

Finite Fields

Recall: If F is a field, F contains a prime field $F_0 \subseteq F$ and $F_0 \cong \mathbb{Q}$ or $F_0 \cong \mathbb{F}_p$ for some p .

Lemma: If F is a finite field, then F is a finite extension of \mathbb{F}_p . If $[F : \mathbb{F}_p] = n$, then $|F| = p^n$.

Theorem: If F is a finite field, $F^\times = (F \setminus \{0\}, \cdot)$ is cyclic.

Proof: F^\times is a finite abelian group, so by the Fundamental Theorem of Finitely Generated Abelian Groups

$F^\times \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ for some integers $m_1 | m_2 | \cdots | m_k$, so $x^{m_k} - 1 = 0$ for all $x \in F^\times$. However, $x^{m_k} - 1 = 0$ has at most m_k roots in F , so

$|F| = m_1 m_2 \cdots m_k \leq m_k$, so $k=1$ and $F^\times \cong \mathbb{Z}_m$.

Corollary: If F is a finite field, $F = \mathbb{F}_p(\alpha)$ for some $\alpha \in F$.

Observation: If F is a finite field of characteristic p ,

then $x \mapsto x^p$ is an automorphism of F (because $(x+y)^p = x^p + y^p$ in characteristic p). What is fixed by this?

We have $a^p = a$ for any $a \in \mathbb{F}_p$ and $x^p - x$ has at most p roots in F , so the fixed field is \mathbb{F}_p so

$\{x \mapsto x^p\} \in \text{Aut}_{\mathbb{F}_p}(F)$.

Proposition: F is a finite field with p^n elements if and only if F is the splitting field of $x^{p^n} - x$ over \mathbb{F}_p .

Proof: Assume $|F| = p^n$, i.e. $[F : \mathbb{F}_p] = n$. Then $|F^\times| = p^n - 1$

so $\alpha^{p^n-1} - 1 = 0$ for any $\alpha \in F^\times$, so $\alpha^{p^n} - \alpha = 0$ for any $\alpha \in F$. In particular, F contains all roots of $x^{p^n} - x$ over \mathbb{F}_p , so F contains a splitting field of $x^{p^n} - x = 0$, but all elements are roots, so F is a splitting field.

Conversely, if F is a splitting field of $x^{p^n} - x$, note $(x^{p^n} - x)' = -1$ so this polynomial has no repeated roots.

So f has p^n distinct roots in F . The fixed field of $x \mapsto x^p$ is some subfield of F . But F is generated by the roots of $x^{p^n} - x = 0$, so F is this fixed field.

$F = \{\text{roots of } x^{p^n} - x\}$ which contains p^n roots.

Corollary: If F_1 and F_2 are finite fields and $|F_1| = |F_2|$, then $F_1 \cong F_2$.

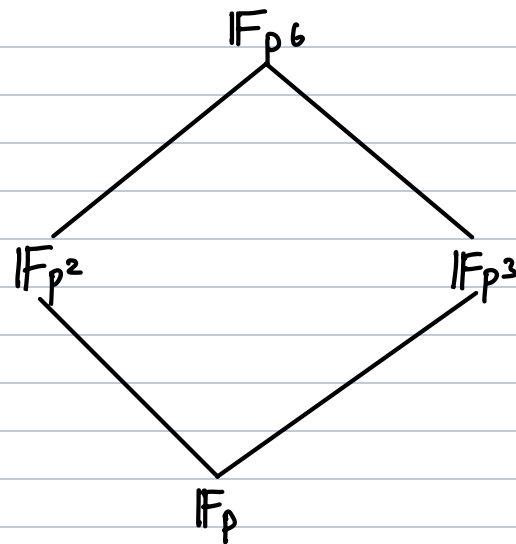
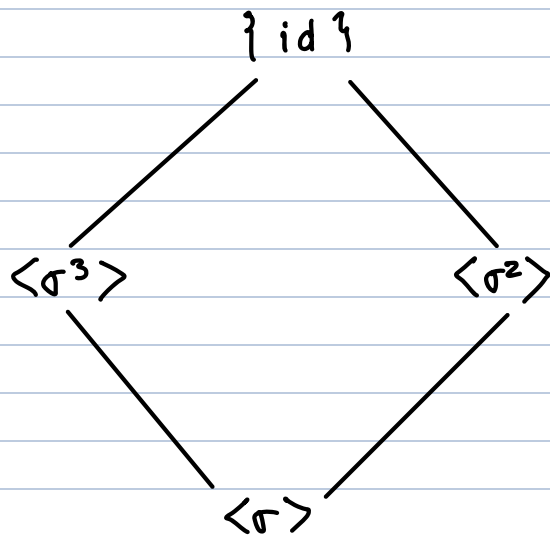
Proposition: If F is a finite field, then F is a cyclic Galois extension of \mathbb{F}_p , i.e. $\text{Gal}(F/\mathbb{F}_p)$ is cyclic.

Proof: F is a splitting field of $x^{p^n} - x$, which is separable, so F/\mathbb{F}_p is Galois.

Let $\sigma(x) = x^p$, $\sigma \in \text{Gal}(F/\mathbb{F}_p)$. Observe that $\sigma^n(x) = x^{p^n} = x$ for all $x \in F$. So $\sigma^n = \text{id}$. On the other hand, for $j < n$, $\sigma^j(x) = x$ has at most p^j roots, so σ^j does not fix F , so σ has order n , but $|\text{Gal}(F/\mathbb{F}_p)| = [F:\mathbb{F}_p] = n$, so $\text{Gal}(F/\mathbb{F}_p) = \langle \sigma \rangle \cong \mathbb{Z}_n$.

The subgroups of $\text{Gal}(F/\mathbb{F}_p)$ are $\langle \sigma^d \rangle$ where $d|n$, so the corresponding intermediate fields of size p^d where $d|n$.

Example: If $n=6$. Then



Cyclic Extensions

All finite extension fields of finite fields are cyclic. In general, call a Galois extension **cyclic** if $\text{Gal}(F/K)$ is cyclic.

Example: Let ζ be a primitive n th root of unity and let $x^n - a$ be irreducible over $K = \mathbb{Q}(\zeta)$. Let α be a root and $F = K(\alpha)$. Over F ,

$$x^n - a = (x - \alpha)(x - \zeta\alpha) \cdots (x - \zeta^{n-1}\alpha) \in F[x]$$

so F is a splitting field of $x^n - a$ over K . Because $[F:K] = n$ as $x^n - a$ is irreducible over K and $|\text{Gal}(F/K)| = n$ for every root $\zeta^j \alpha$ of $x^n - a$, there is a $\sigma_j \in \text{Gal}(F/K)$ with $\sigma_j(\alpha) = \zeta^j \alpha$, so $\text{Gal}(F/K) = \{\sigma_0, \dots, \sigma_{n-1}\}$. Observe that

$$\sigma_j \sigma_k(\alpha) = \sigma_j(Z^k \alpha) = Z^k \sigma_j(\alpha) = Z^k Z^j \alpha = Z^{j+k} \alpha = \sigma_{j+k}(\alpha).$$

In particular, $\text{Gal}(F/K) \cong \mathbb{Z}_n$ $j \mapsto \sigma_j(\alpha)$. Thus F/K is a cyclic extension.

Proposition: Let F/K be a cyclic extension of degree n of fields of characteristic p . Then there are intermediate subfields $F \supseteq E_0 \supseteq E_1 \supseteq \dots \supseteq E_e = K$ such that

F is a cyclic extension of E_0 of degree m with $p \nmid m$ and E_k is a cyclic extension of E_{k+1} of degree p so $n = p^e m$.

Proof: The lattice of subgroups of a cyclic group for example $\text{Gal}(F/K)$ has a subgroup of order m , and its fixed field E_0 of F as a degree m extension. E_0 is a cyclic extension of K of degree p^e . Proceed inductively.

Note: Just understand cyclic extensions of degree p or degree prime to p , in char p .

Definition: Let F be a finite separable extension of K , and let \bar{K} be some algebraic closure K (or just algebraically closed extension). Let $\sigma_1, \dots, \sigma_r$ be the distinct embeddings of F into \bar{K} which fixes K . Define

$$\bullet N_{F/K}(\alpha) = \prod_{i=1}^r \sigma_i(\alpha) \quad \text{the norm of } \alpha$$

$$\bullet \text{Tr}_{F/K}(\alpha) = \sum_{i=1}^r \sigma_i(\alpha) \quad \text{the trace of } \alpha$$

Example: $K = \mathbb{R}$, $F = \mathbb{C}$, $\bar{K} = F$, $\sigma_1 = \text{id}$, $\sigma_2(x+iy) = x-iy$.

$$\bullet N_{\mathbb{C}/\mathbb{R}}(x+iy) = (x+iy)(x-iy) = x^2 + y^2$$

$$\bullet \text{Tr}_{\mathbb{C}/\mathbb{R}}(x+iy) = (x+iy) + (x-iy) = 2x$$

Note: If F/K is Galois, then F is a stable subfield of \bar{K} , so $\sigma: F \rightarrow \bar{K}$ is an embedding fixing K , then $\sigma(F) = F$
 $\Rightarrow \sigma \in \text{Aut}_K(F) = \text{Gal}(F/K)$, so

$$\bullet N_{F/K}(\alpha) = \prod_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha)$$

$$\bullet \text{Tr}_{F/K}(\alpha) = \sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha)$$

Note: If $\tau \in \text{Gal}(F/K)$, $\tau(\text{Tr}_{F/K}(\alpha)) = \tau\left(\sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha)\right)$

$$= \sum_{\sigma \in \text{Gal}(F/K)} \tau\sigma(\alpha) = \sum_{\tau\sigma \in \text{Gal}(F/K)} \sigma(\alpha) = \text{Tr}_{F/K}(\alpha)$$

$\Rightarrow \text{Tr}_{F/K} \in K$ and similar for $N_{F/K}$.