第四章　域

§4.1　域的扩张

概要: 扩域; 次数公式; 生成子域.

回顾在第三章中已建立的本章将用到的域的知识:

- 每个非零元都可逆的交换幺环称为域.
- 域 F 的特征 $\operatorname{char} F$ 是 0 或者是一个素数; 而且:
  — 如果 $\operatorname{char} F = 0$, 则 F 的最小子域同构于 $\mathbb{Q}$.
  — 如果 $\operatorname{char} F = p$ 是一个素数, 则 F 的最小子域同构于 $\mathbb{Z}_p$; 且

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \ , \qquad \forall \ \ a, b \in F \, , \ \ n \in \mathbb{Z}^+ \, , n > 0 \ .$$

- 域上的一元多项式环是欧氏环从而是主理想整环, 是因子分解整环.
- 域上的 n 次一元多项式在域中最多有 n 个不同的根.
- 域 K 上的一元多项式环 $K[x]$ 的不可约多项式 $p(x)$ 生成的理想 $K[x]p(x)$ 是极大理想, 因而商环 $K[x]/K[x]p(x)$ 是一个域.

定义. 如果 K 是域, 而 F 是包含 K 为子域的域, 则称 F 是 K 的 *扩域*, 或称 F 是域 K 的 *扩张*.

设 F 是域 K 的扩张. 那么, 第一 $(F, +)$ 是加群; 第二, K 的元素与 F 的元素相乘: $K \times F, (k, f) \mapsto kf$, 作为系数乘法; 易验证: F 成为 K 上的向量空间. 所以进一步定义:

定义. 记号如上. F 作为域 K 上的向量空间的维数 $\dim_K F$ 称为扩域 F 在子域 K 上的 *次数 (degree)*, 记作 $|F : K|$. 如果 $|F : K| < \infty$ 就称 F 是 K 的 *有限扩张 (finite extension)*; 如果 $|F : K| = \infty$ 称 F 是 K 的 *无限扩张 (infinite extension)*.

4.1.1 引理 (次数公式). *设 $E \supseteq F \supseteq K$ 是域. 那么 $|E : K| = |E : F| \cdot |F : K|$.*

证. 设 U 是 F 作为 K- 向量空间的基底, 设 V 是 E 作为 F- 向量空间的基底. 只需证明: uv, 其中 $u \in U$ 而 $v \in V$, 恰构成 E 作为 K- 向量空间的基底.

首先，若 $u_1,\cdots,u_m \in U$ 和 $v_1,\cdots,v_n \in V$ 以及 $a_{ij} \in K$ 其中 $i=1,\cdots,m$ 和 $j=1,\cdots,n$, 使得 $\sum\limits_{1\le i\le m,\ 1\le j\le n} a_{ij}u_iv_j = 0$; 那么

$$\sum_{j=1}^{n}(\sum_{i=1}^{m} a_{ij}u_i)v_j = 0\ ,$$

由于集合 V 是 F- 线性无关的，就得

$$\sum_{i=1}^{m} a_{ij}u_i = 0\ , \qquad j=1,\cdots,n\ ;$$

再根据集合 U 是 K- 线性无关的，得出

$$a_{ij}=0\ , \qquad \forall\ \ i=1,\cdots,m,\ \ j=1,\cdots,n\ .$$

所以 $\{\ uv \mid u\in U,\ v\in V\ \}$ 是 K- 线性无关集合.

其次，对任 $w\in E$ 有 $v_1,\cdots,v_n\in V$ 和 $b_1,\cdots,b_n\in F$ 使得 $w=\sum\limits_{j=1}^{n} b_jv_j$; 然后，每个 $b_j\in F$ 是 U 中元的有限 K- 线性组合；即：可以找到有限个 $u_1,\cdots,u_m\in U$ 使得 $b_j=\sum\limits_{i=1}^{m} a_{ij}u_i$, 其中 $a_{ij}\in K$; 那么

$$w=\sum_{1\le i\le m,\ 1\le j\le n} a_{ij}u_iv_j\ . \qquad \square$$

注. 按简单的归纳法即可得一般的 *次数公式*: 如果 $F_n\supseteq F_{n-1}\supseteq\cdots\supseteq F_1\supseteq K$ 是域扩张链，则

$$|F_n:K| = |F_n:F_{n-1}|\cdot|F_{n-1}:F_{n-2}|\cdots|F_1:K|\ . \qquad \square$$

例. $\mathbb{C}\supseteq\mathbb{R}$, 所以 $\mathbb{C}$ 可作为 $\mathbb{R}$- 向量空间；$\{1,\ \mathrm{i}\}$ 是 $\mathbb{C}$ 的 $\mathbb{R}$- 基底；所以 $|\mathbb{C}:\mathbb{R}|=2$.

4.1.2 定义. 设 E 是域 K 的扩张；设 S 是 E 的子集.

(1) 显然，E 中既包含 K 也包含 S 的所有子环的交集仍然是既包含 K 也包含 S 的子环，它是 E 中既包含 K 也包含 S 的最小子环，称为由子集 S 在 K 上 *生成的环*, 记作 $K[S]$.

(2) E 中既包含 K 也包含 S 的所有子域的交集仍然是既包含 K 也包含 S 的子域，它是 E 中既包含 K 也包含 S 的最小子域，称为由子集 S 在 K 上 *生成的域*, 记作 $K(S)$.

如果 $S=\{\alpha_1,\cdots,\alpha_n\}$, 则简记 $K[S]$ 为 $K[\alpha_1,\cdots,\alpha_n]$; 记 $K(S)$ 为 $K(\alpha_1,\cdots,\alpha_n)$.

一个元生成的域 $K(\alpha)$ 称为 K 的 *单扩域*, 或称 *单扩张*.

注. "生成的域" $K(S)$ 是域 K 的扩张.

"生成的环" $K[S]$ 则不能称为域 K 的扩张；但有时称为 *环 K 的扩张*.

4.1.3 引理. (1). $K[\alpha]=\{\ f(\alpha)\mid f(x)\in K[x]\ \}$.

(2) $K(\alpha)=\left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x),g(x)\in K[x]\,,\ \ g(\alpha)\neq 0 \right\}$.

证. (1). 按定义, $K[\alpha]$ 是 E 既包含 K 也包含 α 的最小子环.

记 $K_\alpha := \{\, f(\alpha) \mid f(x)\in K[x] \,\}$. 首先证明 K_α 是既包含 K 也包含 α 的一个子环. 取 $f(x)=a\in K$ 是常数多项式, 就知道 $a=f(\alpha)\in K_\alpha$, 即 $K_\alpha\supseteq K$. 同样, 取 $f(x)=x$, 就知道 $\alpha=f(\alpha)\in K_\alpha$. 对任 $f(\alpha),g(\alpha)\in K_\alpha$, 这里 $f(x),g(x)\in K[x]$, 由于 $f(x)-g(x)$ 仍是 K- 多项式即 $f(x)-g(x)\in K[x]$, 故 $f(\alpha)-g(\alpha)\in K_\alpha$; 同理, $f(\alpha)g(\alpha)\in K_\alpha$. 最后, $1\in K\subseteq K_\alpha$. 所以 K_α 是子环.

再设 R 是 E 中 R 既包含 K 也包含 α 的子环. 对任 $f(x)=\sum a_ix^i\in K[x]$, 因为 a_i, α 都在 R 中, 故 R 包含 $\sum a_i\alpha^i=f(\alpha)$; 所以 $R\supseteq K_\alpha$.

也就是说 K_α 是 E 中既包含 K 也包含 α 的最小子环. 即 $K[\alpha]=K_\alpha$. □

(2). 类似于 (1) 的证明. 记 $\tilde{K}_\alpha := \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x),g(x)\in K[x]\,,\ \ g(\alpha)\neq 0 \right\}$.

完全类似于 (1) 的第一段推理, $\tilde{K}_\alpha$ 是 E 的一个既包含 K 也包含 α 的子域. 也完全类似于 (1) 的第二段推理, 如果 E 的子域既包含 K 也包含 α, 则必包含 $\tilde{K}_\alpha$. □

对多个元素的扩张可以得到类似的结论.

4.1.4 引理. *设 E 是域 K 的扩张, 设 $S\subseteq E$ 是任意非空子集. 则*

$$K(S)=\left\{ \frac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)} \;\middle|\; \begin{array}{r} f(x_1,\cdots,x_n),g(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]\,,\\ \alpha_1,\cdots,\alpha_n\in S\,,\ g(\alpha_1,\cdots,\alpha_n)\neq 0\,,n\geq 0 \end{array} \right\}.\quad \square$$

4.1.5 推论. *记号同上. 对任 $u\in K(S)$ 存在有限子集 $S_0\subseteq S$ 使得 $u\in K(S_0)$.*

证. 由引理 4.1.7, 存在有限个 $\alpha_1,\cdots,\alpha_n\in S$ 和 $f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$, $g(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$, 使得 $g(\alpha_1,\cdots,\alpha_n)\neq 0$ 且

$$u=\frac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)}\,;$$

那么 $u\in K(\alpha_1,\cdots,\alpha_n)$. □

显然, 有限个元素的扩张可以通过逐步单扩张实现:

4.1.6 $$K(\alpha_1,\cdots,\alpha_n)=K(\alpha_1,\cdots,\alpha_{n-1})(\alpha_n)=K(\alpha_1)(\alpha_2,\cdots,\alpha_n)\,.$$

证. 按定义 4.1.3(2) 就知道 $K(\alpha_1,\cdots,\alpha_n)$ 是既包含 $K(\alpha_1,\cdots,\alpha_{n-1})$ 也包含 α_n 的子域; 所以 $K(\alpha_1,\cdots,\alpha_n)\supseteq K(\alpha_1,\cdots,\alpha_{n-1})(\alpha_n)$. 另一方面, 同样按定义 4.1.3(2) 知道: $K(\alpha_1,\cdots,\alpha_{n-1})(\alpha_n)$ 既包含 K 也包含所有 $\alpha_1,\cdots,\alpha_{n-1},\alpha_n$, 所以 $K(\alpha_1,\cdots,\alpha_n)\subseteq K(\alpha_1,\cdots,\alpha_{n-1})(\alpha_n)$.

类似地证明另一等式 $K(\alpha_1,\cdots,\alpha_n)=K(\alpha_1)(\alpha_2,\cdots,\alpha_n)$. □

4.1.7 例. (1). 设 $K=\mathbb{Q}$, 取 $E=\mathbb{Q}(x)$ 是所有有理系数的分式构成的域 (有理系数分式域), 则 E 是 K 的扩张. 取 $\alpha=x\in E$. 则 $\mathbb{Q}[\alpha]=\mathbb{Q}[x]$ 是有理系数多项式环; 而 $\mathbb{Q}(\alpha)=\mathbb{Q}(x)$ 是有理系数分式域. 显然, $\mathbb{Q}[\alpha]\subsetneqq\mathbb{Q}(\alpha)$.

(2). 设 $K=\mathbb{Q}$, 取 $E=\mathbb{C}$ 是复数域. 则 E 是 K 的扩张. 取 $\alpha=\sqrt{2}\in E$. 利用 $\alpha^2=2$ 易计算 $\mathbb{Q}[\alpha]=\{\ a+b\alpha\mid a,b\in\mathbb{Q}\ \}$, $\mathbb{Q}(\alpha)=\{\ a+b\alpha\mid a,b\in\mathbb{Q}\ \}$. 所以, $\mathbb{Q}[\alpha]=\mathbb{Q}(\alpha)$. 而且 $1,\alpha$ 在 $\mathbb{Q}$ 上线性无关 (若有不全为零的 $a,b\in\mathbb{Q}$ 使得 $a\cdot1+b\sqrt{2}=0$ 则 $\sqrt{2}$ 是有理数), 所以 $|\mathbb{Q}(\alpha):\mathbb{Q}|=2$.

这些例子说明: 关系 $K[S]\subseteq K(S)$ 中等号有时能成立. 在 $S=\{\alpha\}$ 只含一个元素时, 下面将看到等号成立的条件.

习题 4.1

1. 没有真子域的域称为 *素域 (prime field)*. 证明:

(1) 一个素域如果特征为 0 则同构于 $\mathbb{Q}$.

(2) 一个素域如果特征为一个素数 p 则同构于 $\mathbb{Z}_p$.

2. 设 R 是整环, $R\subseteq Q$, Q 是 R 的分式域. 设 F 是域. 设 $f:R\to F$ 是环同态.

(1) $\operatorname{Ker}f$ 是 R 的素理想;

(2) 如果 $\operatorname{Ker}f=0$, 则有唯一环同态 $\tilde{f}:Q\to F$ 使得 $\tilde{f}|_R=f$; 此时 $\tilde{f}$ 是单同态, 即 Q 嵌入 F.

3. 设 E 是 K 的扩域, $\alpha,\ \beta\in E$, $|K(\alpha):K|<\infty$, $|K(\beta):K|<\infty$. 证明:

(1) $|K(\alpha,\beta):K|\le|K(\alpha):K|\cdot|K(\beta):K|$.

(2) 若 $|K(\alpha):K|$ 与 $|K(\beta):K|$ 互素, 则 $|K(\alpha,\beta):K|=|K(\alpha):K|\cdot|K(\beta):K|$.

4. 证明: $K(\alpha)=K[\alpha]$ 当且仅当 α 是 K 上的代数元.

5. (1) 证明: $\mathbb{Q}(\sqrt[3]{2})=\mathbb{Q}[\sqrt[3]{2}]$.

(2) 求: $|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}|$.

6. (1). 证明: $\mathbb{Q}(\sqrt{2},\ \sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

(2) 求: $|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}|$.

7. 设 p 是一个素数. 设 F 是一个域, $|F|\ge p$. 证明: 如果 $(a+b)^p=a^p+b^p$ 对所有 $a,b\in F$ 成立, 则 $\operatorname{char}F=p$.

§4.2 单扩张

概要: 域的嵌入与同构; 超越元与代数元; 代数单扩张的结构; 代数单扩张的存在性.

设 E 和 F 是域. 如果 $\sigma:E\to F$ 是环同态, 即

$$\sigma(1_E)=1_F\,,\quad \sigma(a+b)=\sigma(a)+\sigma(b)\,,\quad \sigma(a\cdot b)=\sigma(a)\cdot\sigma(b)\,,\qquad \forall\ a,b\in E\ ;$$

则因 $\mathrm{Ker}\,\sigma$ 是 E 的理想，域只有零理想和单位理想，若 $\mathrm{Ker}\,\sigma = E$ 是单位理想则 $\sigma = 0$ 是零同态，与 σ 不是零同态 (因为 $\sigma(1) = 1$) 相矛盾；所以只能是 $\mathrm{Ker}\,\sigma = 0$. 而且对 $0 \neq a \in E$, 因为 $1 = \sigma(1) = \sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1})$, 所以 $\sigma(a^{-1}) = \sigma(a)^{-1}$. 所以我们 把域之间的环同态也称为域同态.

总结上述，有结论： 域同态一定是单同态，即可以看作域 E 嵌入域 F.

因此，如果域同态 $\sigma : E \to F$ 是满的则是双射，称为 域同构, 这时称域 E 与域 F 同构，记作 $E \cong F$; 或更准确地记作 $E \overset{\sigma}{\cong} F$, 意思是 "$E$ 通过 σ 同构于 F".

设 E 和 F 都是域 K 的扩域. 如果同态 $\sigma : E \to F$ 还满足： $\sigma(c) = c, \forall\, c \in K$, 就称 σ 是一个 K- 同态; 因为这时对任 $a \in E, c \in K$ 有 $\sigma(ca) = \sigma(c)\sigma(a) = c \cdot \sigma(a)$; 即这种 σ 不仅是环同态，而且把 E, F 作为 K- 向量空间时它还是 K- 线性映射.

域 K 上的多项式环 $K[x]$ 包含 K 作为子域. 因为：通过把 K 的元 c 作为 $K[x]$ 中的常数多项式 c, K 就 嵌入 了 $K[x]$ 作为了 $K[x]$ 的子环，但它是域，故是 $K[x]$ 的子域.

以下设 F 是域 K 的扩域， $\alpha \in F$. 下述映射称为 赋值映射:

$$\nu_\alpha :\ K[x] \ \longrightarrow\ F\,, \quad f(x) \ \longmapsto\ f(\alpha)\,.$$

类似于 3.6.10, 易验证 ν_α 是环同态；而且，它还是 K- 线性映射，因为：对 $c \in K$ 有 $\nu_\alpha(c) = c$, 即常值多项式 c 在 α 处取值 c. 所以也说 ν_α 是 K- 同态. 按 ν_α 的定义就得：

$$\mathrm{Im}(\nu_\alpha) = \{\ f(\alpha) \mid f(x) \in K[x]\ \} = K[\alpha]\,.$$

同态核 $\mathrm{Ker}(\nu_\alpha)$ 是 $K[x]$ 的理想. 回想：如果多项式 $h(x)$ 使得 $h(\alpha) = 0$ 就称 $h(x)$ 是 α 的 零化多项式. 仍按 ν_α 的定义即知：同态核理想

$$\mathrm{Ker}(\nu_\alpha) = \{\ h(x) \in K[x] \mid h(\alpha) = 0\ \}$$

就是 α 的所有零化多项式的集合，称为 α 的 零化理想. 因为 $K[x]$ 是主理想整环，核 $\mathrm{Ker}(\nu_\alpha)$ 可由一个元 $g(x)$ 生成： $\mathrm{Ker}(\nu_\alpha) = K[x]g(x)$. 现在引用同态基本定理：

$$\begin{array}{ccc} K[x] & \xrightarrow{\ \nu_\alpha\ } & K[\alpha] \\ {\scriptstyle \mathrm{bar}}\big\downarrow & \nearrow {\scriptstyle \bar\nu_\alpha} & \\ K[x]/(K[x]g(x)) & & \end{array}$$

$\mathrm{Ker}(\nu_\alpha) =$

其中 $\mathrm{bar} : K[x] \to K[x]/(K[x]g(x))$ 是自然同态，它把 $f(x)$ 映射为 $f(x)$ 所在剩余类

$$\overline{f(x)} = \{f(x) + u(x)g(x) \mid u(x) \in K[x]\} = \{h(x) \in K[x] \mid h(x) \equiv f(x)\ (\mathrm{mod}\ g(x))\}\ ;$$

而其中 $\bar\nu_\alpha$ 是我们所要的环同构映射：

4.2.1 $$\bar\nu_\alpha :\quad K[x]/(K[x]g(x)) \ \xrightarrow{\ \cong\ }\ K[\alpha]\ , \quad \overline{f(x)} \ \longmapsto\ f(\alpha)\ .$$

注. 剩余类环 $K[x]/(K[x]g(x))$ 也包含 K 作为子域. 因为:

第一步, K 已嵌入 $K[x]$ 成为 $K[x]$ 的子域, 通过把 K 的元 c;

第二步, 再通过映射 bar 映射为常数多项式 c 所在的剩余类 $\bar{c}$,

这样, K 就嵌入了剩余类环 $K[x]/(K[x]g(x))$ 成为它的子域.

那么 4.2.1 也是 K- 向量空间同构, 因为: 对 $c \in K$, 它作为 $K[x]/(K[x]g(x))$ 的元是剩余类 $\bar{c}$, 按 $\bar{\nu}_\alpha$ 的定义, $\bar{\nu}_\alpha(\bar{c}) = c$. 即 $\bar{\nu}_\alpha$ 把 $K \subseteq K[x]/(K[x]g(x))$ 的元 $\bar{c}$ 恒等地映射为 $K \subseteq K[\alpha]$ 的元 c.

4.2.2 定义. 记号如同 4.2.1.

(1) 如果 $g(x) = 0$ 即 $\mathrm{Ker}(\nu_\alpha) = 0$, 则称 α 是 K 上的 *超越元*.

(2) 如果 $g(x) \neq 0$ 即 $\mathrm{Ker}(\nu_\alpha) \neq 0$, 则称 α 是 K 上的 *代数元*, 称 $g(x)$ 为 α 的 *极小多项式*; 称 $K(\alpha)$ 是代数单扩张.

注. 按上述讨论知道: 代数元 α 的极小多项式 $g(x)$ 的特征性质是: *多项式 $h(x)$ 零化 α(即 $h(\alpha) = 0$) 当且仅当 $g(x) \,|\, h(x)$.*

4.2.3 例. (1). 取 $K = \mathbb{Q}$, $F = \mathbb{Q}(x)$, 参看例 4.1.7(1). 取 $\alpha = x$. 则 ν_α 是单射, 只有 0 是 α 的零化多项式. 即 $\alpha = x$ 是 $\mathbb{Q}$ 上的超越元.

(2). 取 $K = \mathbb{Q}$, $F = \mathbb{C}$. 取 $\alpha = \pi$ (圆周率). 则 π 是 $\mathbb{Q}$ 上的超越元 (这结论的证明很不容易). 因此, $\nu_\pi : \mathbb{Q}[x] \to \mathbb{R}$, $f(x) \mapsto f(\pi)$, 是单同态; 于是 $\mathbb{Q}[\pi]$ 与有理多项式环 $\mathbb{Q}[x]$ 同构; 且由习题 4.1.3, $\mathbb{Q}(\pi)$ 与有理分式域 $\mathbb{Q}(x)$ 同构.

(3). 例 4.1.7(2) 中的 $\alpha = \sqrt{2}$ 是代数元.

4.2.4 例. 如果 $|F : K| = 2$, 则存在 $\alpha \in F - K$ 使得 $\alpha^2 = a \in K$ 而 $F = K(\alpha)$.

注. $\alpha^2 = a$, 就是说 α 是 a 的平方根, 所以也记 $\alpha = \sqrt{a}$, 那么 $F = K(\sqrt{a})$. 所以称 $F = K(\sqrt{a})$ 为 *平方根扩张*.

证. 取 $\beta \in F - K$, 则 $F \supseteq K(\beta) \neq K$; 由次数公式 $|F : K(\beta)| \cdot |K(\beta) : K| = |F : K| = 2$; 只能是 $|F : K(\beta)| = 1$; 即 $F = K(\beta)$. 而 $|K(\beta) : K| = 2$, β 在 K 上的极小多项式是二次多项式 $ax^2 + bx + c$, 即

$$0 = a\beta^2 + b\beta + c = a\Big(\beta + \frac{b}{2a}\Big)^2 + \frac{4ac - b^2}{4a}$$

令 $\alpha = \beta + \frac{b}{2a}$, 则

$$F = K(\beta) = K(\alpha)\,, \qquad \text{且} \qquad \alpha^2 = \frac{b^2 - 4ac}{4a} \in K\,. \qquad \square$$

注. 平方根扩张很容易描述. 例如取 $K = \mathbb{Q}$ 是有理数域, 取 $\alpha = \sqrt{2}$, 则 $x^2 - 2$ 是它的一个极小多项式. 且极易验证赋值映射

$$\nu_{\sqrt{2}} : \quad \mathbb{Q}[x] \longrightarrow \mathbb{R}, \quad f(x) \longmapsto f(\sqrt{2})$$

的象 $\mathrm{Im}(\mu_{\sqrt{2}}) = \mathbb{Q}[\sqrt{2}] = \{\ a+b\sqrt{2} \mid a,b \in \mathbb{Q}\ \}$, 它本身就是一个域, 因为, 如同熟知的, "分母可以有理化": $(a+b\sqrt{2})^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2}$. 实际上, 这是一个普遍规律.

4.2.5 定理. *设 α 是域 K 上的代数元, $p(x) \in K[x]$ 是 α 在 K 上的极小多项式. 则 $p(x)$ 是 $K[x]$ 的不可约多项式, 而且:*

(1) $|K(\alpha) : K| = \deg p(x)$;

(2) $K(\alpha) = K[\alpha] \cong K[x]/(K[x]p(x))$.

证. 如果 $p(x) = p_1(x)p_2(x)$, 则 $p_1(\alpha)p_2(\alpha) = p(\alpha) = 0$; 那么或者 $p_1(\alpha) = 0$ 或者 $p_2(\alpha) = 0$; 也就是说或者 $p_1(x)$ 是 α 的零化多项式, 或者 $p_1(x)$ 是 α 的零化多项式; 故或者 $p(x)|p_1(x)$, 或者 $p(x)|p_2(x)$. 所以 $p(x)$ 是不可约多项式.

(1). 设 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ (可以设 $p(x)$ 是首一的). 那么对任意不全为零的 $c_0, c_1, \cdots, c_{n-1} \in K$, $c_0 + \cdots + c_{n-1}x^{n-1}$ 是 $K[x]$ 中的次数 $< n$ 的非零多项式, 故它不零化 α, 即

$$c_0 \cdot 1 + \cdots + c_{n-1} \cdot \alpha^{n-1} \neq 0\ .$$

所以 $1, \alpha, \cdots, \alpha^{n-1}$ 在 K 上线性无关. 另一方面, 由于 $p(\alpha) = 0$, 即

$$\alpha^n = (-a_0) \cdot 1 + \cdots + (-a_{n-1}) \cdot \alpha^{n-1}\ ,$$

所以 $K[\alpha]$ 的任意元素可以写成 $1, \alpha, \cdots, \alpha^{n-1}$ 在 K 上的线性组合. 所以 $1, \alpha, \cdots, \alpha^{n-1}$ 是 $K[\alpha]$ 作为 K- 向量空间的基底. 也就是 $|K[\alpha] : K| = n = \deg p(x)$.

(2). 按 4.2.1, $K[\alpha] \cong K[x]/(K[x]p(x))$. 因为 $p(x)$ 不可约, 所以 $K[x]/(K[x]p(x))$ 是域; 从而 $K[\alpha]$ 是域. 从而 $K[\alpha]$ 是 F 的包含 K 和 α 的子域, 故 $K[\alpha] \supseteq K(\alpha)$. 即得 $K[\alpha] = K(\alpha)$. □

4.2.6 注. 熟知的 "分母有理化" 其实就是 4.2.5 的结论 (2): $K(\alpha) = K[\alpha]$ 的另一个证明. 叙述如下.

已证明了 α 的极小多项式 $p(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n$ 是素多项式, 而且已证明 $1, \alpha, \cdots, \alpha^{n-1}$ 是 $K[\alpha]$ 作为 K- 向量空间上的基底, 即 $K[\alpha]$ 的任一元形如 $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$, 其中 $c_i \in K$; 如果它不是零, 就要证明

$$\frac{1}{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}} = (c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})^{-1} \in K[\alpha]\ .$$

这时多项式 $f(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ 不是零多项式; 由于 $\deg f(x) < \deg p(x)$ 故 $p(x) \nmid f(x)$; 而 $p(x)$ 是素多项式, 故 $f(x)$ 必与 $p(x)$ 互素, 有 $u(x), v(x) \in K[x]$ 使得 $f(x)u(x) + p(x)v(x) = 1$. 由于 $p(\alpha) = 0$, 所以 $f(\alpha)u(\alpha) = 1$; 即

$$\frac{1}{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}} = \frac{1}{f(\alpha)} = \frac{u(\alpha)}{f(\alpha)u(\alpha)} = u(\alpha) \in K[\alpha]\ .$$

所以 $K[\alpha]$ 是 F 的子域, 从而 $K(\alpha) = K[\alpha]$.

例. 取 $K=\mathbb{Q}, \alpha=\sqrt[3]{2}$. 则 α 的极小多项式 $p(x)=x^3-2$. 对 $(\sqrt[3]{2})^2+\sqrt[3]{2}+1\in\mathbb{Q}[\sqrt[3]{2}]$, 由于

$$(x^2+x+1)(x-1)+(x^3-2)(-1)=1\ ,$$

所以 $(\sqrt[3]{2})^2+\sqrt[3]{2}+1)(\sqrt[3]{2}-1)=1$; 即

$$\frac{1}{(\sqrt[3]{2})^2+\sqrt[3]{2}+1}=\frac{1(\sqrt[3]{2}-1)}{(\sqrt[3]{2})^2+\sqrt[3]{2}+1)(\sqrt[3]{2}-1)}=\sqrt[3]{2}-1\ .$$

上面从 4.2.1 开始的讨论都是在 α 已经存在的前提下进行. 但是 4.2.1 和 4.2.5(2) 启示我们: 在单扩张尚不存在 (即 α 尚不存在) 的前提下, 对素多项式 $p(x)\in K[x]$ 可以构造出单扩张 $K(\alpha)$ 使得 α 是 K 上的代数元它以 $p(x)$ 为极小多项式.

4.2.7 引理. *设 $p(x)$ 是域 K 上的不可约多项式. 则剩余类环 $F:=K[x]/(K[x]p(x))$ 是 K 的扩域; 且令 $\alpha:=\overline{x}\in F$ 是多项式 x 所在剩余类, 则 $F=K(\alpha)$, α 是 K 上的代数元, $p(x)$ 是 α 的极小多项式.*

证. 不可约多项式生成的理想 $K[x]p(x)$ 是 $K[x]$ 的极大理想, 商环 $F=K[x]/(K[x]p(x))$ 是域. 4.2.1 后的注解已说明 F 包含 K 为子域, 即 F 是 K 的扩域. 看赋值映射

$$\nu_\alpha:\quad K[x]\longrightarrow F\ ,\quad f(x)\longmapsto f(\alpha)\ .$$

设 $f(x)=\sum_{i=0}^n c_ix^i$, 注意 $c_i\in K$ 作为 F 的元是 $\bar{c}_i$, 由于 bar: $K[x]\to K[x]/K[x]p(x)$, $f(x)\mapsto\overline{f(x)}$, 是自然同态映射, 得

$$\nu_\alpha(f(x))=f(\alpha)=\sum_{i=0}^n\bar{c}_i\alpha^i=\sum_{i=0}^n\bar{c}_i\bar{x}^i=\overline{\sum_{i=0}^n c_ix^i}=\overline{f(x)}\ .$$

所以, 此时赋值映射 ν_α 就是自然同态映射 bar. 故 $K[\alpha]=\mathrm{Im}(\nu_\alpha)=F$, $\mathrm{Ker}(\nu_\alpha)=K[x]p(x)$; 且 $\alpha=\bar{x}$ 是 K 上的代数元, $p(x)$ 是它的极小多项式. □

4.2.8 例. 取 $K=\mathbb{R}$ 是实数域, 取 $p(x)=x^2+1$. 则 $p(x)$ 是 $\mathbb{R}$ 上的不可约多项式, 因为: $\deg p(x)=2$, 若 $p(x)$ 可约则有一次因子, 也就是说 $p(x)=x^2+1$ 有实根 α, 即实数 α 使得 $\alpha^2+1=0$; 左边是正实数, 此式不可能成立.

那么由引理 4.2.7, $\mathbb{R}[x]/(\mathbb{R}[x](x^2+1))$ 是 $\mathbb{R}$ 的一个扩域 $\mathbb{C}=\mathbb{R}(\mathrm{i})$, 它的生成元 i 以 $p(x)=x^2+1$ 为极小多项式; 即 $\mathbb{C}$ 是 $\mathbb{R}$ 上的二次扩张, 作为 $\mathbb{R}$- 向量空间以 $1,\mathrm{i}$ 为基底:

$$\mathbb{C}=\{\,a+b\,\mathrm{i}\mid a,b\in\mathbb{R}\,\},\qquad \mathrm{i}^2=-1\ .$$

我们知道这就是复数域.

4.2.9 定理. *设 $f(x)$ 是域 K 上的 n 次多项式. 则存在扩域 $F\supseteq K$ 使得:*

(1) *在 $F[x]$ 中 $f(x)$ 可以分解为一次因式之积 $f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$;*

(2) *$F=K(\alpha_1,\cdots,\alpha_n)$.*

证. 对 $\deg f(x)$ 进行归纳. $\deg f(x)=1$ 时显然正确, 取 $F=K$ 即可.

设 $\deg f(x)=n>1$. 设 $p(x)\in K(x)$ 是 $f(x)$ 的不可约因式, 设 $f(x)=p(x)q(x)$. 由引理 4.2.7, 存在扩张 $K_1=K(\alpha_1)$ 使得 $p(x)$ 是 α_1 在 K 上的极小多项式, 特别有 $p(\alpha_1)=0$. 由余式定理, 在 $K_1[x]$ 中有: $p(x)=(x-\alpha_1)p_1(x)$. 从而在 $K_1(x)$ 中有: $f(x)=(x-\alpha_1)f_1(x)$. 由此, $\deg f_1(x)=n-1$. 按归纳法, 对 $f_1(x)$ 存在 K_1 的有限扩张 $F\supseteq K_1$ 满足 (1),(2) 两条, 即: 在 $F[x]$ 中 $f_1(x)=a(x-\alpha_2)\cdots(x-\alpha_m)$ 且 $F=K_1(\alpha_2,\cdots,\alpha_n)$. 而 $\alpha_1\in K_1\subseteq F$, $K_1=K(\alpha_1)$, 所以, 在 $F[x]$ 中

$$f(x)=(x-\alpha_1)f_1(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)\ ,$$

而且

$$F=K_1(\alpha_2,\cdots,\alpha_n)=K(\alpha_1)(\alpha_2,\cdots,\alpha_n)=K(\alpha_1,\alpha_2,\cdots,\alpha_n)\ .$$

即对 $f(x)$, 扩张 F 满足 (1),(2) 两条. □

注. **8** 在这个定理中, 显然 a 是 $f(x)$ 首项系数, $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$ 的全部根. 所以定理中的 (1) 就是说域 F 包含 $f(x)$ 的全部根, (2) 则是说 F 是在域 K 上由 $f(x)$ 的全部根生成的扩域. 满足这两条的扩张称为 K- 多项式 $f(x)$ 的 分裂域. 它就是使得 $f(x)$ 可分裂为一次因式之积的极小的扩域.

例. 取 $K=\mathbb{Q}$ 是有理数域. 取 $f(x)=x^3-2$. 那么 $f(x)$ 就是 K 上的不可约多项式. 所以

$$K_1=K[x]/K[x](x^3-1)=K(\alpha_1),\quad (\text{ 实际上 }\alpha_1=\sqrt[3]{2}\text{ 就是 }f(x)\text{ 的一个根}).$$

在 $K_1[x]$ 中, $f(x)=x^3-1=(x-\alpha_1)(x^2+\alpha_1x+\alpha_1^2)$, 即

$$f(x)=x^3-1=(x-\alpha_1)f_1(x)\ ,\quad \text{其中 } f_1(x)=x^2+\alpha_1x+\alpha_1^2\ ;$$

而 $f_1(x)$ 是 K_1 上的不可约多项式. 所以

$$K_2=K_1[x]/K_1[x]f_1(x)=K_1(\alpha_2),\quad (\text{ 实际上 }\alpha_2=\omega\alpha_1=\omega\sqrt[3]{2}\text{ 就是 }f_1(x)\text{ 的一个根}),$$

其中 $\omega=\exp(2\pi\mathrm{i}/3)=\frac{-1+\sqrt{-3}}{2}$ 是一个 3 次本原单位根. 那么在 $K_2[x]$ 中, $f_1(x)=(x-\omega\alpha_1)(x-\omega^2\alpha_1)$, 令 $\alpha_3=\omega^2\alpha_1\in K_2$. 则在 K_2 中 $f_1(x)=(x-\alpha_2)(x-\alpha_3)$, 故而

$$f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)=(x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})\ ;$$

而

$$K_2=K(\alpha_1,\,\alpha_2,\,\alpha_3)=\mathbb{Q}\left(\sqrt[3]{2},\,\omega\sqrt[3]{2},\,\omega^2\sqrt[3]{2}\right)$$

即 $F=K_2$ 符合定理要求. 附带指出

$$|K_2:\mathbb{Q}|=|K_2:K_1|\cdot|K_1:K|=2\cdot3=6\ .$$

习题 4.2

1. 证明：若 $K(\alpha)=K[\alpha]$, 则 α 是域 K 上的代数元.

(提示: 提示： α 在 $K[\alpha]$ 中可逆，存在 $f(x)\in K[x]$ 使得 $\alpha\cdot f(\alpha)=1$.)

2. 设 $p(x)\in K[x]$ 使得 $p(\alpha)=0$, 而且 $p(x)$ 是 $K[x]$ 的素多项式，则 $p(x)$ 是 α 在 K 上的极小多项式.

3. 求 $a\in\mathbb{Q}$ 使得 $\mathbb{Q}\left(\frac{-1+\sqrt{-3}}{2}\right)=\mathbb{Q}(\sqrt{a})$.

4. (1) 求 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的极小多项式.

(2) 求 $\sqrt[3]{2}$ 在 $\mathbb{R}$ 上的极小多项式.

5. 求 $1/(\mathrm{i}-1)$ 在 $\mathbb{Q}$ 上的极小多项式.

(提示: 令 $x=1/(\mathrm{i}-1)$, 变形得 $\mathrm{i}x=x+1$, 得 $2x^2+2x+1=0$.)

6. 做分母有理化 $\dfrac{\sqrt[3]{2}-1}{(\sqrt[3]{2})^2+2\sqrt[3]{2}+1}$.

7. 设 p 是素数；令 $\omega=e^{2\pi\,\mathrm{i}/p}$. 证明： $|\mathbb{Q}(\omega):\mathbb{Q}|=p-1$.

(提示: ω 在 $\mathbb{Q}$ 上的极小多项式是 $x^{p-1}+\cdots+x+1$; 参看习题 3.10.7.)

8. 设 $K(x)$ 是域 K 上的不定元 x 的分式域 (即 x 是 K 上的超越元), $K\subsetneqq F\subseteq K(x)$. 证明： x 是 F 上的代数元.

§4.3 代数扩张

概要: 有限扩张；代数扩张；代数闭域.

始终设 K 是一个域.

4.3.1 定义. 如果 K 的扩张 F 的任何元素都是 K 上的代数元，则称 F 是 K 的代数扩张.

4.3.2 引理. *K 的扩域的元素 α 是 K 上的代数元当且仅当 $|K(\alpha):K|<\infty$.*

证. 由定理 4.2.6 知：如果 α 是超越元则 $|K(\alpha):K|=\infty$. 而由定理 4.2.7 知：如果 α 是代数元则 $|K(\alpha):K|=\deg p(x)<\infty$, 其中 $p(x)$ 是 α 的极小多项式. □

注. 充分性的另一直接证明：设 $|K(\alpha):K|=n<\infty$; 则 $1,\alpha,\cdots,\alpha^n$ 共有 $n+1$ 个元故在 K 上线性相关，即存在不全为零的 $a_0,a_1,\cdots,a_n\in K$ 使得 $\sum\limits_{i=0}^{n}a_i\alpha^i=0$; 那么 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$ 是 K 上的非零多项式它零化 α.

4.3.3 引理. *设 $K\subseteq F\subseteq E$ 是域. 设 $\alpha\in E$. 则*

$$|F(\alpha):F|\le|K(\alpha):K|\le|E:K|\,.$$

证. 先证前一不等式. 如果 $|K(\alpha):K|=\infty$ (即 α 是 K 上的超越元), 显然成立. 再设 $|K(\alpha):K|=n<\infty$, 由引理 4.3.2, α 是 K 上的代数元; 那么 α 在 K 上的极小多项式形如 $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$, 其中各系数 $a_i\in K$. 但 $K\subseteq F$, 即 $p(x)$ 也是 F 上的多项式, 它零化 α; 所以 α 在 F 上的极小多项式 $q(x)|p(x)$. 因此

$$|F(\alpha):F|=\deg q(x)\leq\deg p(x)=|K(\alpha):K|\ .$$

后一不等式是显然的：因为 $K\subseteq K(\alpha)\subseteq E$, 由次数公式 4.1.2 即可推出结论： $|E:K|=|E:K(\alpha)|\cdot|K(\alpha):K|$. □

例. 取 $K=\mathbb{Q}$, $F=\mathbb{R}$, $E=\mathbb{C}$, 取 $\alpha=\frac{1}{\sqrt{2}}(1+\mathrm{i})$, 其中 $\mathrm{i}=\sqrt{-1}$. 则 $|F(\alpha):F|=2$, $|K(\alpha):K|=4$.

证. 对 $\alpha=\frac{1}{\sqrt{2}}(1+\mathrm{i})$; 两边平方, 得 $\alpha^2=\mathrm{i}$, 再平方得 $\alpha^4=-1$; 即 x^4+1 是 α 的零化多项式. 易验证这个多项式在有理数域上不可约, 所以它就是 α 在 $K=\mathbb{Q}$ 上的极小多项式; 因此 $|K(\alpha):K|=4$.

但 $\mathrm{i}=\sqrt{2}\alpha-1\in F(\alpha)$, 故 $F(\alpha)=E=\mathbb{C}$. 所以 $|F(\alpha):F|=2$. (又证: $x^4+1=x^4+2x^2+1-2x^2=(x^2+1)^2-2x^2=(x^2+1+\sqrt{2}x)(x^2+1-\sqrt{2}x)$, 由于 $\alpha^2=\mathrm{i}$, 所以 $x^2+1-\sqrt{2}x$ 零化 α; 而 $x^2+1-\sqrt{2}x$ 是实不可约多项式 (它的判别式 <0), 所以它是 α 在 $F=\mathbb{R}$ 上的极小多项式; 因而 $|F(\alpha):F|=2$.)

4.3.4 定理. (1) *F 是域 K 的有限次扩张当且仅当 F 在 K 上由有限个代数元生成; 此时 F 必为 K 的代数扩张.*

(2) *F 是域 K 的代数扩张当且仅当 F 在 K 上由代数元生成.*

证. (1). 必要性. 设 $|F:K|=n<\infty$. $n=1$ 时 $F=K=K(1)$. 设 $n>1$, 那么有 $\alpha_1\in F-K$, 则 $K(\alpha_1)\supsetneqq K$, 故 $|K(\alpha_1):K|>1$; 由次数公式 $n=|F:K|=|F:K(\alpha_1)|\cdot|K(\alpha_1):K|$, 故 $|F:K(\alpha_1)|<n$. 按归纳法,

$$F=K(\alpha_1)(\alpha_2,\cdots,\alpha_k)=K(\alpha_1,\alpha_2,\cdots,\alpha_k)\ ;$$

对每 α_i 有 $|K(\alpha_i):K|\leq|F:K|<\infty$, 据引理 4.3.2, 每 α_i 都是 K 上的代数元. 对任 $\alpha\in F$, 都有 $|K(\alpha):K|\leq|F:K|<\infty$, 即 α 是 K 上的代数元; 故 F 是 K 的代数扩张.

充分性. 设 $F=K(\alpha_1,\cdots,\alpha_n)$, 其中每 α_i 是 K 上的代数元, 即 $|K(\alpha_i):K|<\infty$. 根据引理 4.3.3,

$$|K(\alpha_1,\cdots,\alpha_{i-1},\alpha_i):K(\alpha_1,\cdots,\alpha_{i-1})|\leq|K(\alpha_i):K|<\infty\ .$$

再引用次数公式, 得

$$\begin{aligned}|F:K| &= |K(\alpha_1,\cdots,\alpha_{n-1},\alpha_n):K|\\ &= |K(\alpha_1,\cdots,\alpha_{n-1},\alpha_n):K(\alpha_1,\cdots,\alpha_{n-1})|\cdots|K(\alpha_1):K|\\ &\leq |K(\alpha_n):K|\cdot|K(\alpha_{n-1}):K|\cdots|K(\alpha_1):K|<\infty\ .\end{aligned}$$

(2). 必要性. 设 F 是域 K 的代数扩张, 则 $S = F - K$ (差集) 的每个元都是 K 上的代数元, 而且显然 $F = K(S)$.

充分性. 设 $F = K(S)$, 其中 S 的每个元素都是 K 上的代数元. 设 $\alpha \in K(S)$. 由推论 4.1.5, 存在 $\alpha_1, \cdots, \alpha_n \in S$ 使得 $\alpha \in K(\alpha_1, \cdots, \alpha_n)$. 而每 α_i 是 K 上的代数元, 按结论 (1),

$$|K(\alpha_1, \cdots, \alpha_n) : K| < \infty \ .$$

而, $\alpha \in K(\alpha_1, \cdots, \alpha_n)$, 由引理 4.3.3,

$$|K(\alpha) : K| \leq |K(\alpha_1, \cdots, \alpha_n) : K| < \infty \ ;$$

因此 α 是 K 上的代数元. □

4.3.5 推论. *若 E 是 F 的代数扩张而 F 是 K 的代数扩张, 则 E 是 K 的代数扩张.*

证. 设 $\alpha \in E$. 则 α 是 F 上的代数元, 即有多项式

$$f(x) = \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0 \ , \qquad \alpha_n, \cdots, \alpha_1, \alpha_0 \in F \ ,$$

使得 $f(\alpha) = 0$. 但多项式 $f(x)$ 的系数都在域 $K' = K(\alpha_0, \alpha_1, \cdots, \alpha_n)$ 之中, 所以 α 是域 K' 上的代数元, 故 $|K'(\alpha) : K'| < \infty$. 而 $\alpha_0, \alpha_1, \cdots, \alpha_n$ 都是 F 中的元从而是 K 上的代数元, 由定理 4.3.4(1), $|K' : K| < \infty$. 因此

$$|K(\alpha) : K| \leq |K'(\alpha) : K| = |K'(\alpha) : K'| \cdot |K' : K| < \infty \ ;$$

所以 α 是 K 的代数元. □

4.3.6 定义. (1). 如果域 F 没有真正的代数扩域, 即只要 E 是 F 的代数扩域就必有 $E = F$, 就称 F 是 *代数闭域*.

(2). 如果 F 是 K 的代数扩张而且 F 是代数闭域, 就称 F 是 K 的 *代数闭包*.

例. 后面将证明 $\mathbb{C}$ 是代数闭域. 而已知 $\mathbb{C}$ 是 $\mathbb{R}$ 的代数扩张 (习题 2), 所以 $\mathbb{C}$ 是 $\mathbb{R}$ 的代数闭包.

下面给出代数闭包的一个判别法它也提供了构造代数闭包的方法.

4.3.7 命题. *如果 F 是域 K 的代数扩张, 而且 $K[x]$ 的任何多项式在 F 中可分裂为一次因式之积, 则 F 是 K 的代数闭包.*

证. 只需证明 F 是代数闭域. 设 E 是 F 的代数扩张, 设 $\alpha \in E$. 那么 α 是 F 上的代数元, 即存在 $f(x) = a_0 + \cdots + a_m x^m \in F[x]$ 使得 $f(\alpha) = 0$. 而 $f(x)$ 的系数在域 $K' = K(a_0, \cdots, a_m)$ 之中, 所以 α 是 K' 上的代数元, 特别有 $|K'(\alpha) : K'| < \infty$. 按假设, $a_0, \cdots, a_m$ 都是 K 上的代数元. 根据定理 3.2.7, $|K' : K| < \infty$. 因此

$$|K'(\alpha) : K| = |K'(\alpha) : K'| \cdot |K' : K| < \infty \ .$$

而 $|K(\alpha):K| \le |K'(\alpha):K|$, 所以 $K(\alpha)$ 也是 K 的有限扩张. 故 α 是一个 K 上的多项式 $h(x)$ 的根; 但按假设, $h(x)$ 的根都在 F 之中, 即 $\alpha \in F$. 总之, 得 $E = F$. □

4.3.8 定理. *任意域的代数闭包存在且在同构意义下唯一.*

从 4.2.9 和 4.3.7, 利用 *超限归纳法*, 可以完成证明. 但我们没有介绍超限归纳法, 故这里略去证明. □

习题 4.3

1. 证明 $\mathbb{C}$ 是 $\mathbb{R}$ 的代数扩张, 但不是 $\mathbb{Q}$ 的代数扩张.

2. 如果 $a \in \mathbb{C}$ 是一个有理多项式的根就称 a 是一个 *代数数*. 所有代数数的集合记作 $\mathbb{A}$. 证明:

(1) 两个代数数的和, 差, 积, 商仍为代数数. $\mathbb{A}$ 是 $\mathbb{C}$ 的子域.

(2) $\mathbb{A}$ 是 $\mathbb{Q}$ 的代数扩张. (称为 *代数数域*).

(3) 在代数基本定理的基础上证明 $\mathbb{A}$ 是 $\mathbb{Q}$ 的代数闭包 (称 $\mathbb{A}$ 为 *代数数域*).

3. 求 $x^4 - 1$ 在 $\mathbb{Q}$ 上的分裂域.

4. 求 $x^{p^n} - 1$ 在 $\mathbb{Z}_p$ 上的分裂域.

5. 令 $\omega = e^{2\pi \mathrm{i}/n}$ 其中 $\mathrm{i} = \sqrt{-1}$. 证明: $\mathbb{Q}(\sqrt[n]{2},\ \omega)$ 是 $x^n - 2$ 在 $\mathbb{Q}$ 上的分裂域.

6. 设 K 是域, $f(x) \in K[x]$, $\deg f(x) = n$. 设 F 是 $f(x)$ 在 K 上的分裂域. 证明 $|F:K|$ 是 $n!$ 的约数.

§4.4 直尺圆规作图

概要: *尺规作图规则的代数化; 可作性判别; 三个古典作图问题; 正多边形作图.*

直尺圆规作图, 以下简称 *尺规作图*, 是在平面上从一些已知图形出发用直尺和圆规按两条规则作新图形: 通过已知两点作直线, 通过已知点和已知半径作圆.

仔细分析会发现: 第一, 所谓已知半径并非从度量仪器取得的长度, 而是从两已知点决定的线段; 第二, 所谓作直线作圆只是形象说法, 并非作的直线作的圆上任意点都可用作下一步作图的已知点,

只是作的直线作的圆的交点可用作下一步作图的已知点; 第三, 所谓作出新图形如三角形或者圆, 实际上是作出决定该图形的点, 如三角形就是三个点, 圆也是三个点 (一个圆心一条线段).

因此可叙述如下 (以点 P 为圆心线段 P_1P_2 为半径的圆写作 圆 $(P_3, \overline{P_4P_5})$):

4.4.1 尺规作图规则.

操作对象: 平面上的一个有限点集 Ω_0, $|\Omega_0| \ge 2$. 从 $\Omega = \Omega_0$ 开始操作.

操作步骤: 对 $P_1, P_2, P_3, P_4, P_5, P_6 \in \Omega$,

1) 如果直线 P_1P_2 与直线 P_3P_4 相交则将交点作为新的已知点加入 Ω;

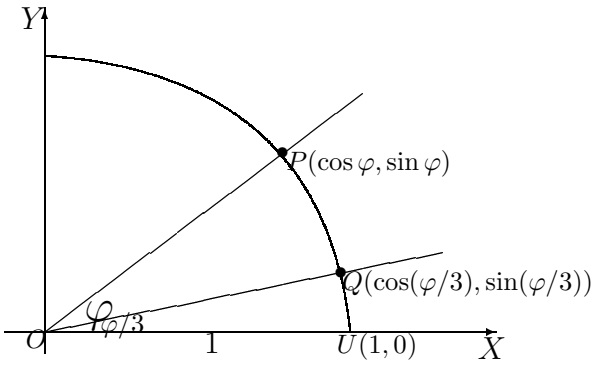
2) 如果直线 P_1P_2 与圆 $(P_3, \overline{P_4P_5})$ 相交则将交点作为新的已知点加入 Ω;

3) 如果圆 $(P_1, \overline{P_2P_3})$ 与圆 $(P_4, \overline{P_5P_6})$ 相交则将交点作为新的已知点加入 Ω.

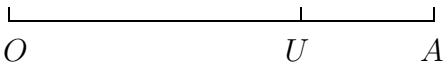
尺规作图问题: 给定初始点集 Ω_0, 给定求作点 Q(或求作线段 $Q'Q''$); 从点集 $\Omega = \Omega_0$ 开始, 能否经有限步操作使得 $Q \in \Omega$ (或有 $P', P'' \in \Omega$ 使得 (线段 $P'P''$ 长) = (线段 $Q'Q''$ 长))?

4.4.2 三个古典尺规作图问题.

(A) 三等分角. 已知点 O, U, P; 求点 Q 使得 角$QOU = \frac{1}{3}$(角POU). 图示:



(B) 倍立方. 给定点 O, U; 求点 A 使得 (线段 $OA)^3 = 2$(线段 $OU)^3$. 图示:



(C) 化圆为方. 已知点 O, U; 求作线段其长度 x 满足 $x^2 = \pi \cdot$(线段$OU)^2$, 这里 π 是圆周率.

通过建立适当坐标系把尺规作图问题从几何语言转化为代数语言.

初始点集 Ω_0 至少有两个点 O, U; 以 O 为原点以线段 OU 为单位长建立直角坐标系让 U 在 X 正反向上. 这样任 $P \in \Omega_0$ 的坐标 $P(x_P, y_P)$ 作为初始数据, 得到有限个实数的集合 $\Gamma_0 = \{\, x_P, y_P \mid P \in \Omega_0\}$. 特别的, $O(0,0), U(1,0) \in \Omega_0$, 故 $0, 1 \in \Gamma_0$. 求作点 (或求作线段) 当然也由坐标决定, 故可称为求作数. 例如上面 "三等分角" 问题的示意图, $\Gamma_0 = \{\, 0, 1, \cos\varphi, \sin\varphi \,\}$. 求作数是 $\cos(\varphi/3)$, $\sin(\varphi/3)$. 再把 4.4.1 中的操作步骤转化为代数语言, 注意: 通过点 $(a_1, b_1), (a_2, b_2)$ 的直线方程是 $(b_2 - b_1)(x - a_1) = (a_2 - a_1)(y - b_1)$; 以点 (a_1, b_1) 为圆心以点 (a_2, b_2) 到点 (a_3, b_3) 线段为半径的圆的方程是 $(x - a_1)^2 + (y - b_1)^2 = (a_3 - a_2)^2 + (b_3 - b_2)^2$; 就可陈述如下:

4.4.3 尺规作图规则 (代数陈述).

操作对象: 有限集 $\Gamma_0 \subseteq \mathbb{R}$, $0, 1 \in \Gamma_0$. 从 $\Gamma = \Gamma_0$ 开始操作.

操作步骤: 对 $a_1,b_1,a_2,b_2,a_3,b_3,a_4,b_4,a_5,b_5,a_6,b_6\in\Gamma$,

1) 如果方程组 $\begin{cases}(b_2-b_1)(x-a_1)=(a_2-a_1)(y-b_1)\\(b_4-b_3)(x-a_3)=(a_4-a_3)(y-b_3)\end{cases}$ 有解则将解作为新的已知实数加入 Γ;

2) 如果方程组 $\begin{cases}(b_2-b_1)(x-a_1) &= (a_2-a_1)(y-b_1)\\(x-a_3)^2+(y-b_3)^2 &= (a_5-a_4)^2+(b_5-b_4)^2\end{cases}$ 有解则将解作为新的已知实数加入 Γ;

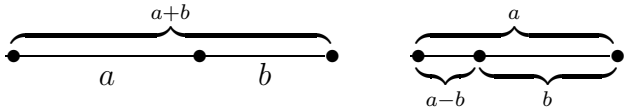
3) 如果方程组 $\begin{cases}(x-a_1)^2+(y-b_1)^2 &= (a_3-a_2)^2+(b_3-b_2)^2\\(x-a_4)^2+(y-b_4)^2 &= (a_6-a_5)^2+(b_6-b_5)^2\end{cases}$ 有解则将解作为新的已知实数加入 Γ.

尺规作图问题: 给定初始实数集 Γ_0, 给定求作实数 α; 从点集 $\Gamma=\Gamma_0$ 开始, 能否经有限步操作使得 $\alpha\in\Gamma$?

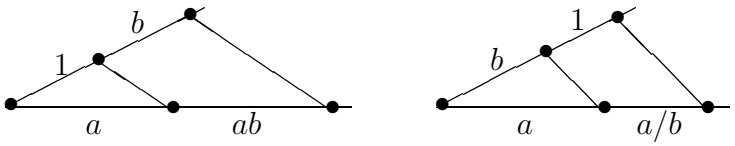
定义. 如果答案是 "能", 就说实数 α 可从有限实数集 Γ_0 尺规作出; 在默认初始有限实数集 Γ_0 时, 简称实数 α 可作.

4.4.4 引理. *如果实数 a,b 可作, 则 $a+b$, $a-b$, ab 可作, 且 $b\neq 0$ 时 a/b 可作.*

证. $a+b$ 和 $a-b$ 作法如下:



ab 和 a/b 都可用 "平行线截线段成比例" 来完成如下:



4.4.5 推论. *有理数域上由 Γ_0 生成的扩域 $K_0:=\mathbb{Q}(\Gamma_0)$ 的每个数可作.*

证. 任何有理数可作. 因为 $0,1\in\Gamma_0$, 对任正整数 n, 将 1 反复加 n 次得到 $n\in\Gamma$, 对负整数类似地做. 对 m/n 按引理 4.4.4 也只需有限步可作出.

再设 $\alpha\in K_0$. 由引理 4.1.4, 存在 $f(x_1,\cdots,x_n)$, $g(x_1,\cdots,x_n)\in\mathbb{Q}[x_1,\cdots,x_n]$ 和 $a_1,\cdots,a_n\in\Gamma_0$ 使得 $\alpha=\frac{f(a_1,\cdots,a_n)}{g(a_1,\cdots,a_n)}$. 因为 $f(x_1,\cdots,x_n)$, $g(x_1,\cdots,x_n)$ 的系数只涉及有限个有理数它们经有限步操作作出来, 而 α 通过 $a_1,\cdots,a_n$ 与这有限个有理数经过有限次加减乘除得出, 那么由引理 4.4.4, α 是可作的. □

完全相同的论证可证明下述更一般结论.

4.4.6 命题. *设 $K\subseteq\mathbb{R}$, $\alpha\in\mathbb{R}$. 如果 K 的每个数可作而且 α 可作, 则 $K(\alpha)$ 的每个数可作.* □

现在从初始有限集 $\Gamma_0 \subseteq \mathbb{R}, 0, 1 \in \Gamma_0$, 开始. 虽然 4.4.3 的每种操作所产生的实数不一定是一个, 但为了简单我们不妨每次只添加一个作出的实数到 Γ 中. 假定我们经过有限步操作添加了 $\alpha_1, \cdots, \alpha_n$ 到 Γ 中, 最后的 α_n 是我们求作的实数. 从 $K_0 = \mathbb{Q}(\Gamma_0)$ 开始, 令

$$K_1 = K_0(\alpha_1), \quad K_2 = K_1(\alpha_2), \quad \cdots, \quad K_n = K_{n-1}(\alpha_n)\ ;$$

这就得到 $\mathbb{R}$ 内的域扩张链

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{i-1} \subseteq K_i \subseteq \cdots \subseteq K_n\ . \tag{$*$}$$

考察其中从任 K_{i-1} 到 $K_i = K_{i-1}(\alpha_i)$ 的单扩张, α_i 是 4.4.3 中 (1),(2),(3) 三类方程组之一的解, 而方程的系数都在 K_{i-1} 中. 分别情形讨论.

- 如果 α_i 是 4.4.3 方程组 (1) 的解, 因为是线性方程组, 所以 $\alpha_i \in K_{i-1}$; 故 $K_i = K_{i-1}$.
- 如果 α_i 是 4.4.3 方程组 (2) 的解, 从方程组的第一个线性方程可消去第二个方程的一个未知数得到一个一元二次方程 (或一次方程)$f(x) = 0$, α_i 是它的解即 $f(\alpha) = 0$; 所以 α 是 K_{i-1} 上的代数元而且, 根据 4.2.2 后的注解, α_i 的极小多项式是 $f(x)$ 的因式, 故为一次的或二次的多项式. 根据定理 4.2.5, $|K_i : K_{i-1}| = |K_{i-1}(\alpha) : K_{i-1}| \leq 2$.
- 最后, 设 α_i 是 4.4.3 方程组 (3) 的解, 为简单, 把方程组写为

$$\begin{cases} (x-c_1)^2 + (y-d_1)^2 - e_1^2 &= 0\,, \\ (x-c_2)^2 + (y-d_2)^2 - e_2^2 &= 0\,; \end{cases} \qquad c_1, d_1, e_1, c_2, d_2, e_2 \in K_{i-1}\ .$$

两方程相减产生一个一次方程

$$(c_2 - c_1)(2x - c_1 - c_2) + (d_2 - d_1)(2y - d_1 - d_2) + (e_2^2 - e_1^2) = 0\ ;$$

用它消去二次方程的一个未知元, 象上面一样得一个一元二次方程 (或一次方程)$f(x) = 0$, 于是仍然得到 $|K_i : K_{i-1}| = |K_{i-1}(\alpha) : K_{i-1}| \leq 2$.

总之, 扩张链 $(*)$ 的任一项对前项的次数 ≤ 2. 当然我们可以去掉 $(*)$ 中的重复项使得任一项对前项的次数 $= 2$.

这样, 我们就得到了一个实数可作的必要条件, 即已证得下述定理的必要性部分.

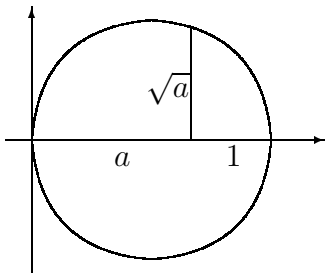
4.4.7 定理. *设有限集 $\Gamma_0 \subseteq \mathbb{R}, 0, 1 \in \Gamma_0$; 令 $K_0 = \mathbb{Q}(\Gamma_0)$. 那么实数 α 可从 Γ_0 尺规作出当且仅当存在实数域内的域扩张链*

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n\ ,$$

使得 $|K_i : K_{i-1}| = 2$ 其中 $i = 1, \cdots, n$, 且 $\alpha \in K_n$.

证. 对 n 归纳证明充分性. 设 $n = 0$. 推论 4.4.5 已指出 K_0 的元都可作出; $\alpha \in K_n = K_0$, 故 α 可作.

再设 $n > 0$, 按归纳假设 K_{n-1} 的元都可作出. 因为 $|K_n : K_{n-1}| = 2$, 由例 4.2.4, 存在 $a \in K_{n-1}$ 使得 $K_n = K_{n-1}(\sqrt{a})$. 那么 a 已经是可作的. 再按下图操作:



$a+1$ 可作；已知线段的中点可作，于是以 $a+1$ 为直径的圆可作；过直线上定点的直线的垂线可作，于是垂线与圆的的交点可作，它的纵坐标就是 $\sqrt{a}$; 即 $\sqrt{a}$ 是可作的. 最后，由命题 4.4.6, $K_n = K_{n-1}(\sqrt{a})$ 的每个元可作. 而 $\alpha \in K_n$, 所以 α 可从 Γ_0 尺规作出. □

注. 这个定理也可以用复数的形式陈述, 见 N. Jacobson, Basic Algebra I, W.H. Freeman and Company, San Francisco, 1974; §4.2.

注. 因为 $\alpha \in K_n$, 所以 $K_0 \subseteq K_0(\alpha) \subseteq K_n$; 由次数公式

$$|K_n : K_0(\alpha)| \cdot |K_0(\alpha) : K_0| = |K_n : K_0| = 2^n ;$$

所以

$$|K_0(\alpha) : K_0| = 2^k .$$

也就是说我们证明了下述定理的必要性部分.

4.4.8 定理. 实数 α 可从含 0 与 1 的实数有限集 Γ_0 尺规作出的充分必要条件是 $|K_0(\alpha) : K_0| = 2^k$ 是 2 的幂，其中 $K_0 = \mathbb{Q}(\Gamma_0)$.

从域扩张的 Galois 理论很容易推出充分性. 但介绍 Galois 理论需要较大篇幅，这里不可能做这件事了. □

现在我们容易指出： 4.4.2 中的 “倍立方” 和 “化圆为方” 都是直尺圆规不可作问题.

例. 对 4.4.2(B)“倍立方” 问题，取立方体的边长为单位长，即那里图示中的线段 OU 长度 1; 则 $K_0 = \mathbb{Q}$. 要作的线段 OA 长 $\sqrt[3]{2}$. 但 $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ 不是 2 的幂，所以 $\sqrt[3]{2}$ 不能直尺圆规作出.

例. 对 4.4.2(C)“化圆为方” 问题，取圆半径是单位长，同样得 $K_0 = \mathbb{Q}$, 要作 α 使得 $\alpha^2 = \pi$, 即 $\alpha = \sqrt{\pi}$. 但由例 4.2.3(2), $|\mathbb{Q}(\pi) : \mathbb{Q}| = \infty$, 故

$$|\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)| \cdot |\mathbb{Q}(\pi) : \mathbb{Q}| = \infty .$$

所以 π 不能直尺圆规作出.

对 “三等分角” 问题，则有

4.4.9 命题. 一个角 φ 可以三等分当且仅当 $4x^3 - 3x + \sin\varphi$ 是 $\mathbb{Q}(\sin\varphi, \cos\varphi)$ 上的可约多项式.

证. 由条件, $\Gamma_0=\{0,1,\sin\varphi,\cos\varphi\}$, 即 $K_0=\mathbb{Q}(\sin\varphi,\cos\varphi)$. 将 φ 三等分就是求作 $\sin(\varphi/3)$. 由三角公式, $\sin(\varphi/3)$ 是多项式 $4x^3-3x+\sin\varphi$ 的根; 所以 $\sin(\varphi/3)$ 在 K_0 上的极小多项式是 $4x^3-3x+\sin\varphi$ 在 $K_0[x]$ 的不可约因式. 而 $|K_0(\sin(\varphi/3):K_0|$ 等于这个极小多项式的次数. 因此 $|K_0(\sin(\varphi/3):K_0|\le 2$ 当且仅当 $4x^3-3x+\sin\varphi$ 是 $\mathbb{Q}(\sin\varphi,\cos\varphi)$ 上的可约多项式. □

例. 如果 $\varphi=90^o$. 则 $\sin\varphi=1$ 而 $4x^3-3x+1=(2x-1)(2x^2+x-1)$; 故 $\varphi=90^o$ 可以直尺圆规三等分.

例. 设 $\varphi=30^o$. 则 $\sin\varphi=1/2$, $\cos\varphi=\sqrt{3}/2$, $K_0=\mathbb{Q}(\sqrt{3})$. 求作 $\beta=\sin(\varphi/3)$. 我们要看 $4x^3-3x+\frac{1}{2}$ 在 K_0 上是否可约, 等价的, 要看 $f(x)=8x^3-6x+1$ 在 K_0 上是否可约. 若 $f(x)$ 在 K_0 上可约, 则 $|K_0(\beta):K_0|=1$ 或 2; 由次数公式,

$$|\mathbb{Q}(\sqrt{3},\beta):\mathbb{Q}|=|\mathbb{Q}(\sqrt{3},\beta):\mathbb{Q}(\sqrt{3})|\cdot|\mathbb{Q}(\sqrt{3}:\mathbb{Q}|=2\text{ 或 }4\ ;$$

而 $|\mathbb{Q}(\beta):\mathbb{Q}|\ \Big|\ |\mathbb{Q}(\sqrt{3},\beta):\mathbb{Q}|$; 且 $f(x)$ 零化 β, 故 $|\mathbb{Q}(\beta):\mathbb{Q}|\le 3$; 所以 $|\mathbb{Q}(\beta):\mathbb{Q}|=2$ 或 1. 那么 $f(x)$ 在 $\mathbb{Q}[x]$ 中有二次或 1 次因式. 总之 $f(x)$ 在 $\mathbb{Q}$ 有根. 设 $a/b\in\mathbb{Q}$ 是它的根, 则必有 $a=\pm1$ 而 $b=1,2,4,8$; 但马上可验证这些都不是 $f(x)$ 的根. 所以 $\varphi=30^o$ 不能用直尺圆规三等分.

再讨论正多边形的几何作图.

4.4.10 命题. *设 p 是一个素数. 那么正 p 边形可以直尺圆规作出的必要充分条件是 $p=2^{2^m}+1$ 是 Fermat 素数.*

证. 正 p 边形可以直尺圆规作出就是说 $\cos\frac{2\pi}{p}$, $\sin\frac{2\pi}{p}$ 可以直尺圆规作出. 由定理 4.4.8, 得: 正 p 边形尺规可作当且仅当 $|\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p}):\mathbb{Q}|=2^n$.

设 $|\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p}):\mathbb{Q}|=k$. 令 $\zeta=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$ 是 p 次本原单位根; 那么 $\mathbb{Q}(\zeta,\mathrm{i})=\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p},\mathrm{i})$, 但

$$|\mathbb{Q}(\zeta,\mathrm{i}):\mathbb{Q}(\zeta)|=2=|\mathbb{Q}(\cos\tfrac{2\pi}{p},\sin\tfrac{2\pi}{p},\mathrm{i}):\mathbb{Q}(\cos\tfrac{2\pi}{p},\sin\tfrac{2\pi}{p})|$$

故 $|\mathbb{Q}(\zeta):\mathbb{Q}|=k$. 由于 $x^p-1=(x-1)(x^{p-1}+\cdots+x+1)$, 可知 ζ 是 $x^{p-1}+\cdots+x+1$ 的根. 从 Eisenstein 判别法知 $x^{p-1}+\cdots+x+1$ 是有理不可约多项式 (见习题 3.7.6), 所以 $|\mathbb{Q}(\zeta):\mathbb{Q}|=p-1$. 综上得 $p-1=k$, 即 $p=k+1$.

正 p 边形尺规可作当且仅当 $k=2^n$, 当且仅当 $p=2^n+1$. 若 $n=st$ 且 $t>1$ 是奇数, 则 $2^n+1=(2^s+1)\Big((2^s)^{t-1}-(2^s)^{t-2}+\cdots+(-1)^{t-1}\Big)$ 就不是素数. 因而 $n=2^m$, 即 $p=2^{2^m}+1$ 是 Fermat 素数. □

注. 从这命题, 马上知道正 7 边形, 正 11 边形和正 13 边形都是不能用尺规作出的. 另一方面, 前三个 Fermat 素数是 3, 5, 17. 正三边形和正五边形的尺规作图法是早已知道的. 高斯 (Gauss) 给出了正 17 边形的尺规作图法.

习题 4.3

1. 证明 72^o 可以直尺圆规三等分；但 60^o 不能直尺圆规三等分.

2. 证明正 9 边形不能用直尺圆规作出.

§4.5 代数基本定理

复数域 $\mathbb{C}$ 是实数域 $\mathbb{R}$ 的二次代数扩张 $\mathbb{C} = \mathbb{R}(\mathbf{i})$, 其中 $\mathbf{i} = \sqrt{-1}$; 所以作为实向量空间, $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}\mathbf{i}$.

4.5.1 代数基本定理. *复数域上的非常数多项式一定有复根.*

证. 设 $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{C}[x]$, $a_n = 1$, $n > 0$. 记 $\bar{f}(x) = \sum_{k=0}^{n} \bar{a}_k x^k$, 它是 $f(x)$ 的复共轭多项式；这里 $\bar{a}_k$ 是复数 a_k 的共轭复数. 那么

$$\overline{f(x)\bar{f}(x)} = \bar{f}(x)f(x) = f(x)\bar{f}(x) \,,$$

所以 $f(x)\bar{f}(x)$ 是实多项式. 如果 $f(x)\bar{f}(x)$ 有复根 α, 则 α 或者是 $f(x)$ 的根或者是 $\bar{f}(x)$ 的根；在后一情形, $\bar{\alpha}$ 就是 $f(x)$ 的根. 所以我们只要证明非常数首一实多项式一定有复根，就可以完成证明.

以下设 $f(x)$ 是实多项式，设 $\deg f(x) = n = 2^\ell d$, 其中 d 是奇数, $\ell \geq 0$. 对 ℓ 归纳证明: $f(x)$ 有复根.

先设 $\ell = 0$, 即 $f(x)$ 是奇次数的实多项式，它作为实函数在全实数轴上连续. 在 x 充分大的时候, $f(x)$ 的值的符号由首项系数的符号确定；而已假定 $f(x)$ 是首一的，所以在 $x \to +\infty$ 时 $f(x) > 0$, 而在 $x \to -\infty$ 时 $f(x) < 0$. 由连续函数的性质，存在实数 α 使得 $f(\alpha) = 0$. 结论成立.

再设 $\ell > 0$. 由定理 4.2.9, 存在 $\mathbb{C}$ 的扩张 E 使得 $f(x)$ 在 E 中有 n 个根 $\alpha_1, \cdots, \alpha_n$, 即

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \,. \tag{A}$$

任给定 $r \in \mathbb{R}$. 令

$$\beta_{ij} = \alpha_i \alpha_j + r(\alpha_i + \alpha_j) \qquad 1 \leq i < j \leq n \,; \tag{B}$$

并且令

$$g(x) = \prod_{1 \leq i < j \leq n} (x - \beta_{ij}). \tag{G}$$

那么

$$\deg g(x) = \frac{1}{2} n(n-1) = 2^{\ell-1}(d(2^\ell d - 1))$$

其中 $d(2^\ell d - 1)$ 是一个奇数；以下证明 $g(x)$ 是实多项式，如此就可按归纳法，得出 $g(x)$ 有复根. $g(x)$ 的系数可以表写成 β_{ij} 的对称多项式，从 (B) 式易检验, β_{ij} 的任一对称多项式用 (B) 代换以后就成为 $\alpha_1, \cdots, \alpha_n$ 的对称多项式，故可以表写成 α_i 的对称多项式；所

以 $g(x)$ 的系数可以表写成 α_i 的对称多项式. 再由对称多项式基本定理 2.4.8, α_i 的对称多项式都可以表写成 α_i 的初等对称多项式的表达式, 也就是 $f(x)$ 的系数的多项式 (见 (A) 式), 因此一定是实数. 也就是说 β_{ij} 的对称多项式是实数; 即得知 $g(x)$ 的系数是实数. 所以按归纳法, 得出 $g(x)$ 有复根. 由 $g(x)$ 的构造 (G) 式, 至少一个 $\beta_{ij} \in \mathbb{C}$.

小结上段, 就是说对任一 $r \in \mathbb{R}$ 有一对指标 (i,j) 使得 $\beta_{ij} = \alpha_i\alpha_j + r(\alpha_i + \alpha_j) \in \mathbb{C}$. 指标对 (i,j) 只有 $n(n-1)/2$ 个, 然而实数 $\mathbb{R}$ 有无限多; 所以一定有指标对 (i,j) 使得至少有两个不相等的实数 $r \neq r' \in \mathbb{R}$ 满足

$$c = \alpha_i\alpha_j + r(\alpha_i + \alpha_j) \in \mathbb{C} \qquad \text{且} \qquad c' = \alpha_i\alpha_j + r'(\alpha_i + \alpha_j) \in \mathbb{C}.$$

那么

$$\alpha_i + \alpha_j = \frac{c - c'}{r - r'} \in \mathbb{C} \qquad \text{且} \qquad \alpha_i\alpha_j = \frac{rc' - r'c}{r - r'} \in \mathbb{C}.$$

所以 α_i 和 α_j 是二次复多项式 $x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j$ 的根; 由二次多项式的求根公式得 $\alpha_i, \alpha_j \in \mathbb{C}$. 也就是说 α_i 和 α_j 是 $f(x)$ 的复根. □

代数基本定理有一些形式上不同的表述方式.

4.5.2 命题. *以下陈述彼此等价:*

(1) *复数域上的非常数多项式一定有复根.*

(2) *复数域上的不可约多项式只有一次多项式.*

(3) *复数域是代数闭域.*

(4) *复数域是实数域的代数闭包.*

证. (1) ⇒ (2). 一次多项式不可能有真因式, 当然是不可约多项式. 如果复多项式 $f(x)$ 的次数 $\deg f(x) > 1$, 由 (1), $f(x)$ 有复根 α, 那么 $x - \alpha \mid f(x)$, $f(x) = (x - \alpha)g(x)$; 按次数公式, $\deg g(x) > 0$. 所以 $f(x)$ 可约. 所以 (2) 成立.

(2) ⇒ (3). 设 E 是 $\mathbb{C}$ 的代数扩张, 设 $\alpha \in E$. 那么 α 是 $\mathbb{C}$ 的代数元, 它的极小多项式 $g(x)$ 是 $\mathbb{C}$ 上的不可约多项式. 由 (2), $g(x) = ax + b$ 是一次多项式, 其中 $a, b \in \mathbb{C}$ 且 $a \neq 0$. 而 $g(\alpha) = 0$, 故 $\alpha = -b/a \in \mathbb{C}$. 所以 $E = \mathbb{C}$. 即 $\mathbb{C}$ 没有真代数扩张, $\mathbb{C}$ 是代数闭域.

(3) ⇒ (4). $\mathbb{C}$ 是 $\mathbb{R}$ 的代数扩张, 由 (3), $\mathbb{C}$ 还是代数闭域. 即: $\mathbb{C}$ 是 $\mathbb{R}$ 的代数闭包.

(4) ⇒ (1). 注意 $\mathbb{C}$ 是 $\mathbb{R}$ 的代数闭包已蕴含 $\mathbb{C}$ 是代数闭域. 设 $f(x)$ 是复多项式且 $\deg f(x) > 0$, 设 $p(x)$ 是 $f(x)$ 的不可约因式. 如果 $\deg p(x) > 1$, 由命题 4.2.9, $\mathbb{C}$ 有代数扩张 $\mathbb{C}(\alpha)$ 使得 $|\mathbb{C}(\alpha) : \mathbb{C}| = degp(x)$, $\mathbb{C}(\alpha)$ 就是 $\mathbb{C}$ 的真代数扩张, 与 (4) 矛盾. 故 $\deg p(x) = 1$. 令 $p(x) = ax + b$, 则 $-b/a$ 是 $p(x)$ 的复根因而也是 $f(x)$ 的复根. □

注. 由 4.5.1, 我们知道 4.5.2 中的四条陈述都是正确的, 它们中任何一条都可作为 "代数基本定理" 的陈述方式.

注. 由于复数域上多项式环因式分解定理成立, 所以 4.5.2 的陈述 (2) 还意味着任何 n ($n > 0$) 次多项式 $f(x)$ 可以分裂为 n 个一次多项式之积, 也就是 $f(x)$ 的 n 个根 (计重

数) 全在复数域中. 所以代数基本定理还可陈述为: "任何非常数复多项式可以分裂为一次多项式之积".

习题 4.5

1. 证明: 不可约实多项式只有两类: 1 次多项式, 形如 ax^2+bx+c, 其中 $b^2-4ac<0$, 的二次多项式.

2. 如果 $\mathbb{R}(\gamma)$ 是 $\mathbb{R}$ 的真代数扩张, 那么 $\mathbb{R}(\gamma)=\mathbb{R}(\sqrt{-1})$. (提示: 由上题, $|\mathbb{R}(\gamma):\mathbb{R}|=2$; 由例 4.2.4, 存在 $\sigma\in\mathbb{R}(\gamma)$ 使得 $\sigma^2=a\in\mathbb{R}$ 且 $\mathbb{R}(\gamma)=\mathbb{R}(\sqrt{a})$, 此时必有 $a<0$.)

§4.6 四元数系

简单回顾:

- 从自然数的公理开始, 得到整数环.
- 通过分式化 (局部化) 从整数环构造出有理数域.
- 通过完备化从有理数域构造出实数域.
- 通过代数扩张从实数域得到复数域.

作为实二维空间, $\mathbb{C}=\mathbb{R}\oplus\mathbb{R}\mathbf{i}$, 很自然地引入范数 (也就是高斯的复数几何解释). 现在我们知道了: 复数域

- 从代数性质来说是代数闭域 (任何多项式有根 — 代数基本定理);
- 从拓扑性质来说是完备域 (任何 Cauchy 序列有极限 — 推论 3.5.6).

复数域似乎是一个完美的终点. 不过历史上人们对数系扩张的追求并非到此结束.

4.6.1 定义. 设 A 是一个环, 而且从实数域 $\mathbb{R}$ 到其中心 $Z(A)$ 有一个嵌入 $\mathbb{R}\to Z(A)$, 那么称 A 是一个 *实代数*. 如果 A 还是除环, 就称 A 为 *实可除代数*.

注意: 为方便可设 $\mathbb{R}\subseteq Z(A)$. 此时 A 也是一个实向量空间, 纯量乘法为:

$$\mathbb{R}\times A\longrightarrow A,\ (r,a)\longmapsto ra\ .$$

所以 $\mathbb{C}$ 是一个 2- 维实可除代数, 即平常所说 "可做加减乘除", 故也称为 *二元数系*. 人们的进一步的追求是: 有没有更多更大的实可除代数, 即 *多元数系*?

人们形式化地构造出了四元数系:

令 $\mathbb{H}$ 是以 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ 为基底的实向量空间

$$\mathbb{H}=\{\ a+b\,\mathbf{i}+d\,\mathbf{j}+d\,\mathbf{k}\mid a,b,c,d\in\mathbb{R}\ \}$$

定义乘法为按下述规则线性扩张：

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \, ;$$

$$\mathbf{i}\,\mathbf{j} = \mathbf{k} \, , \qquad \mathbf{j}\,\mathbf{k} = \mathbf{i} \, , \qquad \mathbf{k}\,\mathbf{i} = \mathbf{j} \, ,$$

$$\mathbf{j}\,\mathbf{i} = -\mathbf{k} \, , \qquad \mathbf{k}\,\mathbf{j} = -\mathbf{i} \, , \qquad \mathbf{i}\,\mathbf{k} = -\mathbf{j} \, ;$$

可直接验证 $\mathbb{H}$ 是一个实代数. 而且, 对 $h = a + b\,\mathbf{i} + d\,\mathbf{j} + d\,\mathbf{k}$, 令 $h^* = a - b\,\mathbf{i} - d\,\mathbf{j} - d\,\mathbf{k}$; 则

$$h\,h^* = h^*\,h = a^2 + b^2 + c^2 + d^2 \, ;$$

换言之对, $Q(h) = a^2 + b^2 + c^2 + d^2, \forall\, h \in \mathbb{H}$, 是实空间 $\mathbb{H}$ 上的正定二次型, $|h| = Q(h)^{1/2}$ 是 h 的范数. $h \neq 0$ 的逆元就是

$$h^{-1} = \frac{h^*}{h\,h^*} \, .$$

所以 $\mathbb{H}$ 是一个实可除代数.

历史上对复数的几何实现消除了人们对复数的疑虑. 对上述形式化地构造的四元数系则可以通过矩阵来实现：

$$\mathcal{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \,\middle|\, \alpha, \beta \in \mathbb{C} \right\}$$

具体对应是：

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \quad \mathbf{i} \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} , \quad \mathbf{j} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} , \quad \mathbf{k} \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

那么

$$h = a + b\,\mathbf{i} + d\,\mathbf{j} + d\,\mathbf{k} \qquad \overset{\text{对应于}}{\longleftrightarrow} \qquad H = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} .$$

而 h^* 对应于 H^* (矩阵 H 的转置共轭).

下述结果真正终止了对数系扩张的追求.

4.6.2 Frobenius 定理. 有限维实可除代数只有 $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$.

证. 设 A 是一个有限维实可除代数, $\mathbb{R} \subseteq Z(A)$. 为方便, 记 $\mathbb{R}^+ = \{\, a \in \mathbb{R} \,|\, a \geq 0 \,\}$, $\mathbb{R}^- = \{\, a \in \mathbb{R} \,|\, a \leq 0 \,\}$. 令

$$I(A) = \{\, u \in A \mid u^2 \in \mathbb{R}^- \,\} \, ;$$

首先证明: $I(A)$ 是 A 的子空间.

对任 $u \in I(A)$ 和 $a \in \mathbb{R}$, 显然 $(au)^2 = a^2 u^2 \in \mathbb{R}^-$.

再设 $u, v \in I(A)$ 线性无关；那么 $u^2 = a \in \mathbb{R}^-$, $v^2 = b \in \mathbb{R}^-$; 而且我们证明 1, u, v 线性无关：若 1, u, v 线性相关，则有 $c, d \in \mathbb{R}$ 使得 $1 = cu + dv$, 于是 $dv = 1 - cu$, 得

$$d^2 b = 1 - 2cu + c^2 a\,, \quad \text{即} \quad 2cu = 1 + c^2 a - d^2 b \in \mathbb{R}\,,$$

但 $u \notin \mathbb{R}$, 所以 $c = 0$, $d^2 b = 1$, 这与 $b \in \mathbb{R}^-$ 相矛盾.

那么 $u + v \notin \mathbb{R}$, $u - v \notin \mathbb{R}$, 它们都是 $\mathbb{R}$ 上的二次代数元；故有 $c, d, e, f \in \mathbb{R}$ 使

$$(u+v)^2 + c(u+v) + d = 0\,, \qquad \text{其中 } c^2 - 4d < 0\,;$$

$$(u-v)^2 + e(u-v) + f = 0\,, \qquad \text{其中 } e^2 - 4f < 0\,;$$

而 $(u \pm v)^2 = u^2 + v^2 \pm (uv + vu) = a + b \pm (uv + vu)$, 得

$$a + b + (uv + vu) + c(u+v) + d = 0\,,$$

$$a + b - (uv + vu) + e(u-v) + f = 0\,;$$

两式相加得

$$(2a + 2b + d + f) + (c+e)u + (c-e)v = 0\,;$$

由于 1, u, v 线性无关，得 $c + e = 0 = c - e$, 故 $c = e = 0$; 所以

$$u + v = -d \in \mathbb{R}^-\,.$$

即 $u + v \in I(A)$. 所以 $I(A)$ 是 A 的子空间.

然后，对 $u, v \in I(A)$, 令 $q(u) = -u^2 \in \mathbb{R}^+$, 令

$$f(u,v) = \frac{1}{2}\Big(q(u+v) - q(u) - q(v)\Big) = -\frac{1}{2}(uv + vu)\,; \tag{I}$$

易验证 $f(u,v)$ 是 $I(A)$ 上的正定对称双线性型 (内积), 而 $q(u)$ 就是相应的二次型.

现在容易完成证明. 如果 $\dim A = 1$, 那么 $A = \mathbb{R}$.

再设 $\dim A > 1$. 对任 $z \in A - \mathbb{R}$, z 是 $\mathbb{R}$ 上的二次元, 即有 $a, b \in \mathbb{R}$ 使得 $z^2 + az + b = 0$ 且 $a^2 - 4b < 0$, 那么

$$(z + a/2)^2 = (a^2 - 4b)/4 < 0$$

所以 $z + a/2 \in I(A)$, 从而 $z \in \mathbb{R} + I(A)$; 后者显然是直和，即

$$A = \mathbb{R} \oplus I(A)\,.$$

还可以把内积 (I) 扩张到 A:

$$f(a+u,\, b+v) = ab - \frac{1}{2}(uv + vu)\,, \qquad \forall\ a+u,\, b+v \in \mathbb{R} \oplus I(A)\,.$$

取 $\mathbf{i} \in I(A)$ 为单位向量： $f(\mathbf{i},\, \mathbf{i}) = 1$, 即 $\mathbf{i}^2 = -1$.

如果 $\dim I(A)=1$, 那么 $A=\mathbb{R}\oplus\mathbb{R}\,\mathbf{i}=\mathbb{C}$.

否则还有单位向量 $\mathbf{j}$ 正交于 $\mathbf{i}$: $f(\mathbf{j},\mathbf{j})=1$, $f(\mathbf{i},\mathbf{j})=0$; 即

$$\mathbf{j}^2=-1\,,\qquad \mathbf{i}\,\mathbf{j}+\mathbf{j}\,\mathbf{i}=0\,;$$

特别有: $\mathbf{i}\,\mathbf{j}=-\mathbf{i}\mathbf{j}$. 令

$$\mathbf{k}=\mathbf{i}\,\mathbf{j}\,,\quad \text{从而}\quad \mathbf{j}\,\mathbf{i}=-\mathbf{i}\,\mathbf{j}=-\mathbf{k}\,;$$

还易计算:

$$\mathbf{k}^2=\mathbf{i}\,\mathbf{j}\,\mathbf{i}\,\mathbf{j}=-\mathbf{i}\,\mathbf{i}\,\mathbf{j}\,\mathbf{j}=-(-1)(-1)=-1\,;$$

$$\mathbf{j}\,\mathbf{k}=\mathbf{j}\,\mathbf{i}\,\mathbf{j}=-\mathbf{j}\,\mathbf{j}\,\mathbf{i}=\mathbf{i}\,,\qquad \mathbf{k}\,\mathbf{j}=\mathbf{i}\,\mathbf{j}\,\mathbf{i}=-\mathbf{i}\,;$$

$$\mathbf{k}\,\mathbf{i}=\mathbf{i}\,\mathbf{j}\,\mathbf{i}=-\mathbf{i}\,\mathbf{i}\,\mathbf{j}=\mathbf{j}\,,\qquad \mathbf{i}\,\mathbf{k}=\mathbf{i}\,\mathbf{i}\,\mathbf{j}=-\mathbf{j}\,;$$

特别有

$$f(\mathbf{k},\mathbf{i})=-\frac{1}{2}(\mathbf{k}\,\mathbf{i}+\mathbf{i}\,\mathbf{k})=0\,,$$

$$f(\mathbf{k},\mathbf{j})=-\frac{1}{2}(\mathbf{k}\,\mathbf{j}+\mathbf{j}\,\mathbf{k})=0\,;$$

所以 $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ 构成 $I(A)$ 的正交向量组; 以下证明它们构成 $I(A)$ 的标准正交基就可完成全部证明, 因为那样就有

$$A=\mathbb{R}\oplus\mathbb{R}\,\mathbf{i}\oplus\mathbb{R}\,\mathbf{j}\oplus\mathbb{R}\,\mathbf{k}$$

而且 $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ 正好满足四元数的运算规则; 即 $A=\mathbb{H}$.

反证法. 若 $\dim I(A)>3$, 就有单位向量 $\mathbf{m}\in I(A)$ 与 $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ 都正交:

$$f(\mathbf{m},\mathbf{i})=-\frac{1}{2}(\mathbf{m}\,\mathbf{i}+\mathbf{i}\,\mathbf{m})=0\,,$$

$$f(\mathbf{m},\mathbf{j})=-\frac{1}{2}(\mathbf{m}\,\mathbf{j}+\mathbf{j}\,\mathbf{m})=0\,,$$

$$f(\mathbf{m},\mathbf{k})=-\frac{1}{2}(\mathbf{m}\,\mathbf{k}+\mathbf{k}\,\mathbf{m})=0\,;$$

但由前两条 (它们是 $\mathbf{m}\,\mathbf{i}=-\mathbf{i}\,\mathbf{m}$ 和 $\mathbf{m}\,\mathbf{j}=-\mathbf{j}\,\mathbf{m}$) 可推出

$$\mathbf{m}\,\mathbf{k}=\mathbf{m}\,\mathbf{i}\,\mathbf{j}=-\mathbf{i}\,\mathbf{m}\,\mathbf{j}=\mathbf{i}\,\mathbf{j}\,\mathbf{m}=\mathbf{k}\,\mathbf{m}\,;$$

代入第三条得 $\mathbf{m}\,\mathbf{k}=0$; 这与 $\mathbf{m}$ 与 $\mathbf{k}$ 都非零相矛盾. □