分裂域与正规扩张

定义 1 (分裂域)**.** 设域扩张 K/F，$f(x)\in F[x]$ 且 $\deg f(x)=n$，若

1. $f(x)$ 在 $K[x]$ 内可分解为一次因式乘积，即

$$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

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

则称 K 是 $f(x)\in F[x]$ 的**分裂域**.

注. *1. 满足条件 1 的域 K 称为根域，则 $f(x)\in F[x]$ 的分裂域为最小的根域. 这个分解隐含了 n 次多项式有 n 个根.*

2. 分裂域与基域 F 有关，例如 $f(x)=x^2-2\in\mathbb{Q}[x]$ 的分裂域为 $\mathbb{Q}(\sqrt{2})$，而 $g(x)=x^2-2\in\mathbb{R}[x]$ 的分裂域为 $\mathbb{R}$.

3. 分裂域 $K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$ 是 F 的有限扩张.

证明分裂域的存在性之前，先证明一个引理.

引理 1. 不可约多项式 $p(x)\in F[x]$ 都在 F 的某一扩域上有根.

证明. 设 $p(x)=\sum_{k=0}^{n}a_kx^k$，作自然同态

$$\begin{aligned}\pi: F[x]&\to F[x]\Big/\langle p(x)\rangle\\ f(x)&\mapsto f(x)+\langle p(x)\rangle\end{aligned}$$

由于 $\langle p(x)\rangle$ 是 $F[x]$ 的极大理想，于是 $F[x]\Big/\langle p(x)\rangle$ 是域. 作限制映射

$$\pi\big|_F: a\mapsto a+\langle p(x)\rangle,\ a\in F,$$

可以证明 $\pi\big|_F$ 是单同态，又因为 $\pi\big|_F$ 是满同态，则 $F\cong\pi(F)\subset F[x]\Big/\langle p(x)\rangle$.

记 $\alpha=x+\langle p(x)\rangle\in F[x]\big/\langle p(x)\rangle$，则

$$p(\alpha)=\sum_{k=0}^{n}a_k\alpha^k=\sum_{k=0}^{n}a_kx^k+\langle p(x)\rangle=\overline{0}\in F[x]\Big/\langle p(x)\rangle.$$

故 $\alpha=x+\langle p(x)\rangle$ 是 $p(x)\in F[x]$ 在扩域 $F[x]\Big/\langle p(x)\rangle$ 中的根. □

定理 1. 设 $f(x)\in F[x]$ 且 $\deg f(x)=n>0$，则 $f(x)\in F[x]$ 的分裂域一定存在且 $f(x)$ 在分裂域下有 n 个根.

证明. 对 n 作数学归纳法. 当 $n=1$ 时，设 $f(x)=ax+b\ (a\neq 0)$，则 $-\dfrac{b}{a}\in F$ 是 $f(x)$ 的根. 于是 $f(x)$ 在 F 的扩域 $K=F(-\dfrac{b}{a})=F$ 中有且仅有一个根.

下设 $n-1$ 时结论成立，去证 n 时结论仍成立. 由引理1，可设 α_1 是 $f(x)\in F[x]$ 在某扩域中的根，记 $F_1=F(\alpha_1)$，于是

$$f(x)=(x-\alpha)f_1(x)\in F_1[x],\quad \deg f_1(x)=n-1.$$

据归纳假设，$f_1(x)\in F_1[x]$ 在 K 中有 $n-1$ 个根 $\alpha_2,\alpha_3,\cdots,\alpha_n$ 且有分裂域

$$K=F_1(\alpha_2,\alpha_3,\cdots,\alpha_n).$$

则

$$f_1(x)=c(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)\in K[x],\quad c\in F.$$

又 $\alpha_1\in F\subset K$，于是

$$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\in K[x].$$

故 $K=F_1(\alpha_2,\alpha_3,\cdots,\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 $f(x)\in F[x]$ 的分裂域，且 $f(x)\in K[x]$ 有 n 个根. □

推论 1. 设 K 是 $f(x)\in F[x]$ 的分裂域且 $\deg f(x)=n$，则 $[K:F]\leqslant n!$.

证明. 由

$$[K:F]=[F(\alpha_1,\alpha_2,\cdots,\alpha_n):F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})]\cdots[F(\alpha_1,\alpha_2):F(\alpha_1)][F(\alpha_1):F],$$

其中 $[F(\alpha_1):F]\leqslant n$，因为 α 是 $f(x)$ 的根. 同理有 $[F(\alpha_1,\alpha_2):F(\alpha_1)]\leqslant n-1$，以此类推即可. □

推论 2. 设 K 是 $f(x)\in F[x]$ 的分裂域，且有域扩张 $K/E/F$，则 K 也是 $f(x)\in E[x]$ 的分裂域.

证明. 设 $\deg f(x)=n$，$f(x)$ 的 n 个根为 $\alpha_1,\alpha_2,\cdots,\alpha_n$，则

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

而 $f(x)\in E[x]$ 的分裂域为 $E(\alpha_1,\alpha_2,\cdots,\alpha_n)$，又因为 $F\subset E$，于是

$$K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)\subset E(\alpha_1,\alpha_2,\cdots,\alpha_n)\subset K,$$

故 $E(\alpha_1,\alpha_2,\cdots,\alpha_n)=K$. □

定义 2 (同构开拓). 设 σ 是环 R_1 到 R_2 的同构映射，K_1 是 R_1 的扩张，K_2 是 R_2 的扩张，若存在 η 是 K_1 到 K_2 的同构映射且 $\eta\big|_{R_1}=\sigma$，则称 η 是 σ 的**同构开拓**.

注. 设 K_1 与 K_2 是 F-等价扩张，则有同构映射 $\eta:K_1\to K_2$，满足 $\eta\big|_F=\mathrm{id}_F$，于是 η 是 id_F 的同构开拓.

下面不加证明地给出有关分裂域唯一性的两个定理.

定理 2. 设 σ 是 F 到 $\overline{F}$ 上的域同构，则

1. σ 可开拓为 $F[x]$ 到 $\overline{F}[x]$ 上的同构映射，仍记为 σ，$p(x)\in F[x]$ 不可约当且仅当 $\sigma p(x)\in\overline{F}[x]$ 不可约.
2. 设 $K,\overline{K}$ 分别为 $F,\overline{F}$ 的扩域且 $p(x)\in F[x]$ 不可约，又设 $\alpha\in K$，$\overline{\alpha}\in\overline{K}$ 分别为 $p(x)$ 和 $\sigma p(x)$ 的根，则 σ 可唯一开拓为 $F(\alpha)$ 到 $\overline{F}(\overline{\alpha})$ 的同构映射 $\overline{\sigma}$ 使得 $\sigma(\alpha)=\overline{\alpha}$.

定理 3. 设 σ 是 F 到 $\overline{F}$ 上的域同构，开拓为 $F[x]$ 到 $\overline{F}[x]$ 上的同构映射仍记为 σ. 设 $E,\overline{E}$ 分别为 $f(x)\in F[x]$ 和 $\sigma f(x)\in\overline{F}[x]$ 的分裂域，则 σ 可开拓为 E 到 $\overline{E}$ 的同构映射. 而且不同开拓的个数不超过 $\left[\overline{E}:\overline{F}\right]$，当且仅当 $\sigma f(x)$ 的所有不可约因子在 $\overline{E}$ 中都无重根时等号成立.

推论 3 (分裂域的唯一性). 设 F 是域，$f(x)\in F[x]$ 且 $\deg f(x)=n>0$. 则 $f(x)$ 的任何两个分裂域 E 和 $\overline{E}$ 是 F-等价扩张. 特别地，当 E 与 $\overline{E}$ 是 F 的同一扩域 K 的子域时，$E=\overline{E}$.

证明. 取 $\overline{F}=F$，$\sigma=\mathrm{id}_F$，由定理3，σ 可开拓为 $f(x)\in F[x]$ 的两个分裂域 E 和 $\overline{E}$ 的同构映射且满足 $\sigma\big|_F=\mathrm{id}_F$，故 E 和 $\overline{E}$ 是 F-等价扩张.

设域扩张 K/F 满足 $E\subset K$ 且 $\overline{E}\subset K$，因为 $f(x)\in F[x]=\overline{F}[x]$，可设 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，$\overline{E}=\overline{F}(\overline{\alpha_1},\overline{\alpha_2},\cdots,\overline{\alpha_n})$，于是

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\in E[x]\subset K[x],$$

$$f(x)=(x-\overline{\alpha_1})(x-\overline{\alpha_2})\cdots(x-\overline{\alpha_n})\in\overline{E}[x]\subset K[x],$$

其中 $x-\alpha_i$ 与 $x-\overline{\alpha_i}$ 都是不可约多项式. 由于域上多项式环是 Euclid 环，进而是唯一析因环，于是在相伴与不计次序下 $f(x)$ 在 $K[x]$ 中分解唯一，故存在 $\pi\in S_n$ 使得 $\alpha_i=\overline{\alpha_{\pi(i)}}$，故 $E=\overline{E}$. □

注. $f(x)\in F[x]$ 的分裂域的形式可以不同，但它们之间都是 F-等价扩张，在这个意义下分裂域是唯一的. 例如 $x^2-2\in\mathbb{Q}[x]$ 的分裂域可以是 $\mathbb{Q}\left[\sqrt{2}\right]$，也可以是 $\mathbb{Q}[x]\Big/\langle x^2-2\rangle$.

注. $f(x)\in F[x]$ 在不同分裂域中根的表现形式也可以不同，但实质 (即在同构意义下) 是一样的. 如是否有重根、根的重数、根与根之间的运算以及根的极小多项式等.

注. 当 K 与 $\overline{K}$ 同含于 K 时，$E=\overline{E}$，此时两组根的形式也相同，只有次序的差别.

命题 1. 设 $f(x)\in F[x]$ 的分裂域为 E，σ 是 E 的 F-自同构，则 σ 把 $f(x)$ 的根仍映为 $f(x)$ 的根.

注. 这里的 σ 不一定是恒等映射. 而且在 σ 下 α_i 并不一定能够映射到 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的任意一个，因为 $f(x)$ 未必是不可约多项式，当分解为不可约多项式时，只有每个不可约多项式的根之间可以互相映射.

推论 4. 设 $f(x)\in F[x]$ 的分裂域为 E，则 E 的不同 F-自同构的个数不超过 $[E:F]$ 且等号成立当且仅当 $f(x)$ 的不可约因子都无重根.

证明. 这是定理3的直接推论. □

推论 5. 设域扩张 K/F，E 是 $f(x)\in F[x]$ 的分裂域且 $E\subset K$，则对 K 的任一 F-自同构 σ，都有 $\sigma E=E$.

证明. 将 x 在 $K[x]$ 上的开拓仍记为 σ，$f(x)$ 在 $K[x]$ 中有分解

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\quad a_i\in E\subset K.$$

于是由 $f(x)\in F[x]$，$\sigma\big|_F=\mathrm{id}_F$ 有

$$f(x)=\sigma f(x)=(x-\sigma(\alpha_1))(x-\sigma(\alpha_2))\cdots(x-\sigma(\alpha_n)),$$

因而存在 $\pi\in S_n$ 使得 $\sigma(\alpha_i)=\alpha_{\pi(i)}$，故

$$\sigma E=\sigma(F(\alpha_1,\alpha_2,\cdots,\alpha_n))=F(\alpha_{\pi(1)},\alpha_{\pi(2)},\cdots,\alpha_{\pi(n)})=E.$$

□

例 1. 求 $x^2+ax+b\in F[x]$ 的分裂域 E 及 $[E:F]$.

解. 若 $x^2+ax+b\in F[x]$ 可约，则有

$$x^2+ax+b=(x-c_1)(x-c_2),\quad c_1,c_2\in F,$$

则分裂域 $E=F(c_1,c_2)=F$，$[E:F]=1$.

若 $x^2+ax+b\in F[x]$ 不可约，则由引理1，x^2+ax+b 在扩域 $F[x]\Big/\langle x^2+ax+b\rangle$ 上有根，记为 $\alpha_1=x+\langle x^2+ax+b\rangle$，则在 $F(\alpha_1)$ 中，有分解

$$x^2+ax+b=(x-\alpha_1)(x-\alpha_2),\quad \alpha_2\in F(\alpha_1),$$

于是分裂域 $E=F(\alpha_1,\alpha_2)=F(\alpha_1)$. 而 x^2+ax+b 是 α_1 在 F 上的极小多项式，故 $[E:F]=[F(\alpha_1):F]=\deg(\alpha_1,F)=2$.

例 2. 求 $f_1(x)f_2(x) \in F[x]$ 的分裂域 E 及 $[E:F]$.

解. 思路：不妨设 $f_1(x), f_2(x)$ 在 $F[x]$ 上不可约，看 $f_1(x)$ 在 $F[x]\Big/\langle f_1(x)\rangle$ 上能否彻底分解，若不能，则把 $F[x]\Big/\langle f_1(x)\rangle$ 中的根除掉，再对剩下的多项式讨论. 以此类推，得到 $f_1(x) \in F[x]$ 的分裂域 K_1.

再看 $f_2(x) \in F[x]$ 在 K_1 上能否彻底分解，与上面类似地，得到 $f_1(x)f_2(x) \in F[x]$ 的分裂域.

例 3 (分圆域)**.** 设 p 是素数. 求 $x^p-1 \in \mathbb{Q}[x]$ 的分裂域 E 及 $[E:\mathbb{Q}]$.

解. $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+x+1)$，由 Eisenstein 判别法可知 $x^{p-1}+x^{p-2}+\cdots+x+1$ 在 $\mathbb{Q}$ 上不可约. 记 ε 是 $x^{p-1}+x^{p-2}+\cdots+x+1$ 的一个根，可以证明 $\varepsilon^0=1, \varepsilon^1, \cdots, \varepsilon^{p-1}$ 是 x^p-1 的 p 个不同的根，于是 $E=\mathbb{Q}(\varepsilon^0, \varepsilon^1, \cdots, \varepsilon^{p-1})=\mathbb{Q}(\varepsilon)$，$[E:\mathbb{Q}]=[\mathbb{Q}(\varepsilon):\mathbb{Q}]=p-1$.

注. 称 ε 是 p 次**本原单位根**. 由于 x^p-1 的不可约因子无重根，于是 E 的不同 $\mathbb{Q}$-自同构的个数就是扩张次数 $p-1$.

例 4. 设 p 是素数. 求 $x^p-2 \in \mathbb{Q}[x]$ 的分裂域 E 及 $[E:F]$.

解.

$$E=\mathbb{Q}(\sqrt[p]{2}\varepsilon^0, \sqrt[p]{2}\varepsilon^1, \cdots, \sqrt[p]{2}\varepsilon^{p-1})=\mathbb{Q}(\sqrt[p]{2}, \varepsilon)$$
$$[E:\mathbb{Q}]=\left[\mathbb{Q}(\sqrt[p]{2}, \varepsilon):\mathbb{Q}(\sqrt[p]{2})\right]\left[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}\right]=(p-1)p.$$

定义 3 (正规扩张)**.** 设域扩张 K/F 是代数扩张，对任意不可约多项式 $p(x) \in F[x]$，若 $p(x)$ 在 K 中有一个根能推出 K 中含有 $p(x)$ 所有的根，则称 K 为 F 的**正规扩张**.

定理 4. 设域扩张 E/F 是有限扩张，则 E/F 是正规扩张当且仅当 E 是 $F[x]$ 中一个多项式的分裂域.

证明. **必要性：**设 $[E:F]=r$，取 E 作为域 F 上 r 维线性空间的一组基 $\alpha_1, \alpha_2, \cdots, \alpha_r$，则 $E=F(\alpha_1, \alpha_2, \cdots, \alpha_r)$. 令

$$f(x)=\mathrm{Irr}(\alpha_1, F)\mathrm{Irr}(\alpha_2, F)\cdots\mathrm{Irr}(\alpha_r, F) \in F[x],$$

设它的分裂域为 $F(\beta_1, \beta_2, \cdot, \beta_s)$，其中 $s>r$，则 $\{\alpha_1, \alpha_2, \cdots, \alpha_r\} \subset \{\beta_1, \beta_2, \cdot, \beta_s\}$. 对任意 $\mathrm{Irr}(\alpha_i, F)$，$\alpha_i \in E$，而 E/F 是正规扩张，则 $\mathrm{Irr}(\alpha_i, F)$ 的所有根都在 E 中，故 $\beta_1, \beta_2, \cdot, \beta_s \in E$，有

$$E=F(\alpha_1, \alpha_2, \cdots, \alpha_r) \subset F(\beta_1, \beta_2, \cdot, \beta_s) \subset E,$$

故 $E=F(\beta_1, \beta_2, \cdot, \beta_s)$ 为 $f(x) \in F[x]$ 的分裂域.

充分性：设 E 是 $f(x) \in F[x]$ 的分裂域，对任意不可约多项式 $p(x) \in F[x]$，$p(x)$ 的一个根 $\alpha \in E$. 记 β 是 $p(x)$ 的任一根，下证 $\beta \in E$.

取 K 是 $p(x) \in E[x]$ 的分裂域，则 K 也是 $g(x)=p(x)f(x) \in F[x]$ 的分裂域. 据定理3，id_F 可开拓为 $g(x) \in F[x]$ 的分裂域 K 的 F-自同构 σ，且适当调换顺序有 $\sigma(\alpha)=\beta$. □