抽象代数-域论-part 整理

回忆

- 【定理】k是域，$p(x)$是$k[x]$中不可约多项式，考虑$k[x]/(p(x))$. $\deg p(x)=n\geq 1$.
  - $k[x]/(p(x))$是域（k是域，所以$k[x]$是ED，PID，所以$(p(x))$是极大理想，所以$k[x]/(p(x))$是域）
  - $i:k\to k[x]/(p(x))$，$a\mapsto \overline{a}$是单同态，因为如果$\overline{a}=\overline{b}$，则必然有$p(x)$整除$a-b$，这只有$a-b=0$时才对.

    （正因如此，$k[x]/(p(x))$中的$\overline{a}$可以看成k嵌入，记号：不再记为$\overline{a}$而是等同地记为a）

    （通过$k\cong \mathrm{Im}i$可以将k看成$k[x]/(p(x))$的子域）
  - 【记号】$\alpha:=\overline{x}\in K$. 则这个新的数$\alpha$满足：
    - $p(\alpha)=0$
    - $K=k[x]/(p(x))$可以看成是k上n维线性空间，其一组$k-$基为$(1,\overline{x},\cdots,\overline{x}^{n-1})$，或者$(1,\alpha,\cdots,\alpha^{n-1})$.
  - $\forall f(x)\in k[x]$：

    ①$f(\alpha)=0\Leftrightarrow \overline{f(x)}=\overline{0}\Leftrightarrow f(x)\in(p(x))\Leftrightarrow p(x)\mid f(x)$.

    ②$f(\alpha)\neq 0$时，必有$p(x)\nmid f(x)$，因为$p(x)$不可约，所以$\gcd(p(x),f(x))=1$，所以根据Bezout 等式，存在$g(x),h(x)\in k[x]$，使得$f(x)g(x)+p(x)h(x)=1$，这样的$g(\alpha)$就是$f(\alpha)$在K中的逆元.

【remark】这个技术是域扩张的基本想法.

域扩张

1. 域扩张

- 【素域】
  - 【定义】域F的特征指的是域F作为环的特征，记为$\mathrm{char}F$.
  - 【命题】整区的特征只能是0或者p（p为素数），特别地，域的特征只能是0或者p.

    【证明】设R是整区，关键是考虑环的“最小子环”，即$S=\langle 1_R\rangle$，若$\mathrm{char}R=0$，则$S\cong\mathbb{Z}$，若$\mathrm{char}R=n$，则$S\cong\mathbb{Z}/n\mathbb{Z}$. 因为$R$是整区，所以其子环都是整区，所以$S$是整区. 而$\mathbb{Z}/n\mathbb{Z}$是整区当且仅当$n$是素数，于是整区的特征只能是0或$p$（$p$为素数）.□
  - 【命题】F是域，如果：
    - $\mathrm{char}F=0$，则它必有同构于$\mathbb{Z}$的子环，更准确地说，这个子环是以下同态的像：

      $$\varphi:\mathbb{Z}\to F,\quad n\mapsto n1_F$$

      因为$\mathrm{char}F=0$，所以$\ker\varphi=0$，于是$\mathrm{Im}\varphi$同构于$\mathbb{Z}$. 因为$\varphi:\mathbb{Z}\to F$是单同态，F是域，由分式域的泛性质，存在唯一的ψ是单同态：$\mathbb{Q}\to F$，使得$\varphi=\psi\circ i$，其中i是$\mathbb{Z}\to\mathbb{Q}$的嵌入同态.

      而且，ψ由这个公式给出：

      $$\psi(\frac{m}{n})=\psi(m\cdot n^{-1})=\varphi(m)(\varphi(n))^{-1}=1_Fm(1_Fn)^{-1}.$$

      因为ψ是单同态，所以$\mathrm{Im}\psi$和$\mathbb{Q}$同构. 所以结论是：

      若$\mathrm{char}F=0$，则F同构于$\mathbb{Q}$的最小子域

      （对最小性的说明：因为如果E是F的子域，那么1_F一定在E里，所以1_Fm和$(1_Fn)^{-1}$也必然在E里，从而整个$\mathrm{Im}\psi$都在E里）
    - $\mathrm{char}F=p$，仍然考虑上面题目的同态φ：

$$\varphi:\mathbb{Z}\to F,\quad n\mapsto n1_F$$

因为$\mathrm{char}F=p$，所以$\ker\varphi=(p)=p\mathbb{Z}$，于是$\mathrm{Im}\varphi$同构于$\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$（同态基本定理），所以$\mathrm{Im}\varphi$是$F$的同构于$\mathbb{F}_p$的子域.

（最小性：和上面相同）

【remark】由上可见有限域的特征必然不为0（否则包含同构于$\mathbb{Q}$的子域），但反之，特征是p的域未必是有限域，例如$\mathbb{F}_p(x)$，其特征是p，而$1,x,\cdots,x^n,\cdots\in\mathbb{F}_p(x)$.

- 【域扩张】
  - 域扩张的想法：这是因为所有的域同态都是单同态，所以如果研究域同态，则一个域总是可以通过这个同态看成另一个域的子域. 所以，可以说域之间的关系只有域扩张.

    设E，F是域，$\varphi:E\to F$是域同态，考虑$\ker\varphi$，注意域是除环，只有平凡理想，所以$\ker\varphi$是零理想，或者是整个E. 但是，如果$\ker\varphi$是整个E，那么$\varphi(1)=0$，在域中$1\neq 0$，所以这与φ是域同态矛盾.

    综上所述，$\ker\varphi=0$，所以这是单同态. 由于$\mathrm{Im}\varphi\cong E$，于是可以通过$\varphi$将$E$看成$F$的子域.
  - 域扩张的记号：$F\subseteq E$或者E/F.
- 【一些重要的中间域的构造】E/F是域扩张，S是E的子集，$\alpha,\beta\in E$
  - $F[\alpha]=\{f(\alpha):f(x)\in F[x]\}$，这是$E$的含有$F$和$\alpha$的最小子环.
  - $F(\alpha)=\mathrm{Frac}(F[\alpha])=\{\frac{f(\alpha)}{g(\alpha)}:f,g\in F,g(\alpha)\neq 0_E\}$，这是$E$的含有$F$和$\alpha$的最小子域.
  - $F[\alpha,\beta]$：含有F和α,β的最小子环.
  - $F(\alpha,\beta)$：含有F和α,β的最小子域.
  - $F[S]$：含有F和S的最小子环
    $F[S]=\{f(\alpha_1,\cdots,\alpha_n):\alpha_i\in S,f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n],n\geq 0\}$.
  - $F(S)$：含有F和S的最小子域.
  - 【单扩张】：若存在$\alpha\in E$，使得$E=F(\alpha)$，则称E/F是单扩张.

    例如$\mathbb{C}=R[i]=R(i)$，$\mathbb{Q}(i)=\mathbb{Q}[i]$，$F(x)$等.
  - **重要命题**：如果S,T都是E的子域，则$F(S\cup T)=F(S)(T)=F(T)(S)$.（想一想最小性刻画即可，这个命题用的很多，这表明先后将S和T加入，或是直接加入是一样的）

    推论：$F(\alpha)(\beta)=F(\beta)(\alpha)=F(\alpha,\beta)$.

2. 单扩张的结构

- 【代数元、超越元】E/F是域扩张，$\alpha\in E$，如果存在$f(x)\in F[x]$使得$f(\alpha)=0_E$，则称α在F上代数，否则称α在F上超越.
- 【最小多项式】设E/F是域扩张，$\alpha\in E$，若α在E上代数，则$\exists!\,p(x)\in F[x]$是首一不可约多项式，使得：
  - $p(\alpha)=0$
  - $\forall f(x)\in F[x]$适合$f(\alpha)=0$，则$p(x)\mid f(x)$.

此时称$p(x)$是F的极小多项式.

【命题】若$p(x)\in F[x]$适合$p(\alpha)=0$，且p首一不可约，则$p(x)$就是α在F上的极小多项式.（设$q(x)$是极小多项式，则有$q(x)\mid p(x)$，由$p(x)$不可约知$p(x)\sim q(x)$，再根据它们都首一知$p(x)=q(x)$）

下面讨论单扩张的结构，顺便说明极小多项式概念的引入.

- 【单扩张的结构】

设E/F是域扩张，$\alpha\in E$，考虑其子扩张$F(\alpha)/F$，则

- 若α在F上代数，则$F(\alpha)=F[\alpha]\cong F[x]/(p(x))$.
- 若α在F上超越，则$F(\alpha)\cong F(x)$，$F[\alpha]\cong F[x]$.

【证明】考虑赋值同态：

$$\varphi : F[x] \to E, \quad f(x) \mapsto f(\alpha)$$

则$\mathrm{Im}\varphi = F[\alpha]$.

下面考虑$\ker\varphi$，分两种情况：

①如果α在F上代数，则存在$f(x) \in F[x]$使得$f(\alpha) = 0_E$，所以$\ker\varphi \neq 0$. 因为$F[x]$是ED，PID，所以$\ker\varphi = (\widetilde{p}(x))$，其中$\widetilde{p}(x) \in F[x] - F^\times - 0$（因为理想非零且是真理想），所以$\deg\widetilde{p}(x) \geq 1$，设其首项系数为$c \in F^\times$，则$\widetilde{p}(x) = cp(x)$，其中$p(x)$是首一多项式而且$\ker\varphi = (p(x))$（因为相伴的元素生成的主理想一样）.

下面验证$p(x)$就是α在F上的极小多项式. 首先：

$$f(\alpha) = 0 \Leftrightarrow f(x) \in \ker\varphi \Leftrightarrow f(x) \in (p(x)) \Leftrightarrow p(x) \mid f(x)$$

其次，$\mathrm{Im}\varphi = F[\alpha]$是$E$的子环，而整区的子环还是整区，所以$F[\alpha]$是整区. 根据同态基本定理：

$$F[x]/(p(x)) \cong F[\alpha].$$

因为左边是整区，根据整区的商环刻画可知$(p(x))$是素理想，在整区中主理想是素理想当且仅当$p(x)$是素元或者0，所以$p(x)$是素元，所以$p(x)$是不可约元. 因为$F[x]$是PID，所以$F[x]/(p(x))$是域，所以$F[\alpha]$是域，于是和它的分式域相同即$F[\alpha] = F(\alpha)$.

②如果α在F上超越，则$\ker\varphi = 0$，所以$F[x] \cong F[\alpha]$，两边同时取分式域，$F(x) \cong F(\alpha)$.

- 【例】
  - $\sqrt[n]{2}$在$\mathbb{Q}$上的极小多项式为$x^n - 2$.（用$\mathbb{Z}$的Eisenstein判别法，$2 \nmid 1$，$2 \mid 0$，$2 \mid -2$，而$4 \nmid -2$，所以$x^n - 2$在$\mathbb{Q}$上不可约）
  - p是素数，$\zeta = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$.

    则$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$. 我们要证明$p(x) = x^{p-1} + \cdots + x + 1$在$\mathbb{Q}$上不可约，注意$p(x+1) = \sum_{i=0}^{p-1} x^i(\sum_{j=i}^{p-1} C_j^i) = \sum_{i=0}^{p-1} C_p^{i+1}x^i$. $p \nmid C_p^p$，$p \mid C_p^{i+1}$，$p^2 \nmid C_p^1$.

    所以$p(x)$是ζ在$\mathbb{Q}$上的极小多项式.
  - E/F是域扩张，$\alpha \in E$，如果α本身就落在F中即$\alpha \in F$，则α必在F上代数，且其极小多项式为$x - \alpha$.
- 【命题】$E/K/F$是域扩张，$\alpha \in E$，且α在F上代数，则α必在K上代数，而且极小多项式有整除关系：

$$\min(\alpha, K) \mid \min(\alpha, F) \quad \text{在}K[x]\text{中}$$

例如，$\mathbb{C}/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$，$\sqrt{2}$在$\mathbb{Q}$上代数给出$\sqrt{2}$在$\mathbb{Q}(\sqrt{2})$上代数，且极小多项式有整除关系$x - \sqrt{2} \mid x^2 - 2$.

【remark】这表明在小的域上代数给出在大的域上代数.

3. 代数扩张、超越扩张、有限扩张

- 【代数扩张】E/F是域扩张，如果E中所有元素都在F上代数，则称E/F是代数扩张，否则称为超越扩张.
- 一些问题：
  - 代数元生成的单扩张是不是代数扩张？一般地，代数元集生成的扩张是不是代数扩张？
  - α，β在F上都代数，那么$\alpha \pm \beta$，$\alpha\beta$，$\alpha/\beta(\beta \neq 0)$是不是也在$F$上代数？
  - 代数扩张有没有传递性？也就是E/K和K/F都是代数扩张，能不能说明E/F也是代数扩张？

以上问题的答案都是【是】，为了说明这个问题，我们需要如下的观点：

- 【扩张次数】E/F是域扩张，则E关于自身的加法以及与它的子域F的乘法是一个$F-$线性空间，其维数$\dim_F E$称为E/F的扩张次数，记为$[E:F]$.

  若$[E:F] < \infty$，则称E/F是有限扩张，否则称为无限扩张.
- 【命题】$F(\alpha)/F$是单扩张.
  - 若α是代数元，则$F(\alpha)/F$是有限扩张，且$[F(\alpha):F] = \deg\min(\alpha, F) = n$，$F(\alpha)$作为$F-$线性空间的一组$F-$基为$1, \alpha, \cdots, \alpha^{n-1}$.

【证明】只需要证明最后一句话，一旦最后一句话成立，前面两句话根据定义自然成立.

这是因为，根据单扩张结构，$F(\alpha)\cong F[x]/p(x)$，而后者可以写成$1,\overline{x},\cdots,\overline{x}^n$的线性组合. 另一方面，该向量组必然线性无关，否则存在$f(x)\in F[x]$，$\deg f(x)\leq n-1$，$f(\alpha)=0$，这与$\deg\min(\alpha,F)=n$矛盾！$\square$

- 若α是超越元，则$F(\alpha)/F$必是无限扩张. 这是因为$F(\alpha)$有一个同构于$F[x]$的子环，即$F(\alpha)$作为$F-$线性空间有一个同构于$F[x]$的线性子空间，而$F[x]$作为$F-$线性空间是无限维的，所以$F(\alpha)$作为$F-$线性空间也是无限维的.$\square$
- 以上结果说明，$[F(\alpha):F]$有限$\Leftrightarrow\alpha$在F上代数，此时$[F(\alpha):F]=\deg\min(\alpha,F)$.

- 【命题】（扩张次数的传递性）设$E/K/F$是域扩张，$\{a_i\}_{i\in I}$是E的一组$K-$基，$\{b_j\}_{j\in J}$是K的一组$F-$基函，则$\{a_ib_j\}_{i\in I,j\in J}$是$E$的一组$F-$基. 因此：

$$|I\times J|=|I||J|\Rightarrow[E:F]=[E:K][K:F]$$

【推论】有限扩张具有传递性. 即如果$E/K/F$是域扩张，E/K和K/F都是有限扩张，那么E/F也是有限扩张.

【证明】用定义，先把E看成$K-$线性空间，将E中的向量展开，然后再把K看成$F-$线性空间，再展开，这就证明$\{a_ib_j\}_{i\in I,j\in J}$生成$E$. 再利用$\{a_i\}$ $K-$线性无关和$\{b_j\}$ $F-$线性无关可以证明$\{a_ib_j\}$ $F-$线性无关.

- 【例】有限域的元素个数一定为p^n.

【证明】回忆，有限域的特征必然为p（否则其素域为$\mathbb{Q}$，这与有限矛盾）. 设域F为特征是p的有限域，考虑其素域$\mathbb{F}_p$，因为$|F|<\infty$，所以F作为线性空间的维数一定也是有限的，即$[F:\mathbb{F}_p]<\infty$，记$[F:\mathbb{F}_p]=n$，则F同构于$\mathbb{F}_p$上n维列向量空间$\mathbb{F}_p^n$. 因为$\#\mathbb{F}_p=p$，所以$|F|=|\mathbb{F}_p^n|=p^n$. $\square$

- 【命题】（**有限扩张等价于有限生成代数扩张**）即以下等价：
  - $[E:F]<\infty$；
  - E/F是代数扩张，而且存在$\alpha_1,\cdots,\alpha_k\in E$，使得$E=F(\alpha_1,\cdots,\alpha_k)$.

特别地，**有限扩张必然是代数扩张**. 因此若α在F上代数，则$F(\alpha)/F$是代数扩张，这回答了上面的问题1，而且说的更多.

【证明】$(1)\Rightarrow(2)$：设$[E:F]<\infty$，先说明E/F是**代数扩张**. 假设$[E:F]=n$，则$\forall\alpha\in E$，$\underbrace{1,\alpha,\cdots,\alpha^n}_{n+1}$必然$F-$线性相关，即存在$c_0,\cdots,c_{n-1}\in F$，使得$c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}=0$，即存在$f(x)\in F[x]$使得$f(\alpha)=0$，所以$\alpha$在$F$上代数.

再说明后面一半. 分情况讨论. 如果$F=E$，则（例如）可以将E写成$E=F(0)$，几乎不用证明.

如果$F\subsetneq E$，则必然存在$\alpha_1\in E$但$\alpha_1\notin F$，于是有$F\subsetneq F(\alpha_1)\subseteq E$，此时若$F(\alpha_1)=E$则已证完，否则存在$\alpha_2\in E$但$\alpha_2\notin F(\alpha_1)$，又有$F\subsetneq F(\alpha_1)\subsetneq F(\alpha_1,\alpha_2)\subseteq E$，此时若有$F(\alpha_1,\alpha_2)=E$则又已证完，否则上一过程继续. 注意$[F(\alpha_1,\cdots,\alpha_i):F(\alpha_1,\cdots,\alpha_{i-1})]>1$对任何$i\geq1$，所以以上过程必然在有限步以后中止（否则$[E:F]=\infty$），即存在$\alpha_1,\cdots,\alpha_k\in E$使得$E=F(\alpha_1,\cdots,\alpha_k)$.

$(2)\Rightarrow(1)$：考虑域扩张链：

$$F\subseteq F(\alpha_1)\subseteq F(\alpha_1,\alpha_2)\subseteq\cdots\subseteq F(\alpha_1,\cdots,\alpha_k)=E.$$

回忆：单扩张是有限扩张当且仅当它是代数单扩张，而注意α_i在F上代数$\Rightarrow$ α_i在$F(\alpha_1,\cdots,\alpha_{i-1})$上代数，从而每个单扩张都是代数单扩张$\Rightarrow$ 有限扩张，再根据有限扩张的传递性（有限次数的有限积仍然有限）可知$[E:F]<\infty$. $\square$

- 【命题】E/F是域扩张，设$E^{\mathrm{alg}}=\{\alpha\in E:\alpha在F上代数\}$，则$E^{\mathrm{alg}}$是$E$的子域，$F$的扩张，且$E^{\mathrm{alg}}$是$E$的子域，$F$的扩域，且$E^{\mathrm{alg}}/F$是$E/F$的**最大代数子扩张**，也就是$\forall K/F$是$E/F$的代数子扩张，即$K\subseteq E^{\mathrm{alg}}$.

【推论】这回答了上面的第二个问题，也就是：若α和β都在F上代数，则$\alpha\beta,\alpha\pm\beta,\alpha/\beta(\beta\neq0)$都在$F$上代数.

【证明】先证明E^{alg}是域. 只需证明E^{alg}中的元素在加、减、乘、除（取逆）下封闭，即：

$\forall \alpha, \beta \in E$在$E$上代数，都有$\alpha\beta, \alpha \pm \beta$，$\alpha/\beta(\beta \neq 0) \in E^{\text{alg}}$. 考虑有限扩张$F(\alpha, \beta)$（有限生成代数扩张$\Leftrightarrow$ 有限扩张），则α在F上代数$\Rightarrow$ $F(\alpha)/F$是有限扩张；β在F上代数$\Rightarrow$ β在$F(\alpha)$上代数$\Rightarrow$ $F(\alpha)(\beta)/F(\alpha)$有限，根据有限扩张的传递性，$F(\alpha, \beta)/F$是有限扩张$\Rightarrow$ $F(\alpha, \beta)/F$是代数扩张，所以$F(\alpha, \beta)$中任何元素都在F上代数，所以$\alpha \pm \beta, \alpha\beta, \alpha/\beta(\beta \neq 0) \in E^{\text{alg}}$. □

- 【例】$\mathbb{C}/\mathbb{Q}$，则$\mathbb{C}^{\text{alg}} = \overline{\mathbb{Q}}$是代数数的全体，根据上面的命题，$\overline{\mathbb{Q}}$是$\mathbb{Q}$的扩域而且$\overline{\mathbb{Q}}/\mathbb{Q}$是代数扩张. 但是它不是有限扩张. 这是因为，假设扩张次数为n，那么考虑$\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt[n+1]{2})/\mathbb{Q}$，因为$x^{n+1} - 2$在$\mathbb{Q}$上不可约（Eisenstein），所以$[\mathbb{Q}(\sqrt[n+1]{2}) : \mathbb{Q}] = n + 1$. 因为$\overline{\mathbb{Q}}/\mathbb{Q}$是最大代数子扩张，所以$\mathbb{Q}(\sqrt[n+1]{2}) \subset \overline{\mathbb{Q}}$，所以$n + 1 \leq n$，矛盾.□
- 【命题】（代数扩张的传递性）

  E/K，K/F都是代数扩张（**不必是有限的**），则E/F也是代数扩张.

  【证明】（还是要用到有限扩张的传递性以及有限扩张等价于代数扩张且有限生成）

  $\forall \alpha \in E$，E/K是代数扩张$\Rightarrow$ α在K上代数，所以存在$f(x) = c_0 + c_1 x + \cdots + c_n x^n \in K[x]$，使得$f(\alpha) = 0$且$f \neq 0$，将这些系数添加进来，即令$K' = F(c_0, \cdots, c_n)$，则$f(x) \in K'[x]$，而且$f(\alpha) = 0$，所以$\alpha$在$K'$上代数.

  注意$F \subseteq K' \subseteq K \subseteq E$，$K/F$是代数扩张，所以$K'$中的所有元素都在$F$上代数，所以$K'/F$是代数扩张. 又因为$K'/F$是有限生成扩张，以上两个条件告诉我们$K'/F$是有限扩张.

  α在K'上代数$\Rightarrow$ $K'(\alpha)/K'$是有限扩张，根据有限扩张的传递性$K'(\alpha)/F$也是有限扩张$\Rightarrow$ 是代数扩张，所以α在F上代数，根据α的任意性知E/F是代数扩张.

  【推论】E/F是域扩张，若$\alpha_1, \cdots, \alpha_k \in E$在$F$上代数，则$F(\alpha_1, \cdots, \alpha_k)/F$是有限扩张. 事实上，$F(\alpha_1, \cdots, \alpha_k)$是有限生成的代数扩张.

  【证明】逐步添加α_i，再利用代数扩张的传递性.□

  【remark1】实际上**在前面就可以证明这个结论了**，因为这是有限的情况，可以在每一步都利用单扩张的结论，而对于单扩张来说，代数扩张已经能推出有限扩张，利用有限扩张的传递性即可！
- 【命题】E/F是域扩张，S是E的子集而且S中的元素都在F上代数（不必是有限子集），则$F(S)/F$是代数扩张，而且$F(S) = F[S]$.

  【remark】这表明，代数元集生成的域扩张必然是代数扩张.

  【引理】E/F是代数扩张，K是E的含F的子环，则K是E的子域.

  【证明】E是域$\Rightarrow$ E是整区. 因为K是E的子环，所以K也是整区，因此只需说明$\forall \alpha \in K - 0$，$\alpha \in K^\times$. 这是因为，α是$F[\alpha]$中的元素，而E/F代数扩张$\Rightarrow$ α在F上代数$\Rightarrow$ $F[\alpha]$是域（单扩张结构），所以$\alpha^{-1} \in F[\alpha]$. 又因为根据定义，$F[\alpha]$是含有$F$和$\alpha$的$E$的最小子环，所以$F[\alpha] \subseteq K$，所以$\alpha^{-1} \in K$，这说明$\alpha \in K^\times$.□

  【命题的证明】考虑$E^{\text{alg}} = \{\alpha \in E : \alpha \text{在} F \text{上代数}\}$，则$E^{\text{alg}}$是$E$的子域，$F$的扩域，且$E^{\text{alg}}/F$是代数扩张.

  考虑$F[S]$，因为$S \subset E^{\text{alg}}$，所以$F[S]$是E^{alg}的含F的子环，根据引理可知它是E^{alg}的子域. 因为它是域，所以其分式域等于本身，所以$F(S) = \text{Frac}(F[S]) = F[S]$. 因为$F(S) \subset E^{\text{alg}}$，所以$F(S)$中元都在$F$上代数，所以$F(S)/F$是代数扩张.□
- 【一个重要例题】$E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$，则$[E : \mathbb{Q}]$是多少？$E$作为$\mathbb{Q}-$线性空间的一组$\mathbb{Q}-$基是什么？为什么$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$?
  - 第一问，$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$，分别求出每个代数单扩张的极小多项式（分别为$x^2 - 2$和$x^2 - 3$，中间涉及到$\min(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = \min(\sqrt{3}, \mathbb{Q})$的证明），进而根据单扩张结构知道每一步的扩张次数（等于极小多项式的次数，都是2），再根据次数的乘性可知$[E : \mathbb{Q}] = 4$. 为了找E的$\mathbb{Q}$基，可以先找E的$\mathbb{Q}(\sqrt{2})-$基$(1, \sqrt{3})$，再找$\mathbb{Q}(\sqrt{2})$的$\mathbb{Q}-$基$(1, \sqrt{2})$，再根据前面扩张次数传递性定理中的构造方法可知E的一组$\mathbb{Q}-$基为$(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$.
  - 第二问，为什么$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$? 很容易看出后面的是前面的一个子域，设$\beta = \sqrt{2} + \sqrt{3}$，注意$1, \beta, \beta^2, \beta^3$作为$\mathbb{Q}(\beta)$中的元素是$\mathbb{Q}-$线性无关的（注意$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$是$\mathbb{Q}-$线性无关的，而这四个向量相当于用可逆线性变换作用这个线性无关向量组，依然是线性无关的），所以$[\mathbb{Q}(\beta) : \mathbb{Q}] \geq 4$，而$[E : \mathbb{Q}] = 4$，所以只能是$[E : \mathbb{Q}(\beta)] = 1$，所以$E = \mathbb{Q}(\beta)$.
- 【例】R是整区，k是R的子域，则R在k中元素的乘法和自身的加法下构成$k-$线性空间. 若已知R作为$k-$线性空间是有限维的即$\dim_k R < \infty$，则R是域.

【证明】设$\dim_k R=n$，取R的一组k基为$\alpha_1,\cdots,\alpha_n\in R$，考虑$k[\alpha_1,\cdots,\alpha_n]$.

断言：α_i在k上代数. 这是因为，$\dim_k R=n$，所以$1,\alpha_i,\cdots,\alpha_i^n$必然$k-$线性相关，即存在$c_0,\cdots,c_n\in k^\times$不全为$0$，使得$c_0+c_1\alpha_i+\cdots+c_n\alpha_i^n=0$，即存在$f(x)\in k[x]$，$f(x)\neq 0$，$f(\alpha_i)=0$，所以$\alpha_i$在$k$上代数.

注意：

$$\begin{aligned}k[\alpha_1,\cdots,\alpha_n]&=k[\alpha_1][\alpha_2,\cdots,\alpha_n]=k(\alpha_1)[\alpha_2][\alpha_3,\cdots,\alpha_n]\\&=k(\alpha_1)(\alpha_2)[\alpha_3][\alpha_4,\cdots,\alpha_n]=\cdots=k(\alpha_1,\cdots,\alpha_n)\end{aligned}$$

这里用到α_i在k上代数$\Rightarrow\alpha_i$在$k(\alpha_1,\cdots,\alpha_{i-1})$上代数.

也可以根据$\{\alpha_1,\cdots,\alpha_n\}$是代数元集直接得到$k[\alpha_1,\cdots,\alpha_n]=k(\alpha_1,\cdots,\alpha_n)$.

因为$k[\alpha_1,\cdots,\alpha_n]$是$R$的子环，另一方面$\alpha_1,\cdots,\alpha_n$是$R$的作为$k-$线性空间的一组生成元，所以有$R=k[\alpha_1,\cdots,\alpha_n]$，所以进一步有$R=k(\alpha_1,\cdots,\alpha_n)$即$R$是域.□

4. 代数闭域和域的代数闭包

- 【代数闭域的等价定义】F是域，则以下等价：
  - $F[x]$中任一非常数多项式在F中有至少一个根；
  - $F[x]$中任一$n(\geq 1)$次多项式在$F[x]$中分解为1次因式的乘积（或：在计入重数的意义下有n个根）
  - $F[x]$中不可约多项式均为一次多项式；
  - F没有真代数扩域，即若E/F是代数扩张，则$E=F$.

  满足这些条件的域称为代数封闭域.
- 【代数学基本定理】$\mathbb{C}$是代数封闭域.
- 【代数闭包】E/F是代数扩张而且E代数封闭，则称E是F的一个代数闭包.

  代数闭包的等价定义：E/F是代数扩张且$F[x]$内任一多项式$f(x)$在$E[x]$中分解为一次因式的乘积（即$F[x]$中任何多项式都在E上分裂），则称E是F的一个代数闭包.

  【证明】①推②用代数闭域的最后一条定义. ②推①：只要证明E代数封闭. 设L/E是代数扩张，去证明$L=E$. $\forall\alpha\in L$，设α在E上的极小多项式为$f(x)$，考虑$L/E/F$，设α在F上的极小多项式为$p(x)$，则$f(x)\mid p(x)$在$E[x]$中. 因为$p(x)\in F[x]$，所以$p(x)$在$E[x]$中分解为一次因式的乘积. 因为$f(x)$是极小多项式，所以$f(x)$是不可约多项式，所以必然有$\deg f(x)=1$（即$f(x)$是$p(x)$在$E[x]$中的一个一次因式，否则，由整除可知$f(x)$在$E[x]$中分解为一次因式的乘积，这与不可约矛盾）. 因为$f(\alpha)=0$，所以$f(x)=x-\alpha$，故$\alpha\in E$，以上证明了$L=E$.□
- 问题：代数闭包是否存在？如果存在，是否唯一？我们首先给出一个特殊情况下代数闭包的构造方法.

  【命题】设L是F的扩域且L**代数封闭**，记$L^{\mathrm{alg}}=\{\alpha\in L:\alpha在F上代数\}$，则根据前面的命题知道$L^{\mathrm{alg}}$是$L$的子域，$F$的扩域，而且$L^{\mathrm{alg}}/F$是代数扩张.

  事实上，L^{alg}也是代数封闭的，这说明L^{alg}是F的一个代数闭包.

  【remark】这个命题的意思是，如果已经有了一个大的域是代数封闭的，则可以通过这个域构造F的代数闭包.

  【证明】只需要证明L^{alg}是代数封闭的. 记$L^{\mathrm{alg}}=E$，设$p(x)$是E中任一不可约多项式，则$p(x)\in E[x]\subseteq L$，因为L是代数封闭的，所以存在$\alpha\in L$，使得$p(\alpha)=0$，所以α在E上代数，所以$E(\alpha)/E$是代数扩张. 根据代数扩张的传递性知道$E(\alpha)/F$是代数扩张，所以α在F上代数，根据定义，$\alpha\in E$，因此$\min(\alpha,E)=x-\alpha$. 注意$p(x)\in E[x]$不可约而且$p(\alpha)=0$，所以$p(x)$是α在E上的最小多项式，所以$p(x)=x-\alpha$，所以$\deg p(x)=1$.□

  【remark】因为E是代数封闭的，所以$F[x]$内非零多项式在L中的根必在E内；反过来，因为E/F是代数扩张，所以E中任何元素都是$F[x]$中某个多项式的根，所以，如果L是代数封闭的，则还可以这样描述按上述方法定义的F的代数闭包：

  $$E=L^{\mathrm{alg}}=\{\alpha\in L:\alpha在F上代数\}=\{\alpha\in L:\alpha是F-系数非零多项式在L中的根\}$$

  【推论】$\mathbb{C}$是代数封闭域，$\overline{\mathbb{Q}}=\mathbb{C}^{\mathrm{alg}}=\{代数数的全体\}$是$\mathbb{Q}$的一个代数闭包.
- 那么，对于一般情况，如何构造代数闭包？我们先叙述最终要证明的大定理：

【定理】（代数闭包的存在唯一性）设F是域，则F的代数闭包存在，且在$F-$同构下唯一，即：若E_1, E_2是F的代数闭包，则存在同构$\sigma: E_1 \to E_2$，且$\sigma|_F = \mathrm{id}_F$.

【证明】存在性：证明思路类似于构造一个多项式的分裂域，不过这里一下子要处理$F[x]$中所有的多项式，所以过程更加复杂，且不可避免地要用到Zorn引理，具体参考：Dummit and Foote, p.544, Prop 30.

唯一性：可以用下面的【命题】说明存在一个从E_1到E_2的$F-$嵌入，即$\sigma: E_1 \to E_2$是单同态，而且$\sigma|_F = \mathrm{id}_F$. 还需说明$\sigma$是满射即可. $\forall \alpha \in E_2$，因为E_2/F是代数扩张，所以α在F上代数. 注意$E_1 \cong \sigma(E_1)$，因为E_1是代数封闭的，所以$\sigma(E_1)$也是代数封闭的（例如用代数封闭域的第三条定义）. α在F上代数$\Rightarrow$ α是$F[x]$中某个多项式在E_2中的根，而$\sigma(E_1)$是F的扩域，E_2的子域，所以$\alpha \in \sigma(E_1)$，这说明$\sigma(E_1) = E_2$，即σ是满射. 所以，σ是$F-$同构.□

- 【命题】E/F是代数扩张，$\overline{F}$是F的一个代数闭包，则存在一个E到$\overline{F}$的$F-$嵌入，即存在$\sigma: E \to \overline{F}$是（单）同态而且$\sigma|_F = \mathrm{id}_F$.

  【remark】我们从一个比较简单的情况入手，即考虑E/F是最简单的代数扩张——代数单扩张的情形.为了给出**一般性的技术**，我们不考虑代数闭包，而是考虑如何构造$F(\alpha)$到一个一般的扩域L上的**延拓**.

- 【命题】设E/F是代数单扩张，即$E = F(\alpha)$，其中，α在F上代数. L是另一个域，而且$\sigma: F \to L$是一个单同态.

  设α在F上极小多项式是$p(x)$，且域同态$\sigma: F \to L$诱导了一个多项式环同态$F[x] \to L[x]$（作用在多项式的系数上），也记录σ，则：

  设$\sigma': F(\alpha) \to L$是$\sigma: F \to L$的一个延拓，即σ'是（单）同态而且$\sigma'|_F = \sigma$. 那么，满足上面的条件的σ'和下面的集合有$1:1$对应，即：

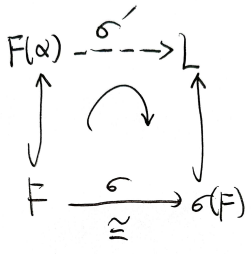
  $$\{\sigma\text{到}F(\alpha)\text{的延拓}\} = \{\sigma(p(x))\text{在}L\text{中的根}\}$$

  对应法则为：

  $$\sigma' \mapsto \sigma'(\alpha)$$

  从右向左：

  $$\beta \mapsto [f(\alpha) \mapsto \sigma(f)(\beta)]$$



【remark】这个级数将$F \to L$的（单）同态σ 延拓为同态：$\sigma': F(\alpha) \to L$.

【证明】

首先假设已经构造出了σ'是σ到$F(\alpha)$的延拓，去证明$\beta = \sigma'(\alpha)$是$\sigma(p(x))$在L中的根. 设$p(x) = c_0 + c_1 x + \cdots + c_n x^n$，则$p(\alpha) = c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$，其中$c_i \in F$，用$\sigma'$作用并根据$\sigma|_F = \mathrm{id}_F$得：

$$\sigma'(p(\alpha)) = \sigma'(c_0) + \sigma'(c_1)\sigma'(\alpha) + \cdots + \sigma'(c_n)(\sigma'(\alpha))^n = \sigma(c_0) + \sigma(c_1)\beta + \cdots + \sigma(c_n)\beta^n = 0$$

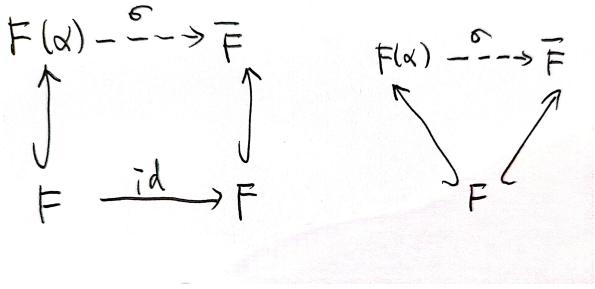
所以$\sigma'(p(\alpha)) = \sigma(p)(\beta) = 0$，于是$\beta$是$\sigma(p(x))$在$L$中的根.

另一方面，设β是$\sigma(p(x))$在L中的根，去构造一个σ在$F(\alpha)$的延拓. 因为α在F上代数，所以$F(\alpha) = F[\alpha]$，所以$F(\alpha)$中的元素形如$f(\alpha)$，其中$f(x) \in F[x]$. 注意$F(\alpha)$是由F和α生成的子域，而$\sigma'|_F = \sigma$，所以这样的σ'由它在α处的取值唯一决定. 令$\sigma'(\alpha) = \beta$，从而$\sigma'(f(\alpha)) = \sigma(f)(\beta)$，我们验证后者是良定义的. 注意在$F(\alpha)$中两个元素相等$f(\alpha) = g(\alpha)$当且仅当$p(x) \mid f(x) - g(x)$，用$\sigma'$作用得$\sigma(p(x)) \mid \sigma(f(x)) - \sigma(g(x))$，因为$\sigma(p)(\beta) = 0$，所以$\sigma(f-g)(\beta) = \sigma(f)(\beta) - \sigma(g)(\beta) = 0$，这样证明了

$f(\alpha)=g(\alpha)\Rightarrow\sigma(f)(\beta)=\sigma(g)(\beta)$，所以$\sigma'$是良定义的. 容易验证$\sigma'$是域同态（保加保乘，保恒等元），而且$\sigma'|_F=\sigma$，这就证明了以上结论.□

【例】看一个简单的例子，设$F(\alpha)/F$是代数单扩张，$\overline{F}$是F的代数闭包，则存在$\sigma:F(\alpha)\to\overline{F}$是一个$F-$嵌入.

【证明】对以下交换图用前面命题中的技术.□



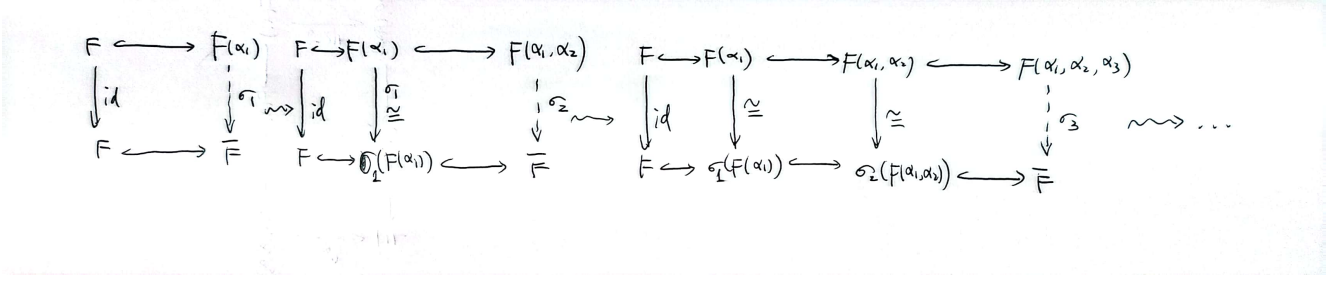
【remark】对于代数单扩张而言，因为$p(x)\in F[x]\subseteq\overline{F}[x]$，所以$p(x)$在$\overline{F}$中至少有1个根，所以上面技术性命题中右边的集合总是非空的，因而从$F(\alpha)$到$\overline{F}$的σ的延拓总是存在的.

- 【命题】E/F是有限扩张，根据有限扩张⇔ 有限生成代数扩张⇔ 有限个代数元生成的扩张：

  存在$\alpha_1,\cdots,\alpha_k\in E$，其中每个$\alpha_i$在$F$上代数，使得$E=F(\alpha_1,\cdots,\alpha_k)$. 这样，$E/F$实现为$k$个代数单扩张的叠加：

  $$F\subseteq F(\alpha_1)\subseteq F(\alpha_1,\alpha_2)\subseteq\cdots\subseteq F(\alpha_1,\cdots,\alpha_k)$$

  在已经有$F-$嵌入$\sigma_{i-1}:F(\alpha_1,\cdots,\alpha_{i-1})\to\overline{F}$的基础上，对下面的交换图用上面的技术可以构造出$\sigma_{i-1}$的延拓$\sigma_i:F(\alpha_1,\cdots,\alpha_i)\to\overline{F}$，如此继续下去就得到了$E\to\overline{F}$的$F-$嵌入$\sigma$.

  □

- 【主命题】E/F是代数扩张，$\overline{F}$是F的一个代数闭包，则存在$\sigma:E\to\overline{F}$是一个$F-$嵌入，即σ是（单）同态而且$\sigma|_F=\mathrm{id}_F$.

  【主命题的证明】这不是有限的情况，因此需要使用Zorn引理. 定义如下的集合X：

  $$X:=\{(K,\sigma)|K/F\text{是}E/F\text{的子扩张},\text{且}\sigma:K\to\overline{F}\text{是一个}F-\text{嵌入}\}.$$

  显然$(F,i:F\to\overline{F})\in X$，所以$X$不是空集. 在$X$上定义一个二元关系：

  $$\preceq:\quad (K_1,\sigma_1)\preceq(K_2,\sigma_2)\Leftrightarrow K_1\subseteq K_2\text{且}\sigma_2\text{是}\sigma_1\text{的延拓},\text{即}\sigma_2|_{K_1}=\sigma_1.$$

  容易验证此二元关系满足反身性、反对称性和传递性，因此这是一个**偏序**.

  取X中的一个链$\{(K_i,\sigma_i)\}_{i\in I}$（i.e. $\forall i,j\in I$，都有$(K_i,\sigma_i)\preceq(K_j,\sigma_j)$或者$(K_j,\sigma_j)\preceq(K_i,\sigma_i)$）我们说明该链有上界. 为此，取$K=\bigcup_{i\in I}K_i$，容易验证$K$对元素的加法、乘法以及取逆是封闭的，因此$K$是$E/F$的中间域. 在$K$上定义$\sigma$：

  $$\sigma:K\to\overline{F},\quad a_i\mapsto\sigma_i(a_i),\forall a_i\in K_i.$$

  容易验证这是良定义的，即如果$a_i\in K_i$且$a_i\in K_j$，则必有$K_i\supseteq K_j$或者$K_i\subseteq K_j$，不妨假设是$K_i\supseteq K_j$，则此时$\sigma_i|_{K_j}=\sigma_j$，所以$\sigma_i(a_i)=\sigma_j(a_i)$.

  进而可以验证这是一个域同态，而且$\sigma|_F=\mathrm{id}_F$，所以$(K,\sigma)\in X$.

注意$\forall i\in I$，都有$K\supseteq K_i$且根据定义方式可知$\sigma|_{K_i}=\sigma_i$，即$(K_i,\sigma_i)\preceq(K,\sigma)$，于是$(K,\sigma)$是链$\{(K_i,\sigma_i)\}_{i\in I}$的上界. 根据Zorn引理，$X$有极大元，也记为$(K,\sigma)$，下面证明$K=E$. 用反证法，假设$K\subsetneq E$，则存在$\alpha\in E$，$\alpha\notin K$，考虑$K(\alpha)$，因为$E/F$是代数扩张，所以$\alpha$在$F$上代数$\Rightarrow$ α在K上代数，所以$K(\alpha)/K$是代数单扩张. 设$p(x)$是α在K上的极小多项式，根据前面的技术性命题可知以下两个集合为1：1对应：

$$\{\tau:K(\alpha)\to\overline{F}:\tau|_K=\sigma\}=\{\sigma(p(x))在\overline{F}中的根\}$$

因为$\overline{F}$是代数闭域，所以$\sigma(p(x))\in\overline{F}[x]$在$\overline{F}$中至少有一个根，所以不是空集，所以存在$(K(\alpha),\tau)\in X$，$\tau$是$\sigma$的延拓，因此有严格序：

$$(K,\sigma)\preceq(K(\alpha),\tau)\quad 且(K,\sigma)\neq(K(\alpha),\tau).$$

这与(K,σ)是X的极大元矛盾，所以$K=E$. 因此这样的延拓σ存在.□

【remark】代数闭包的概念可以扩展. 即如果E是代数封闭域，$i:F\to E$是单同态（i建议我们将F等同于$i(F)$从而看成是E的子域），而$E/i(F)$是代数扩张，那么称(E,i)是F的一个代数闭包.

- 【例】以上命题中的σ是不唯一的，看下例：

  $F=\mathbb{Q}$，$E=\mathbb{Q}(\sqrt{2})$，问$\sigma:F\to\overline{\mathbb{Q}}$在$E$上的延拓是否唯一？

  【解】根据前面的命题，对于代数单扩张E/F，以下为一一对应：

  $$\{\sigma:E\to\overline{\mathbb{Q}}是F-嵌入\}=\{\sigma(p(x))在\overline{\mathbb{Q}}中的根\}$$

  注意$\sigma(p(x))=p(x)=x^2-2$，在$\overline{\mathbb{Q}}$中的根为$\pm\sqrt{2}$，根据对应法则可知有如下两个不同的延拓：

  $$\sigma^{\pm}:E\to\overline{\mathbb{Q}},\quad \sqrt{2}\mapsto\pm\sqrt{2},\quad \sigma^{\pm}|_{\mathbb{Q}}=\mathrm{id}_{\mathbb{Q}}.$$

  但是$\mathrm{Im}\sigma^{\pm}$都等于$\mathbb{Q}(\sqrt{2})$.

多项式的分裂域

1.分裂域，简单分裂域的计算方法

- 【定义】F是域，E/F，$f(x)\in F[x]$，$\deg f(x)\geq 1$，若$f(x)$在$E[x]$内分解为一次多项式的乘积，则称$f(x)$在E上分裂.
- 【例】$F[x]$内非常数多项式在$\overline{F}$上分裂.

  若$L/E/F$，若$f(x)\in F[x]$在E上已经分裂，则$f(x)$在L上分裂.

  $E/K/F$，若$f(x)\in F[x]$在E上分裂，则$f(x)$作为K系数多项式的任何因式都在E上分裂.
- 【分裂域的定义】E/F是域扩张，$f(x)\in F[x]$，$\deg f(x)\geq 1$，若：

  ① $f(x)$在E上分裂；

  ② $f(x)$在E的任何真子域上不分裂.

  或者等价地（下面这个等价定义往往更好用）：

  ① $f(x)$在E上分裂，即存在$\alpha_1,\cdots,\alpha_k\in E$，$c\in F^{\times}$，使得$f(x)=c(x-\alpha_1)\cdots(x-\alpha_k)$.

  ② $E=F(\alpha_1,\cdots,\alpha_k)$.

  （两者为什么等价：上推下：若下面是真包含，则f在E的真子域上分裂已经矛盾；下推上：因为$E=F(\alpha_1,\cdots,\alpha_k)$是包含$F$和$\alpha_1,\cdots,\alpha_k$的最小子域，所以其真子域必不含某个$\alpha_i$，与分裂矛盾）

  则称E是$f(x)$在F上的分裂域，记为$\mathrm{Split}(F,f(x))$.

  【remark1】这说明，如果$f(x)\in F[x]$在F的扩域L上分裂且$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$在$L[x]$中，则$F(\alpha_1,\cdots,\alpha_n)$是$f(x)$在$F$上的一个分裂域.（通过把在大的域上的根加进来得到分裂域）

  【remark2】若E是f在F上的分裂域，K是E/F的中间域，则E也是f在K上的分裂域. 这是因为已知$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$在$E$内，且$E=F(\alpha_1,\cdots,\alpha_n)=K(\alpha_1,\cdots,\alpha_n)$（最后一个等号因为$F(\alpha_1,\cdots,\alpha_n)\subseteq K(\alpha_1,\cdots,\alpha_n)\subseteq E$，根据分裂域的第二个外显定义可知$E$是$f$在$K$上的分裂域.

【remark3】同一个多项式在不同域上的分裂域往往不一样.例如$f(x)=x^2-2$在$\mathbb{C}$上的分裂域就是$\mathbb{C}$，而在$\mathbb{Q}$上的分裂域则是$\mathbb{Q}(\sqrt{2})\neq\mathbb{C}$.

- 【命题】（分裂域的存在性以及分裂域的两种构造）

  设$f(x)\in F[x]$，$\deg f\geq 1$，则$f(x)$在F上的分裂域存在.

  【证明方法1】考虑$\overline{F}$是F的代数闭包（前已证明代数闭包存在），则$f(x)$在$\overline{F}$上分解为一次多项式的乘积（不妨设f是首一多项式）：

  $$f(x)=(x-\alpha_1)\cdots(x-\alpha_k)$$

  考虑$F(\alpha_1,\cdots,\alpha_k)$，则根据分裂域的定义可知$F(\alpha_1,\cdots,\alpha_k)$就是$f(x)$的分裂域.

  【证明方法2】思路是：通过商掉多项式的不可约因子生成的主理想得到扩域，在扩域中多项式可以析出一次因式，逐步做下去即得到多项式的分裂域.

  对多项式的次数用数学归纳法. 若$\deg f=1$，则$f(x)$在F上已经分裂，所以$f(x)$的分裂域就是F.

  假设对于$\deg f\leq n-1$的情形命题都成立，这里考虑$\deg f=n$的情况.

  $f(x)\in F[x]$，不妨设$f(x)$首一，取$f(x)$的不可约因子$p(x)$，考虑$F[t]/(p(t))$，因为$p(x)$是不可约多项式，所以$F[t]/(p(t))$是域. 记这个域为K，$\alpha:=\overline{t}\in K$，则$p(\alpha)=0$. 因为$p(x)\mid f(x)$，所以$f(\alpha)=0$，所以$f(x)=(x-\alpha)g(x)$在$K[x]$中，$\deg g(x)=\deg f-1=n-1$.对$g(x)$和$K$用归纳假设可知存在$E$是$g(x)$在$K$上的分裂域，于是$g(x)$在$E[x]$上分解为一次因式的乘积$g(x)=(x-\alpha_2)\cdots(x-\alpha_n)$，于是$f(x)=(x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n)$在$E[x]$中，所以$f(x)$在$E$上分裂. 因为$E$是$g(x)$在$K$上的分裂域，所以$E$的形状为：$E=K(\alpha_2,\cdots,\alpha_n)=K(\alpha,\alpha_2,\cdots,\alpha_n)$. 注意$p(x)$在$F[x]$不可约且$p(\alpha)=0$，所以$p$是$\alpha$在$F$上的极小多项式，所以根据单扩张的结构：

  $$K=F[t]/(p(t))=F(\alpha).$$

  所以$E=K(\alpha,\alpha_2,\cdots,\alpha_n)$，所以$E=F(\alpha,\cdots,\alpha_n)$，根据分裂域的定义可知$E$是$f$在$F$上的分裂域.□

- 【例】计算$\mathrm{Split}(\mathbb{Q},x^2-2)$；$\mathrm{Split}(\mathbb{Q},(x^2-2)(x^2-3))$

  【解】第一个，如果用方法1的构造思路，考虑x^2-2在$\overline{\mathbb{Q}}$上的根$\pm\sqrt{2}$，则根据分裂域的定义可知：

  $$\mathrm{Split}(\mathbb{Q},x^2-2)=\mathbb{Q}(\sqrt{2},-\sqrt{2})=\mathbb{Q}(\sqrt{2}).$$

  如果用方法2的构造思路，因为x^2-2在$\mathbb{Q}$上已经不可约，所以直接考虑$K=\mathbb{Q}[t]/(t^2-2)$，$\alpha=\overline{t}\in K$满足$\alpha^2-2=0$，在$K[x]$中$x^2-2=(x-\alpha)(x+\alpha)$，所以：

  $$\mathrm{Split}(\mathbb{Q},x^2-2)=K=\mathbb{Q}[t]/(t^2-2).$$

  两种计算方法得到的分裂域是同构的.

  第二个，如果用方法1，$(x^2-2)(x^2-3)$在$\overline{\mathbb{Q}}$上的根为$\pm\sqrt{2}$，$\pm\sqrt{3}$，于是：

  $$\mathrm{Split}(\mathbb{Q},(x^2-2)(x^2-3))=\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

  用方法2：注意x^2-2和x^2-3是两个不可约因式，首先对考虑x^2-2，x^2-2在$\overline{\mathbb{Q}}$上不可约，所以$K:=\mathbb{Q}[t]/(x^2-2)$是扩域，$\alpha:=\overline{t}\in K$，则在$K[x]$上：

  $$(x^2-2)(x^2-3)=(x-\alpha)(x+\alpha)(x^2-3).$$

  $f(x)=(x-\alpha)(x+\alpha)(x^2-3)\in K[x]$在$K$的扩域$E$上分裂当且仅当$x^2-3$在$K$的扩域上分裂，所以$f(x)$在$K$上的分裂域就是$x^2-3$在$K$上的分裂域. 由注意到$\mathrm{Split}(\mathbb{Q},f(x))=\mathrm{Split}(K,f(x))$（前面的事实：若是$\mathbb{Q}$的分裂域，则必然也是中间域的分裂域），所以$\mathrm{Split}(\mathbb{Q},f(x))=\mathrm{Split}(K,x^2-3)$.

  事实上x^2-3在K上不可约（注意x^2-3在$\mathbb{Q}(\sqrt{2})$没有根），所以：

  $$\mathrm{Split}(\mathbb{Q},f(x))=\mathrm{Split}(K,x^2-3)=K[s]/(s^2-3).$$

- 【例】E是$f(x)$在F上的分裂域，$f(x)\in F[x]$是n次多项式，则：E/F是有限扩张，且$[E:F]\leq n!$.

【分析】思路类似于分裂域存在性的第二个构造性证明，即每次对一个不可约因子构造扩域使得多项式在较大的域上先析出一个一次因式（注意不可约因子的根必然也会是$f(x)$的根），然后对次数用归纳假设.

【证明】对多项式的次数用数学归纳法.

$n=1$时，$f(x)$是一次多项式，所以$f(x)$在F上已经分裂，因此$E=F$，此时$[E:F]=1$，命题显然成立.

假设命题对于**任意域**上$n-1$次多项式已经成立（注意上面的归纳基础不依赖于域，所以可以对任意域做归纳假设），去考虑$\deg f(x)=n$的情况.

不妨设$f(x)$是首一多项式，取$f(x)$的一个不可约因子$p(x)$，则$K=F[t]/(p(t))$是E的扩域，令$\alpha=\overline{t}\in K$，则$p(\alpha)=0$. 因为$p(x)\mid f(x)$，所以$f(\alpha)=0$在$K[x]$上，所以$K[x]$上有分解：

$$f(x)=(x-\alpha)g(x).$$

则$\deg g(x)=n-1$，$g(x)\in K[x]$，因为$E=\mathrm{Split}(F,f(x))$，而K可以看成是E/F的中间域，所以$E=\mathrm{Split}(K,f(x))=\mathrm{Split}(K,g(x))$，根据归纳假设可知$E/K$是有限扩张且$[E:K]\leq(n-1)!$. 而因为$K=F[t]/(p(t))=F(\alpha)$，根据代数单扩张的结构可知$[K:F]=\deg\min(\alpha,F)$，由$p(\alpha)=0$以及$p$首一且不可约可知$p(x)$是$\alpha$在$F$上的极小多项式，所以$[K:F]=\deg p(x)\leq\deg f(x)=n$，所以$E/F$也是有限扩张而且：

$$[E:F]=[E:K][K:F]\leq(n-1)!n=n!$$

由数学归纳法可知命题成立.□

- 【例】这道例题是为了考虑清楚域上二次多项式$f(x)=ax^2+bx+c(a\in F^\times)$的一般情况.

  即：若$\mathrm{char}F\neq 2$，计算$\mathrm{Split}(F,ax^2+bx+c)$.

  【解】注意：

$$f(x)=a(x^2+\frac{b}{a}x+\frac{c}{a})=ag(x).$$

$$g(x)=x^2+\frac{b}{2a}x+\frac{b^2}{4a^2}-\frac{b^2-4ac}{4a^2}=h(x+\frac{b}{2a});\quad \frac{b}{2a}\in F.$$

$$h(x)=x^2-\frac{b^2-4ac}{4a^2}=\frac{(2ax)^2-\triangle}{4a^2};\quad \triangle=b^2-4ac\in F.$$

  由此可知

$$\mathrm{Split}(F,f(x))=\mathrm{Split}(F,g(x))=\mathrm{Split}(F,h(x))=\mathrm{Split}(F,x^2-\triangle)=\text{“}F(\sqrt{\triangle})\text{”}$$

  分两种情况：

$$[F(\sqrt{\triangle}):F]=1\Leftrightarrow\triangle\in F^2(\text{i.e.}\exists x\in F,x^2=\triangle)\Leftrightarrow f(x)\text{在}F\text{上已经分裂},$$
$$[F(\sqrt{\triangle}):F]=2\Leftrightarrow\triangle\notin F^2\Leftrightarrow f(x)\text{在}F\text{上不可约}.$$

  前一种情况下，$\mathrm{Split}(F,f(x))=F$，后一种情况下，$\mathrm{Split}(F,f(x))=F(\sqrt{\triangle})$.

  【remark】后一种情况下，$f(x)$是F上二次不可约多项式，此时用前面的第二种构造方式也可以算出F的分裂域是$F[t]/(f(t))$.

- 【例】计算$\mathrm{Split}(\mathbb{Q},x^3-2)$

  【解】第一种构造$\mathrm{Split}(\mathbb{Q},x^3-2)=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=\mathbb{Q}(\sqrt[3]{2},\omega)$

  第二种构造：先构造$K=\mathbb{Q}[t]/(t^3-2)$，设$\alpha=\overline{t}\in K$，则在$K[x]$中有分解：

$$x^3-2=x^3-\alpha^3=(x-\alpha)(x^2+\alpha x+\alpha^2)=\alpha^2(x-\alpha)((\frac{x}{\alpha})^2+\frac{x}{\alpha}+1)$$

  所以

$$\mathrm{Split}(\mathbb{Q},x^3-2)=\mathrm{Split}(K,x^3-2)=\mathrm{Split}(K,x^2+\alpha x+\alpha^2)=\mathrm{Split}(K,x^2+x+1).$$

我们已经学过了判定二次多项式是否分裂的准则，即$\sqrt{\triangle}$是否在K内，计算得到$\triangle=-3$，我们已经知道$\nexists q\in\mathbb{Q}$使得$q^2=-3$，若存在$\gamma\in K$使$\gamma^2=-3$，则有$\mathbb{Q}\subset\mathbb{Q}(\gamma)\subset K$，因为$x^2-3$在$\mathbb{Q}$上不可约，所以$[\mathbb{Q}(\gamma):\mathbb{Q}]=\deg(x^2-3)=2$，而这与$[K:\mathbb{Q}]=3=[K:\mathbb{Q}(\gamma)][\mathbb{Q}(\gamma):\mathbb{Q}]$矛盾，所以$x^2+x+1$在$K$上不可约，于是：

$$\mathrm{Split}(\mathbb{Q},x^3-2)=\mathrm{Split}(K,x^2+x+1)=K[s]/(s^2+s+1)=K(\sqrt{-3}).$$

2. 分裂域的唯一性

- 我们接下来将处理分裂域的唯一性，里面用到的大部分技术是前面提到过的，同时也会衍生出一些新的概念.
- 【定理（分裂域的唯一性）】

  设F_1,F_2是域，$\sigma:F_1\to F_2$是域同构，其诱导的多项式环同构（作用在多项式系数上）也记为$\sigma:F_1[x]\to F_2[x]$. $f_1(x)\in F_1[x]$，$f_2(x)\in F_2[x]$，$\deg f_1=\deg f_2\geq 1$，E_1,E_2分别是$f_1(x)$和$f_2(x)$在F_1和F_2上的分裂域.

  则：

  ①存在同构$\sigma':E_1\to E_2$，且σ'是σ的延拓，即$\sigma'|_{F_1}=\sigma$.

  ②$[E_1:F_1]=[E_2:F_2]$.

  ③满足(1)条件的不同的延拓σ'的个数至多为$[E_i:F_i]$，其中$i=1,2$.

  特别地：取$F_1=F_2=F$，$\sigma=\mathrm{id}$是恒等自同构，则存在$F-$同构$\sigma':E_1\to E_2$即$\sigma'|_F=\mathrm{id}_F$，即：**多项式的分裂域在$F-$同构下唯一**.

  【证明】我们先证明最关键也最困难的结论①.

  思路是逐步构造代数单扩张. 对扩张次数用数学归纳法.

  若$[E_1:F_1]=1$，则$\mathrm{Split}(f_1(x),F_1)=E_1=F_1$，于是$f_1(x)$在$F_1$上分裂，所以$f_1(x)$在$F_1$内分解为一次因式的乘积，不妨设$f_1(x)$是首一多项式，所以：

  $$f_1(x)=(x-\alpha_1)\cdots(x-\alpha_n)$$

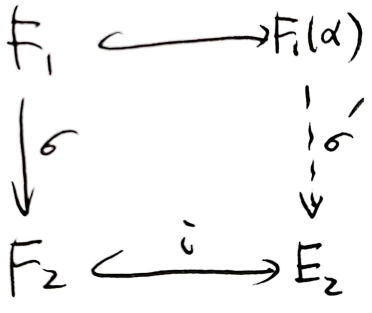
  用σ作用得到

  $$f_2(x)=(x-\sigma(\alpha_1))\cdots(x-\sigma(\alpha_n))$$

  所以$f_2(x)$在F_2上分裂，所以$E_2=\mathrm{Split}(f_2(x),F_2)=F_2$. 所以$E_1=F_1\cong F_2=E_2$. 此时$\sigma'=\sigma$. 显然满足条件的$\sigma'$只有一个.

  下面假设命题①和③对于$[E_1:F_1]\leq m-1$的情形都成立. 取考察$[E_1:F_1]=m$的情况. 不妨设$f_1(x)$，$f_2(x)$首一，因为$f_1(x)=(x-\alpha_1)\cdots(x-\alpha_n)$在$E_1[x]$中，而$E_1=F_1(\alpha_1,\cdots,\alpha_k)$. 因为$[E_1:F_1]>1$，所以$E_1\supsetneq F_1$，因此必然存在某个$\alpha_i$使得$\alpha_i\notin F_1$，适当调换顺序后不妨设是$\alpha_1\notin F_1$，则可以考虑$F_1(\alpha_1)$.因为$[E_1:F_1]$有限，所以$\alpha_1$在$F_1$上代数. 设$\alpha_1$在$F_1$上的最小多项式为$p(x)$，记$i:F_2\to E_2$是嵌入，则$i\circ\sigma$是$F_1\to E_2$为单同态，根据前面的技术性命题，对下面的交换图有如下两个集合的$1:1$对应：

  $$\{\sigma':F_1(\alpha_1)\to E_2\text{是}i\circ\sigma\text{的延拓}\}=\{i\circ\sigma(p(x))=\sigma(p(x))\text{在}E_2\text{中的根}\}$$



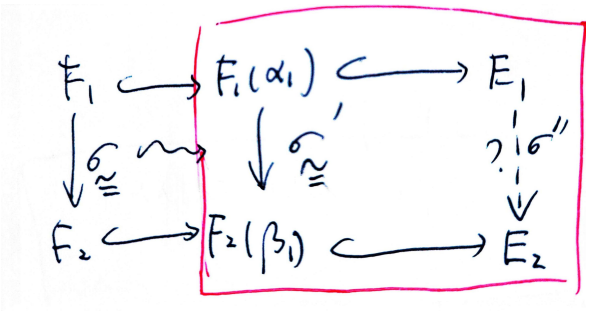
我们说明右边不是空集. 这是因为$f_1(\alpha_1)=0\Rightarrow p_1(x)\mid f_1(x)$在$F_1[x]$中，用$\sigma$作用可得$\sigma(p)(x)\mid f_2(x)$在$F_2[x]$中，而因为$f_2(x)$在$E_2$上分裂，所以$f_2(x)$在$E_2$上分解为一次因式的乘积，因为$\sigma(p)(x)$是非零多项式，所以$\sigma(p)(x)$作为$f_2(x)$的因子在$E_2$上也分解为一次因式的乘积，即$\sigma(p)(x)$在$E_2$中必有根，所以存在这样的$\sigma':F_1(\alpha)\to E_2$是$i\circ\sigma$的延拓. 而且集合的势$\leq \deg\sigma(p)(x)=\deg p(x)=[F_1(\alpha):F_1]$.

对每个σ'，记$\sigma'(\alpha_1)=\beta_1\in E_2$，因为$F_1(\alpha_1)$中元素形如$g_1(\alpha_1)$，$g_1\in F_1[x]$，所以$\sigma'(F_1(\alpha_1))$中元素形如$g_2(\beta_1)$，$g_2\in F_2[x]$. 因此$\sigma'(F_1(\alpha_1))\subseteq F_2(\beta_1)$，而$F_2(\beta_1)$是包含$\beta_1$和$F_2$的最小的$E_2$的子域，所以$\sigma'(\alpha_1)=F_2(\beta_1)$，从而由$\sigma'$给出了$F_1(\alpha_1)\to F_2(\beta_1)$的域同构. 注意$F_1(\alpha_1)\supsetneq F_1$，所以$[E_1:F_1(\alpha-1)]<m$. $F_1(\alpha_1)$是E_1/F_1的中间域$\Rightarrow E_1$是$f_1(x)$在$F_1(\alpha_1)$上的分裂域，同理E_2是$f_2(x)$在$F_2(\beta_1)$上的分裂域，对下图中右边这个框框可以使用归纳假设，于是存在$\sigma'':E_1\to E_2$是域同构，而且$\sigma''|_{F_1(\alpha_1)}=\sigma'$，而且满足这一条件的$\sigma''$的个数$\leq[E_1:F_1(\alpha)]$.

因为$\sigma'|_{F_1}=i\circ\sigma=\sigma$，所以$\sigma''|_{F_1}=\sigma$，因此这样的$\sigma''$是$\sigma$的延拓. 按照这样的构造方式得到的$\sigma''$的个数满足：

$$\#\sigma''\leq[E_1:F_1(\alpha)][F_1(\alpha):F_1]=[E_1:F_1].$$

另一方面，如果已经有了σ''是$E_1\to E_2$的域同构而且是σ的延拓，那么将σ''限制在$F_1(\alpha_1)$上将给出$F_1(\alpha_1)$到E_2的某个子域的域同构σ'，而由于这样的σ'在F_1上的限制也等于σ，所以是$i\circ\sigma$的延拓（当然也对应了某个$\beta_1:=\sigma'(\alpha_1)$是$\sigma(p)(x)$在$E_2$中的根），因此所有满足条件的$\sigma''$都可以通过上面的两步法找到，因此上面的方法构造出了所有的σ''.



这就证明了①和③，对于②，因为$\sigma':E_1\to E_2$是同构而且$\sigma'(F_1)=F_2$. 写下E_1作为F_1-线性空间的一组F_1基满足的等式并用σ'作用，根据$\sigma'(F_1)=F_2$可知σ'将E_1的一组F_1基映为E_2的一组F_2基，从而E_1作为F_1线性空间的维数等于E_2作为F_2线性空间的维数.□

- 【推论】设 $f(x)\in F[x]$，$\deg f\geq 1$, 设E 是$f(x)$在 F上的一个分裂域，并令

$$\mathrm{Aut}(E/F)=\{\sigma\in\mathrm{Aut}(E):\sigma|_F=\mathrm{id}\}$$

也就是E的$F-$自同构群，则 $\mathrm{Aut}(E/F)$ 在复合下是群（事实上是$\mathrm{Aut}(E)$的子群），且对于群阶数有估计 $|\mathrm{Aut}(E/F)|\leq[E:F]$.

【证明】在上面的定理中取$F_1=F_2=F$，$E_1=E_2=E=\mathrm{Split}(F,f)$. □

- 【例】计算$\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$. 这是$(x^2-2)(x^2-3)$在$\mathbb{Q}$上的分裂域.

【解】运用前面的思想，分部构造代数单扩张，分部构造延拓.

先延拓到$\mathbb{Q}(\sqrt{2})$，因为$\min(\sqrt{2},\mathbb{Q})=x^2-2$，在$\mathbb{Q}(\sqrt{2},\sqrt{3})$上的根有$\pm\sqrt{2}$，所以：

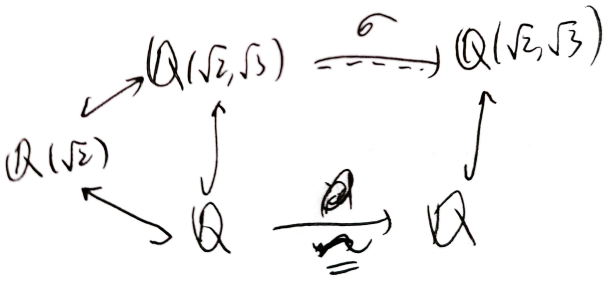
$$\sigma^{\pm}:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2},\sqrt{3}),\quad \sigma^{\pm}|_{\mathbb{Q}}=\mathrm{id}|_{\mathbb{Q}}.$$

$\sigma^+(\sqrt{2})=\sqrt{2}$，$\sigma^-(\sqrt{2})=-\sqrt{2}$.

再延拓到$\mathbb{Q}(\sqrt{2},\sqrt{3})$，$\min(\sqrt{3},\mathbb{Q}(\sqrt{2}))=\min(\sqrt{3},\mathbb{Q})=x^2-3$，$\sigma^{\pm}(x^2-3)=x^2-3$在$\mathbb{Q}(\sqrt{2},\sqrt{3})$上有根$\pm\sqrt{3}$，所以$\sigma^+$有两个延拓$\sigma^{++}$和$\sigma^{+-}$，$\sigma^-$有两个延拓$\sigma^{-+}$和$\sigma^{--}$. 于是：

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})=\{\sigma^{\pm\pm}\}.$$

写下具体公式，或者考虑在生成元处的取值容易看出它有3个2阶元，所以$\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})\cong K_4$.



□

- 【例】计算$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$. 这是$x^3-2$在$\mathbb{Q}$上的分裂域.

  【解】可以分步构造代数扩张，然后分布构造延拓.

  第一步，$\min(\sqrt[3]{2},\mathbb{Q})=x^3-2$，$x^3-2$在$\mathbb{Q}(\sqrt[3]{2},\omega)$中的根为$\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$. 这给出了三种$\mathbb{Q}$嵌入，$\sigma_{0,1,2}:\mathbb{Q}(\sqrt[3]{2})\to\mathbb{Q}(\sqrt[3]{2},\omega)$.

  第二步，$\min(\omega,\mathbb{Q}(\sqrt[3]{2}))=\min(\omega,\mathbb{Q})=x^2+x+1$，$\sigma_{0,1,2}(x^2+x+1)=x^2+x+1$，在$\mathbb{Q}(\sqrt[3]{2},\omega)$中的根为$\omega$和$\omega^2$，者给出$\sigma_i$的两个延拓$\sigma_{i0}$和$\sigma_{i1}$，$\sigma_{i0}(\omega)=\omega$，$\sigma_{i1}(\omega)=\omega^2$.

  事实上$\sigma\in\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$给出了$x^3-2$在其分裂域中的三个根$\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$的置换，即：

  $$x^3-2=\sigma\left(x^3-2\right)=(x-\sigma(\sqrt[3]{2}))(x-\sigma(\sqrt[3]{2}\omega))\left(x-\sigma\left(\sqrt[3]{2}\omega^2\right)\right)$$

  所以

  $$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})=\{\sigma_{ij}:\quad i=0,1,2,\quad j=0,1\}\cong S_3.$$

- 【例】$f(x)=x^4+2$和$g(x)=x^4-2$，作为$\mathbb{Q}$系数多项式在$\mathbb{Q}$上的分裂域相等（作为$\mathbb{C}$的子域），都等于$\mathbb{Q}(\sqrt[4]{2},i)$，此时$\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})\cong D_4$.

- 【Galois扩张】若E是域F上某个“可分多项式”的分裂域，则E/F是一个Galois扩张.

  【例】例如，特征为0的域上所有的多项式都可分，所以上面计算的几个例子都是Galois扩张. 但是$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$不是个Galois扩张，因为$x^3-2$在其上不分裂.

- 【Galois群】E/F是Galois扩张，令：

  $$\mathrm{Gal}(E/F)=\{\sigma\in\mathrm{Aut}_{\text{field}}(E),\quad \sigma|_F=\mathrm{id}_F\}.$$

  则$\mathrm{Gal}(E/F)=\mathrm{Aut}(E/F)$在复合下为群，称为Galois扩张$E/F$的Galois群，若$f(x)$是$F$上可分多项式，$E$是$F$的分裂域，则称为$\mathrm{Gal}_F(f(x)):=\mathrm{Gal}(E/F)$是多项式$f(x)$在$F$上的Galois群.

- 【例】$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})=\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})\cong S_3$

  $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})=\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})\cong D_4$.