MA3D5 Galois Theory
Sheet 7 Solutions

Peize Liu

20 Nov 2024

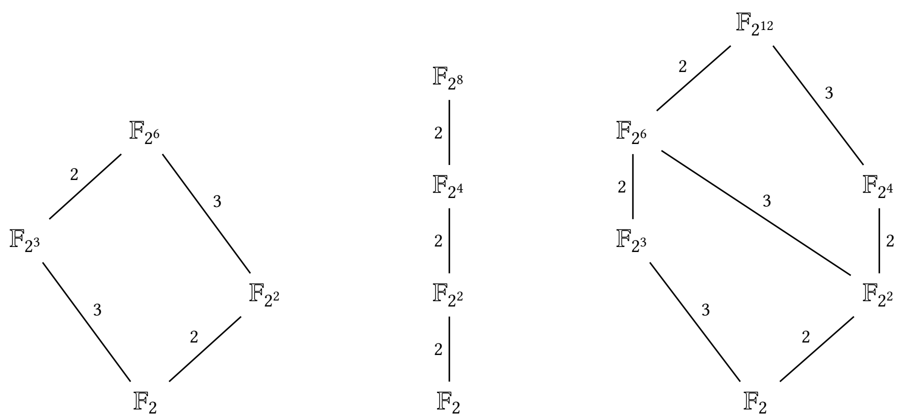
Exercise 7.1

Compute the subfield lattice of $\mathbb{F}_{2^6}$. Do the same for $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^{12}}$.

We claim that for each divisor k of n, there exists a unique subfield of $\mathbb{F}_{2^n}$ of order 2^k. $\mathbb{F}_{2^n}$ contains $\mathbb{F}_2$ as a prime subfield and $[\mathbb{F}_{2^n} : \mathbb{F}_2] = n$. Since $\mathbb{F}_{2^n}$ is the splitting field of the separable polynomial $x^{2^n} - x$ over $\mathbb{F}_2$ (as shown in Question B.1 and B.2 of Sheet 6), $\mathbb{F}_{2^n}/\mathbb{F}_2$ is a Galois extension, and hence $|\operatorname{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)| = n$. We claim that $\operatorname{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$ is isomorphic to the cyclic group $\mathbb{Z}/n$.

Since $\mathbb{F}_{2^n}$ is a finite field of characteristic 2, the Frobenius map $\varphi : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, $\alpha \longmapsto \alpha^2$, is an $\mathbb{F}_2$-automorphism. The fact that $\mathbb{F}_{2^n}$ is the set of roots of $x^{2^n} - x$ implies $\alpha^{2^n} = \alpha$ for all $\alpha \in \mathbb{F}_{2^n}$. So $\varphi^n = \mathrm{id}$. There does not exists $k < n$ such that $\varphi^k = \mathrm{id}$, for otherwise the polynomial $x^{p^k} - x$ has p^n distinct roots. Hence φ has order n in $\operatorname{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$. This proves that claim.

For each divisor k of n, there exists a unique subgroup H of $\operatorname{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2) \cong \mathbb{Z}/n$ of order k. By Galois correspondence, the fixed field $\mathbb{F}_{2^n}^H \subseteq \mathbb{F}_{2^n}$ has degree $[\mathbb{F}_{2^n}^H : \mathbb{F}_2] = k$ over $\mathbb{F}_2$. Hence $\mathbb{F}_{2^n}^H \cong \mathbb{F}_{2^k}$. This is enough to determine the subfield lattices:



Exercise 7.2

Let p be a prime and F be a field of characteristic $p > 0$.

Let $q = p^n$ for some $n \in \mathbb{N}$. Show that the set of elements of F that satisfy $x^q = x$ form a subfield of F.

Show that the set of points of F that satisfy $x^p = x$ are exactly the prime subfield $\mathbb{F}_p \subseteq F$.

Let $K := \left\{\alpha \in L \mid \alpha^{16} = \alpha\right\}$. We claim that K is a subfield of L. It is clear that $\alpha\beta^{-1} \in K$ for $\alpha \in K$ and $\beta \in K^\times$, so K is closed under multiplication and multiplicative inverse. For $\alpha, \beta \in K$, we have

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} + \sum_{i=1}^{p^n-1} \binom{p^n}{i} \alpha^i \beta^{p^n-i}.$$

We claim that $p^n \mid \binom{p^n}{i}$ for $1 \leqslant i \leqslant p^n - 1$. Since p is prime, $\gcd(p^n, i) = p^k$ for some $k < n$. By Bezóut's lemma, there exists $a, b \in \mathbb{Z}$ such that $p^k = ap^n + bi$. Then

$$\frac{1}{p}\binom{p^n}{i} = p^{n-k-1}\frac{p^k}{p^n}\binom{p^n}{i} = p^{n-k-1}\frac{ap^n + bi}{p^n}\binom{p^n}{i} = ap^{n-k-1}\binom{p^n}{i} + bp^{n-k-1}\binom{p^n - 1}{i - 1} \in \mathbb{Z}.$$

IUn particular $\binom{p^n}{i} = 0$ in any field with characteristic p. Hence $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$. The set K preserves addition.

For $\alpha \in K$, if $p = 2$, then $-\alpha = \alpha \in K$; if $p > 2$ is an odd prime, then $(-\alpha)^{p^n} = -\alpha^{p^n} = -\alpha$, and thus $\alpha \in K$. So K is closed under additive inverse. We conclude that K is a subfield of F.

The prime subfield $\mathbb{F}_p$ has multiplicative group $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)$. Hence $\alpha^{p-1} = 1$ for any $\alpha \in \mathbb{F}_p^\times$ (i.e. Fermat's little theorem). It follows that $\alpha^p = \alpha$ for all $\alpha \in \mathbb{F}_p$. Hence all elements in $\mathbb{F}_p$ are roots of $x^p - x$. But $x^p - x$ has at most p roots. We conclude that its set of roots is exactly $\mathbb{F}_p$.

Exercise 7.3

Let p be a prime. Prove that S_p is generated by a single transposition together with any p-cycle.

Prove that any subgroup $H \subseteq S_p$ that has order $\#H$ divisible by p must contain a p-cycle.

Consider a transposition $\tau \in S_p$ and a p-cycle $\sigma \in S_p$. Without loss of generality, let $\sigma = (1\ 2\ \cdots\ p)$ and $\tau = (i\ j)$, where $1 \leqslant i < j \leqslant p$. Note that $\sigma^{j-i}(i) = i + (j - i) = j$. Since p is prime, σ^{j-i} is also a p-cycle. Consider the relabelling $\rho : S_n \longrightarrow S_n$ such that $\rho(i) = 1$ and $\rho(j) = 2$, and $\rho \circ \sigma^{j-i} \circ \rho^{-1}(k) = k + 1$ for all $k \in \{1, ..., n\}$. Then after relabelling we may assume that $G = \langle \sigma', \tau' \rangle$ where $\sigma' = \rho\sigma^{j-i}\rho^{-1} = (1\ 2\ \cdots\ p)$ and $\tau'\rho\tau\rho^{-1} = (1\ 2)$.

We shall prove that $G = S_p$. First we note that

$$(k\ k+1) = (1\ 2\ \cdots\ p)^{-k+1}(1\ 2)(1\ 2\ \cdots\ p)^{k-1} \in G,$$

for any k. Second, if $(1\ k) \in G$, then

$$(1\ k+1) = (1\ k)(k\ k+1)(1\ k) \in G.$$

Hence by induction $(1\ k) \in G$ for any k. Then for any k, ℓ,

$$(k\ \ell) = (1\ k)(1\ \ell)(1\ k) \in G.$$

In particular G contains all transpositions. It is clear that S_p is generated by transpositions. So $G = S_p$.

Suppose that $H \leqslant S_p$ has order $|H|$ divisible by p. By Cauchy's theorem, any finite group whose order divisible by a prime p has an element of order p. So H has an element σ of order p. By the cycle type decomposition, σ is the composition of some disjoint cycles, and the order of σ is the least common multiple of the length of these cycles. Since $\sigma \in S_p$ and p is prime, σ must be a p-cycle.