$. По аналогичен начин "се държи" и числото i съответно над $\mathbb{R}$ и $\mathbb{C}$.

3. Числото π е реално и значи е алгебрично над $\mathbb{R}$ от степен на алгебричност, равна на 1. В същото време π е трансцендентно над полето на рационалните числа $\mathbb{Q}$ (този факт е добре известен, макар и нетривиален).

Твърдение 1. *Нека* F *е поле и* α *е алгебричен над* F *елемент. Тогава:*

а) *съществува минимален полином* f_α *на* α *над* F *и той е единствен;*

б) *ако* $g \in F[x]$, *то* $g(\alpha) = 0 \iff f_\alpha \mid g$;

в) *полиномът* f_α *е неразложим над* F;

г) *полиномът* f_α *няма кратни корени.*

Д о к а з а т е л с т в о. а) Непосредствено се проверява, че множеството $I = \{g \in F[x] \mid g(\alpha) = 0\}$ е ненулев идеал в полиномиалния пръстен $F[x]$. Тъй като всеки идеал в $F[x]$ е главен, то $I = (f) = \{fh | h \in F[x]\}$ за подходящ полином f; при това можем да подберем f да бъде унитарен. Така полиномът f е ненулев, унитарен, $f(\alpha) = 0$ и f е от най-ниска степен с тези свойства (действително, всеки друг полином, на който α е корен, се съдържа в I и значи е кратен на f). Следователно f е търсеният минимален полином f_α на α над F. Нека накрая g също е минимален полином на α над F. От $g(\alpha) = 0$ следва $g \in I$, т. е. $f \mid g$. Но f и g са унитарни и с равни степени (защото са минимални полиноми на α над F). Следователно $g = f$, т. е. минималният полином на α над F е единствен.

б) В означенията от а) имаме: $g(\alpha) = 0 \iff g \in I \iff f_\alpha \mid g$.

в) Ако допуснем, че f_α е произведение на два полинома от по-ниска степен с коефициенти от F, то α би бил корен на поне един от тях, което противоречи на минималността на f_α. Следователно f_α е неразложим над F.

г) Твърдението следва от факта, че всеки неразложим полином f с числови коефициенти няма кратни корени. Действително, в противен случай би следвало, че f не е взаимно прост с производната си f' и тогава (тъй като f е неразложим) $f \mid f'$, което е невъзможно.

Задача 1. *Нека F е поле и $f \in F[x]$ е неразложим над F унитарен полином. Да се докаже, че f е минималният полином на всеки от корените си, в частност корените на f са спрегнати над F. Така спрегнатите на един алгебричен над F елемент α са кореният на минималния му над F полином f_α.*

* * *

Ако едно поле F е подполе на поле K, ще казваме, че K е *разширение* на F и ще пишем $F \leqq K$ (или $F < K$, ако включването е строго). Полето K може да се разглежда по естествен начин като линейно пространство над F. Размерността $\dim_F K$ на това линейно пространство ще наричаме *степен на K над F* и ще я бележим с $[K : F]$. Ако $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, с $F(\alpha_1, \ldots, \alpha_n)$ ще бележим сечението на всички подполета на $\mathbb{C}$, съдържащи F и $\alpha_1, \ldots, \alpha_n$ (т. е. минималното подполе на $\mathbb{C}$, съдържащо F и $\alpha_1, \ldots, \alpha_n$). С непосредствена индукция по n от определението се получава, че $F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = \cdots = F(\alpha_1) \ldots (\alpha_{n-1})(\alpha_n)$.

Определение. *Ще казваме, че разширението $F \leqq K$ е:*

— алгебрично разширение (АР), ако всеки елемент от K е алгебричен над F;

— крайно разширение (КР), ако $[K : F] = \dim_F K < \infty$;

— крайно породено алгебрично разширение (КПАР), ако $K = F(\alpha_1, \ldots, \alpha_n)$, където $\alpha_1, \ldots, \alpha_n$ са алгебрични над F елементи;

— просто алгебрично разширение (ПАР), ако $F = F(\theta)$, където θ е алгебричен над F елемент.

П р и м е р и. 1. Едно разширение K на F съвпада с F точно когато $[K : F] = 1$.

2. Полето $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ е просто алгебрично разширение на $\mathbb{Q}$ и $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (числата 1 и $\sqrt{2}$ са базис на $\mathbb{Q}(\sqrt{2})$ над $\mathbb{Q}$). Полето $\mathbb{C} = \mathbb{R}(i)$ също е просто алгебрично разширение на $\mathbb{R}$ и $[\mathbb{C} : \mathbb{R}] = 2$. Разширението $\mathbb{R} < \mathbb{C}$ е и алгебрично, защото всяко комплексно число е корен на полином с реални коефициенти (от степен, ненадминаваща 2). Разширението $\mathbb{Q} < \mathbb{R}$ не е алгебрично.

3. Нека F е поле, $f \in F[x]$ и $\alpha_1, \ldots, \alpha_n$ са кореният на f. Полето на разлагане на полинома f над F е $F(\alpha_1, \ldots, \alpha_n)$ и е крайно породено алгебрично разширение на F.

Твърдение 2. *Нека разширенията $F \leqq L$ и $L \leqq K$ са крайни. Тогава разширението $F \leqq K$ също е крайно и $[K : F] = [K : L][L : F]$.*

Д о к а з а т е л с т в о. Нека $[L : F] = n$ и $\alpha_1, \ldots, \alpha_n$ е базис на L над F. Аналогично, нека $[K : L] = m$ и $\beta_1, \ldots, \beta_m$ е базис на K над L. Непосредствено се проверява, че всевъзможните произведения $\alpha_i\beta_j$, $i = 1, \ldots, n$; $j = 1, \ldots, m$, образуват базис на K над F. Следователно $[K : F] = mn = [K : L][L : F]$.

Следствие 3. *Нека $F_1 \leqq F_2 \leqq \cdots \leqq F_{t-1} \leqq F_t$ е верига от полета и за всяко $i = 1, \ldots, t-1$ разширението $F_i \leqq F_{i+1}$ е крайно. Тогава разширението $F_1 \leqq F_t$ също е крайно и*

$$[F_t : F_1] = [F_t : F_{t-1}] \ldots [F_3 : F_2][F_2 : F_1].$$

Д о к а з а т е л с т в о т о се извършва с индукция по t, като се използва твърдение 2.

Теорема 4. *Нека F е поле и θ е алгебричен над F елемент от степен на алгебричност n. Тогава:*

а) *$F(\theta) = \{g(\theta) \mid g(x) \in F[x]\}$;*

б) *$F(\theta)$ е крайно разширение на F и $[F(\theta) : F] = n$, по-точно елементите $1, \theta, \ldots, \theta^{n-1}$ образуват базис на $F(\theta)$ над F.*

Д о к а з а т е л с т в о. Нека $f_\theta(x)$ е минималният полином на θ над F; $\deg f_\theta(x) = n$.

а) Да означим $K = \{g(\theta) \mid g(x) \in F[x]\}$. Ясно е, че $K \subseteq F(\theta)$. Ще докажем, че K е поле. Очевидно множеството K е затворено относно операциите събиране и умножение. Остава да проверим, че обратният на всеки ненулев елемент от K е също в K. Нека $0 \neq g(\theta) \in K$. Тъй като θ не е корен на полинома $g(x)$, то $f_\theta(x) \nmid g(x)$ и от неразложимостта над F на $f_\theta(x)$ следва, че $(g(x), f_\theta(x)) = 1$. Тогава съществуват полиноми $u(x), v(x) \in F[x]$, такива че $u(x)g(x)+v(x)f_\theta(x) = 1$. Като заместим x с θ и вземем предвид, че $f_\theta(\theta) = 0$, получаваме $u(\theta)g(\theta) = 1$. Следователно обратният елемент на $g(\theta)$ е $u(\theta) \in K$. И така, K е поле, съдържащо се в $F(\theta)$, но очевидно K съдържа F и θ и от минималността на $F(\theta)$ следва, че K съдържа $F(\theta)$. Следователно $F(\theta) = K$ и твърдението е доказано.

б) Елементите $1, \theta, \ldots, \theta^{n-1}$ са линейно независими над F: в противен случай θ е корен на ненулев полином от $F[x]$, чиято степен е по-малка от n, което е противоречие. Остава да проверим, че всеки елемент от K е тяхна линейна комбинация с коефициенти от F. Ако $\alpha \in K$, то от подусловие а) следва, че $\alpha = g(\theta)$ за подходящ полином $g(x) \in F[x]$. Нека $g(x) = f_\theta(x)q(x) + r(x)$, където $q(x), r(x) \in F[x]$ и $\deg r(x) < n = \deg f_\theta(x)$. Замествайки x с θ, получаваме $g(\theta) = r(\theta)$, т. е. $\alpha = r(\theta)$. Следователно $1, \theta, \ldots, \theta^{n-1}$ е базис на $F(\theta)$ над F и твърдението е доказано.

Задача 2. *Нека F е поле, θ е алгебричен над F елемент и f_θ е минималният полином на θ над F. Да се докаже, че $F(\theta) \cong F[x]/(f_\theta)$.*

У п ъ т в а н е. Приложете теоремата за хомоморфизмите за изображението $\varphi : F[x] \to F(\theta)$, дефинирано чрез равенството $\varphi(g(x)) = g(\theta)$.

Следствие 5. *Нека F е поле и $\alpha_1, \ldots, \alpha_n$ са алгебрични над F елементи. Тогава*

$$F(\alpha_1, \ldots, \alpha_n) = \{g(\alpha_1, \ldots, \alpha_n) \mid g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]\}.$$

Д о к а з а т е л с т в о т о се извършва с индукция по n, използвайки теорема 4 и равенството $F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.

§ 23. Еквивалентност на видовете разширения

Твърдение 1. *Всяко крайно разширение $F \leqq K$ е алгебрично разширение (съкратено пишем $(KP) \Longrightarrow (AP)$). При това степента на алгебричност над F на всеки елемент от K не надминава степента $[K : F]$ на разширението.*

Д о к а з а т е л с т в о. Нека $[K : F] = n$ и $\alpha \in K$. Елементите $1, \alpha, \ldots, \alpha^n$ са $n + 1$ на брой и значи са линейно зависими над F, т. е. съществуват числа $a_0, a_1, \ldots, a_n \in F$, не всички от които са равни на нула, и $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Това означава, че α е корен на ненулевия полином $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, като $\deg f \leqq n$. Следователно α е алгебричен елемент над F и степента на алгебричност на α над F не надминава $n = [K : F]$.

Твърдение 2. *Едно разширение $F \leqq K$ е крайно точно когато е крайно породено алгебрично разширение (т. е. $(KP) \Longleftrightarrow (KПАР)$).*

Д о к а з а т е л с т в о. Нека разширението $F \leqq K$ е крайно. Тогава то е алгебрично (твърдение 1) и ако $\alpha_1, \ldots, \alpha_n$ е базис на K над F, очевидно $K = F(\alpha_1, \ldots, \alpha_n)$, т. е. то е и крайно породено алгебрично разширение.

Нека сега $K = F(\alpha_1, \ldots, \alpha_n)$ е крайно породено алгебрично разширение. Да разгледаме веригата от полета

$$F \leqq F(\alpha_1) \leqq F(\alpha_1)(\alpha_2) \leqq \ldots \leqq F(\alpha_1)(\alpha_2)\ldots(\alpha_n) = F(\alpha_1, \ldots, \alpha_n).$$

Според теорема 4 от § 22 всяка "бръчка" от тази верига е крайно разширение и тогава според следствие 3 от § 22 полето $K = F(\alpha_1, \ldots, \alpha_n)$ също е крайно разширение на F.

Следствие 3. *Ако $F \leqq L$ и $L \leqq K$ са алгебрични разширения, то разширението $F \leqq K$ също е алгебрично.*

Д о к а з а т е л с т в о. Нека $\alpha \in K$. По условие елементът α е алгебричен над L и значи е корен на ненулев полином $f(x) = a_0x^n + \cdots + a_n \in L[x]$. Тогава α очевидно е алгебричен елемент и над полето $F(a_0, \ldots, a_n)$. От своя страна коефициентите $a_0, \ldots, a_n \in L$ са алгебрични над F. Тогава разширенията $F \leqq F(a_0, \ldots, a_n)$ и $F(a_0, \ldots, a_n) \leqq F(a_0, \ldots, a_n; \alpha)$ са крайно породени алгебрични разширения и значи са крайни. Следователно разширението $F \leqq F(a_0, \ldots, a_n; \alpha)$ също е крайно. Така α принадлежи на крайно, а значи и алгебрично разширение на F. Оказва се, че всеки елемент $\alpha \in K$ е алгебричен над F, т. е. K е алгебрично разширение на F.

Теорема 4 (теорема за примитивния елемент). *Всяко крайно породено алгебрично разширение $F \leqq K$ е просто алгебрично разширение (т. е. (КПАР)$\Longrightarrow$(ПАР); обратното е очевидно).*

Д о к а з а т е л с т в о. Нека $K = F(\alpha_1, \ldots, \alpha_n)$ е крайно породено алгебрично разширение на F. Ще докажем теоремата само при $n = 2$; в общия случай твърдението се доказва с непосредствена индукция по n.

И така, нека $K = F(\alpha, \beta)$ и α и β са алгебрични над F. Нека $f_\alpha, f_\beta \in F[x]$ са минималните полиноми над F съответно на α и β и $\alpha = \alpha_1, \ldots, \alpha_n$ са корените на f_α, а $\beta = \beta_1, \ldots, \beta_m$ са корените на f_β. Числата $\beta_1, \ldots, \beta_m$ са две по две различни, защото f_β няма кратни корени. Да означим

$$\gamma_{ij} = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}, \quad i = 1, \ldots, n;\ j = 2, \ldots, m.$$

Тъй като числата γ_{ij} са краен брой, съществува число $c \in F$ и $c \neq \gamma_{ij}$ за всяко $i = 1, \ldots, n$; $j = 2, \ldots, m$. Нека $\theta = \alpha + c\beta (= \alpha_1 + c\beta_1)$; θ е алгебричен елемент над F, понеже $F \leqq K$ е крайно, а значи и алгебрично разширение. Очевидно $F \leqq F(\theta) \leqq F(\alpha, \beta) = K$. Ще докажем, че $\alpha, \beta \in F(\theta)$ и тогава $K = F(\theta)$, с което теоремата ще бъде доказана.

Да означим $h(x) = f_\alpha(\theta - cx)$. Полиномът h е с коефициенти от полето $F(\theta)$. Имаме $h(\beta) = f_\alpha(\theta - c\beta) = f_\alpha(\alpha) = 0$. Следователно полиномите h и f_β имат общ корен β. Ако допуснем, че h и f_β имат друг общ корен, той може да бъде само някое от числата β_j, $j = 2, \ldots, m$. Но от $h(\beta_j) = f_\alpha(\theta - c\beta_j) = 0$ следва, че $\theta - c\beta_j = \alpha_i$ за някое $i = 1, \ldots, n$ и тогава (замествайки $\theta = \alpha_1 + c\beta_1$) получаваме, че $c = \dfrac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} = \gamma_{ij}$, което е противоречие с избора на c. Следователно h и f_β имат единствен общ корен β. При това коефициентите и на двата полинома лежат в полето $F(\theta)$. Тогава най-големият унитарен общ делител на h и f_β с коефициенти от полето $F(\theta)$ е полиномът $x - \beta$. Следователно $\beta \in F(\theta)$, а оттам и $\alpha = \theta - c\beta \in F(\theta)$. Теоремата е доказана.

Елементът θ от доказателството на теорема 4 се нарича *примитивен елемент* на разширението $F \leqq K$.

Резултатите, получени дотук, могат схематично да се запишат по следния начин:

$$\begin{array}{ccccc} (\text{КР}) & \overset{\text{Тв. 2}}{\Longleftrightarrow} & (\text{КПАР}) & \overset{\text{Т. 4}}{\Longleftrightarrow} & (\text{ПАР}) \\ {\scriptstyle \text{Тв. 1}}\Big\Downarrow & & & & \\ (\text{АР}) & & & & \end{array}$$

Освен това в края на параграфа ще видим, че не всяко алгебрично разширение е крайно разширение. В сила е обаче следният факт:

Твърдение 5. *Нека разширението $F \leqq K$ е алгебрично и съществува естествено число n, такова че степента на алгебричност над F на всеки елемент от K не надминава n. Тогава K е крайно разширение на F и $[K : F] \leqq n$.*

Д о к а з а т е л с т в о. Нека $\alpha \in K$ е елемент с максимална степен на алгебричност m; $m = \deg_F \alpha = [F(\alpha) : F]$. По условие $m \leqq n$. Да допуснем, че $F(\alpha) \lneqq K$. Тогава съществува елемент $\beta \in K \setminus F(\alpha)$ и от веригата $F \leqq F(\alpha) < F(\alpha, \beta)$ получаваме, че $[F(\alpha, \beta) : F] > [F(\alpha) : F] = m$. Нека θ е примитивен елемент на разширението $F < F(\alpha, \beta)$, т. е. $F(\alpha, \beta) = F(\theta)$. Тогава $\deg_F \theta = [F(\theta) : F] > m$, което противоречи на избора на α. Следователно $K = F(\alpha)$ и тогава $[K : F] = m \leqq n$.

* * *

Ще завършим този параграф със следната

Теорема 6. *Нека F е поле. Тогава:*

а) множеството $\overline{F}$ от всички алгебрични над F числа е поле;

б) полето $\overline{F}$ е алгебрически затворено.

Д о к а з а т е л с т в о. а) Нека $\alpha, \beta \in \overline{F}$. Елементите $\alpha \pm \beta$, $\alpha\beta$ и $\dfrac{\alpha}{\beta}$ (при $\beta \neq 0$) принадлежат на разширението $F(\alpha, \beta)$ на F, което е крайно породено алгебрично, следователно крайно (твърдение 2), а значи и алгебрично разширение (твърдение 1). Следователно тези елементи принадлежат на $\overline{F}$, което означава, че $\overline{F}$ е поле.

б) Нека $f(x) = a_0 x^n + \cdots + a_n$ е произволен неконстантен полином с коефициенти от полето $\overline{F}$ и α е корен на $f(x)$. Разглеждайки веригата $F \leqq F(a_0, \ldots, a_n) \leqq F(a_0, \ldots, a_n; \alpha)$, точно както в доказателството на следствие 3 заключаваме, че α е алгебричен над F елемент, т. е. $\alpha \in \overline{F}$. Така корените на всеки неконстантен полином с коефициенти от $\overline{F}$ са също в $\overline{F}$, което означава, че полето $\overline{F}$ е алгебрическо затворено.

З а б е л е ж к а. Знаем, че всяко крайно разширение е алгебрично разширение. Обратното обаче не е вярно. Например разширението $\mathbb{Q} < \overline{\mathbb{Q}}$ е алгебрично, но не е крайно. Последното следва от твърдение 1 и от факта, че съществуват неразложими над $\mathbb{Q}$ полиноми от произволно висока степен, а значи съществуват и алгебрични над $\mathbb{Q}$ числа от произволно висока степен на алгебричност.