第十二周作业参考解答及补充

作业

1. (习题 3.4.1)

设 $p>2$ 是素数, $\alpha\in\mathbb{C}$ 是 $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1\in\mathbb{Q}[x]$ 的根. 证明: 域 $L=\mathbb{Q}[\alpha]$ 的自同构群 G 是一个 $p-1$ 阶的循环群.

proof

由 3.1.5 和 3.1.6, $f(x)$ 的所有根构成循环群, α 是生成元, 因此按定义 $\mathbb{Q}[\alpha]$ 是 $f(x)$ 的分裂域, 由 3.3.14 的注记, 这是一个 Galois 扩张. $|\mathrm{Gal}(L/\mathbb{Q})|=p-1$, 而 $\alpha\mapsto\alpha^i, 1\leqslant i\leqslant p-1$ 恰好为 $p-1$ 个 $L/\mathbb{Q}$ 的自同构. 从而 $\mathrm{Gal}(L/\mathbb{Q})=\mathbb{F}_p^*\cong\mathbb{Z}/(p-1)\mathbb{Z}$. □

注:

用到了结论: 当 p 是素数时, $(\mathbb{Z}/p\mathbb{Z})^*\cong\mathbb{Z}/(p-1)\mathbb{Z}$. 证明这个结论需要一个命题.

命题 设 G 是 Abel 群, 若 $g\in G$ 有最大的有限阶, 则 $\forall h\in G, |h|<\infty\implies |h|\Big||g|$.

这个需要对阶进行一些分析. 按阶的定义可以得到一个常用的等式是 $|g^n|=\dfrac{|g|}{(n,|g|)}=\dfrac{[n,|g|]}{n}$, 这里 $[a,b]$ 表示两个正整数的最小公倍数. 根据这个等式可以得到, 若 $gh=hg$ 且 $(|g|,|h|)=1$, 则 $|gh|=|g|\cdot|h|$. 下面用反证发证明这个命题.

假设 $|h|\nmid|g|$, 考虑他们的素因子分解, 那么将存在某个素数 p 使得 $|g|=p^mr, |h|=p^ns, (p,r)=(p,s)=1, m<n$. 此时我们计算 $g^{p^m}h^s$ 的阶

$$
\begin{aligned}
|g^{p^m}|&=\frac{|g|}{(p^m,|g|)}=r,\\
|h^s|&=\frac{|h|}{(s,|h|)}=p^n,\\
(p^n,r)=1&\implies |g^{p^m}h^s|=|g^{p^m}||h^s|=p^nr>|g|
\end{aligned}
$$

从而和 g 有最大有限阶矛盾. (这个证明的技巧性还是挺强的, 以上都在教材 4.3 节)

有了这个命题, 由于 $(\mathbb{Z}/p\mathbb{Z})^*$ 是有限群, 从而存在这样的 g 有最大的有限阶, 我们证明 $|g|=p-1$ 即可. 一方面根据 Fermat 小定理 $g^{p-1}=1$, 因此 $|g|\leqslant p-1$; 另一方面, 任意的 $h\in(\mathbb{Z}/p\mathbb{Z})^*$ 都有 $|h|\Big||g|$, 因此 $h^{|g|}=1$, 也就是说多项式 $x^|g|-1$ 在 $\mathbb{F}_p$ 上有 $p-1$ 个根, 那么 $|g|\geqslant p-1$. 从而只能是 $|g|=p-1$.

2. (习题 3.4.2)

设 $K=\mathbb{Q}$, $L=K[\sqrt[3]{2}]$. 证明: $G=\mathrm{Gal}(L/K)=\{1\}$ (所以 $L^G=L\neq K$). 如果令 $\overline{L}=K[\sqrt[3]{2},\sqrt{-3}]$, 试证明: $\mathrm{Gal}(\overline{L}/K)\cong S_3$. 并求出中间域 $K\subseteq K[\sqrt{-3}]\subseteq\overline{L}$ 对应的子群 $H\subseteq\mathrm{Gal}(\overline{L}/K)$, 即: 求 $H\subseteq\mathrm{Gal}(\overline{L}/K)$ 使得 $\overline{L}^H=K[\sqrt{-3}]$. (提示: $H=\mathrm{Gal}(\overline{L}/K[\sqrt{-3}])\cong A_3$.)

proof

该题的后半部分已在上课时讲过.

由 3.3.2, $\sqrt[3]{2}$ 的极小多项式是 x^3-2, 且三个根中只有 $\sqrt[3]{2}\in L$, 根据 3.3.6, 若 $\sigma\in\mathrm{Gal}(L/K)$, 则 $\sigma(\sqrt[3]{2})\in L$ 也是 x^3-2 的根, 那么只能是 $\sigma(\sqrt[3]{2})=\sqrt[3]{2}$, 从而 $\sigma=\mathrm{id}_L$.

类似 3.1.14, 3.3.4, 同样的分析 degree 的操作可以得到 $[\overline{L}:K]=3\cdot 2=6$. 注意到 $\zeta_3=e^{\frac{2\pi i}{3}}=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$, 因此 $\overline{L}=K[\sqrt[3]{2},\sqrt{-3}]=K[\sqrt[3]{2},\zeta_3]$, 正好是 x^3-2 的分裂域. 由 3.3.14 的注记, $\overline{L}/K$ 是 Galois 扩张. 此时 $\eta\in\mathrm{Gal}(\overline{L}/K)$, 对两个中间域 $K[\sqrt[3]{2}]$ 和 $K[\zeta_3]$ 分别考虑 3.3.6, $\eta(\sqrt[3]{2})=\sqrt[3]{2}\zeta_3^i, i=0,1,2$, $\eta(\zeta)=\zeta^j, j=1,2$. 那么记

$$\alpha: L\to L,\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\zeta_3,\zeta_3\mapsto\zeta_3,\ \beta: L\to L,\ \sqrt[3]{2}\mapsto\sqrt[3]{2},\ \zeta_3\mapsto\zeta_3^2$$

根据 1.3.5 可以验证 α,β 正是生成元, $\mathrm{Gal}(\overline{L}/K)\cong S_3$. 而中间域 $K[\sqrt{-3}]=K[\zeta_3]$, 根据 Galois 对应 (教材定理 3.4.2, 定理 4.4.1), $H=\mathrm{Gal}(\overline{L}/K[\zeta_3]), \overline{L}^H=K[\zeta_3]$. 那么 $|[G:H]|=[K[\zeta_3]:K]=2$, $G/H=\mathbb{Z}/2\mathbb{Z}$; $|H|=[\overline{L}:K[\zeta]]=3$, $H=A_3$. □

注:

阶数 3 以下的群是唯一的, 直接分析乘法表就行, 4 阶群有两种 (4.2.7).