22. Finite fields II

22.1. **Main structure theorems.** Recall that F is a field of characteristic $p > 0$, then the subfield of F generated by 1 (also called the prime subfield of F) is isomorphic to $\mathbb{F}_p$, so F is an extension of $\mathbb{F}_p$.

The following results have been proved in Algebra-I:

(A) If F is a finite field of characteristic p, then $|F| = p^n$ for some n and $F \cong \mathbb{F}_p[x]/(f(x))$, where $f(x) \in F[x]$ is an irreducible polynomial of degree n, which can be chosen monic.

(B) Conversely, if $f(x) \in F[x]$ is irreducible of degree n, then $\mathbb{F}_p[x]/(f(x))$ is a finite field of order p^n.

We proved that for any $n \geq 1$ a field of order p^n exists, but we did not prove uniqueness. We will now give a very short proof of both existence and uniqueness using basic field theory.

Theorem 22.1. *Let p be a prime and $\overline{\mathbb{F}}_p$ a fixed algebraic closure of $\mathbb{F}_p$. For each $n \in \mathbb{N}$ let $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}}_p : x^{p^n} = x\}$. Then F_{p^n} is the unique subfield of $\overline{\mathbb{F}}_p$ of order p^n.*

Remark: If F is any field of order p^n, then the extension $F/\mathbb{F}_p$ is finite (hence algebraic), whence F embeds in $\overline{\mathbb{F}}_p$. Thus, Theorem 22.1 implies that there exists a unique up to isomorphism field of order p^n.

Proof. Step 1: Why is $\mathbb{F}_{p^n}$ a subfield? This is because the map $x \mapsto x^{p^n}$ is a ring homomorphism in any field of characterstic p, and $\operatorname{char} \overline{\mathbb{F}}_p = p$ since characteristic does not change under field extensions.

Step 2: Why is $|\mathbb{F}_{p^n}| = p^n$? The polynomial $\Phi_n(x) = x^{p^n} - x$ is separable since $\Phi_n'(x) = -1$, so $gcd(\Phi_n, \Phi_n') = 1$. Therefore, $\Phi_n(x)$ has $p^n = \deg \Phi_n$ distinct roots in $\overline{\mathbb{F}}_p$.

Step 3: Why unique? If F is any subfield of $\overline{\mathbb{F}}_p$ with $|F| = p^n$, then $|F^*| = p^n - 1$. By Lagrange $x^{p^n-1} = 1$ for any $x \in F^*$, whence $x^{p^n} = x$ for all $x \in F$. Thus $F \subseteq \mathbb{F}_{p^n}$, and so $F = \mathbb{F}_{p^n}$ (as $|F| = |\mathbb{F}_{p^n}| = p^n$). □

The next question is when $\mathbb{F}_{p^m}$ contained in $\mathbb{F}_{p^n}$.

Proposition 22.2. $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ *if and only if* $m \mid n$.

Proof. "⇒" Suppose $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Then $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^m}$ of dimension $d < \infty$. Hence $|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d$, so $p^n = p^{md}$ and $n = md$.

"$\Leftarrow$" If $n = dm$, then any solution of $x^{p^m} = x$ is also a solution of $x^{p^n} = x$. Indeed,

$$x^{p^m} = x \quad \Rightarrow \quad x^{p^{2m}} = (x^{p^m})^{p^m} = x^{p^m} = x \quad \text{etc.}$$

Thus, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. $\square$

Corollary 22.3. *A finite field of order p^n contains a unique subfield of order p^m for each $m \mid n$ and no other subfields.*

Next we will show that if K/F is an extension of finite fields, then K/F is always Galois and its Galois group is cyclic.

Definition. Let K be a field of characteristic $p > 0$. The map $Fr : K \to K$ given by $Fr(x) = x^p$ is called the Frobenius map of K.

The Frobenius map Fr is always an endomorphism of K (since $\operatorname{char} K = p$). Thus, Fr is an automorphism of K if and only if it is surjective (that is, K is perfect); in particular, this happens if K is finite.

Theorem 22.4. *Let K/F be an extension of finite fields. Then K/F is always Galois and $\operatorname{Aut}(K/F)$ is cyclic, generated by Fr^d, where $d = \log_p |F|$.*

Proof. Let $n = [K : F]$, so that $|K| = p^{nd}$. WOLOG we can assume that $F = \mathbb{F}_{p^d}$ and $K = \mathbb{F}_{p^{nd}}$ (defined as subfields of $\overline{\mathbb{F}}_p$).

Note that $Fr(L) \subseteq L$ for every subfield L of $\overline{\mathbb{F}}_p$, and by definition $\mathbb{F}_{p^m}$ is the fixed field of Fr^m for each $m \in \mathbb{N}$.

Thus, Fr^d is an element of $\operatorname{Aut}(K)$ which acts trivially on F, so $Fr^d \in \operatorname{Aut}(K/F)$. Moreover, Fr^m acts trivially on $K \iff nd \mid m$, so Fr^d has order n as an element of $\operatorname{Aut}(K/F)$.

So, $\langle Fr^d \rangle$ is a cyclic subgroup of $\operatorname{Aut}(K/F)$ of order $n = [K : F]$. By Theorem 19.1 this implies that K/F is Galois and $\operatorname{Aut}(K/F) = \langle Fr^d \rangle$. $\square$

22.2. **A few words about the Galois group $\operatorname{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.** We start with a warning that for a field K of positive characteristic the extension $\overline{K}/K$ is not Galois in general (normality is not a problem, but separability need not hold). However, this problem does not occur if K is perfect (in particular, if K is finite) by Theorem 18.1.

In view of Theorem 22.4, a naive guess would be that the Galois group $\operatorname{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}$ and is generated by the Frobenius map Fr. However, it turns out that $\operatorname{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is much larger – it is isomorphic to $\widehat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$; in particular, it is uncountable, as is the Galois group of any infinite Galois extension.

Moreover, Galois groups of infinite Galois extensions come with natural topology, called Krull topology, and in the case of $\overline{\mathbb{F}}_p/\mathbb{F}_p$ the subgroup $\langle Fr \rangle$

is an infinite cyclic subgroup of $\mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ which is dense in Krull topology. We will prove these facts in a couple of weeks.

At this point let us give a simple direct proof of uncountability of $\mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. For each $n \in \mathbb{N}$ let $F_n = \mathbb{F}_{p^{n!}}$. Then we get an ascending union of fields

$$F_1 \subseteq F_2 \subseteq \ldots \text{ and } \cup F_n = \overline{\mathbb{F}}_p.$$

Now note that if we are given a sequence $\{\varphi_n\}_{n=1}^{\infty}$ where

$$\varphi_n \in \mathrm{Aut}(F_n/\mathbb{F}_p) \text{ and } \varphi_{n+1|F_n} = \varphi_n \qquad (***)$$

then there exists $\varphi \in \mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ such that $\varphi_{|F_n} = \varphi_n$ for each n.

We can construct plenty of such sequences as follows. Choose any sequence of integers $d_1, d_2, \ldots$, define $a_1 = d_1$ and $a_n = a_{n-1} + d_{n-1} \cdot n!$ for $n \geq 1$, and let $\varphi_n = Fr^{a_n}$. Since $Fr^{d_{n-1} \cdot n!}$ acts trivially on F_n, each such sequence $\{\varphi_n\}$ satisfies compatibility condition (***) and thus defines some element $\varphi \in \mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

Clearly, there are uncountably many possible sequences $\{d_n\}$. While distinct sequences may yield the same element of $\mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, one can show that uncountably many distinct elements of $\mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ can be constructed in this way. The latter is left as a homework problem.