Finite Fields

[Parts from Chapter 16. Also applications of FTGT]

Lemma [Ch 16, 4.6] *Assume F is a finite field. Then the multiplicative group $F^* := F \setminus \{0\}$ is cyclic.*

Proof Recall from basic group theory (?)

• If G is a finite abelian group and $a, b \in G$ of orders m, n then there is some element $c \in G$ whose order is $lcm(m, n)$ (some c of the form $a^r b^s$).

Usng this repeatedly, we get that F^* has an element α of order r which is the lcm of the orders of all elements. Then $b^r = 1$ for all $0 \neq b \in F$.

All $b \neq 0$ are roots of $x^r - 1$. So $|F^*| \leq r$.

But $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$ are pairwise distinct and hence $|F^*| \geq r$ and then $|F^*| = r$ and $F^* = \langle \alpha \rangle$. $\square$

Corollary [Ch 16, 4.7] Let $E \subset F$ be an extension where E is a finite field. Then $E = F(\alpha)$ for some $\alpha \in E$.

Take $\alpha =$ as above, then $E = \langle \alpha \rangle \cup \{0\}$ and this is equal to $F(\alpha)$.

Let F be a field, then the intersection of all subfields of F is a subfield which has no proper subfields. This is called the *prime field* of F.

Lemma [Ch 16, 4.1] *The prime field of F is either isomorphic to $\mathbb{Q}$ or is isomorphic to $\mathbb{Z}_p$. In the first case say F has characteristic 0, and in the second case it has characteristic p*

[Idea of proof] Let $f : \mathbb{Z} \to F$ be the map $f(n) = n1_F$. Check that this is a ring homomorphism. So the kernel is an ideal and the image is a subring of a field, and hence has no zero divisors.

CASE 1 $\ker(f) = \{0\}$. Then f embeds $\mathbb{Z}$ into F, and this extends to an embedding of $\mathbb{Q}$ into F in the obvious way. This cannot have proper subfields (any subfield contains 1 and the the image of f and all the inverses of these) So it is the prime field.

CASE 2 If the kernel is non-zero then it must be $m\mathbb{Z}$ and the image of f is isomorphic to $\mathbb{Z}_m$. It has no zero divisors, so $m = p$ prime.

EXAMPLES If $F \subseteq \mathbb{C}$ then the prime field is $\mathbb{Q}$. If F is a finite field then the characteristic must be some p, and then $|F| = p^n$ for some $n \geq 1$.

Lemma [4.0] *Assume F has characteristic p.*
(a) The map $\sigma : F \to F$, $\sigma(x) = x^p$, is a homomorphism (an embedding).
(b) If F is finite then σ is also onto, hence an isomorphism.

Proof (a) We have $(ab)^p = a^p b^p$, and by the binomial expansion

$$(a+b)^p = a^p + b^p$$

since the binomial coefficients $\binom{p}{k}$ for $1 \leq k \leq p-1$ are zero in F. And $1^p = 1$. So σ is a homomorphism. It is not the zero map and therefore must be 1-1.

(b) a 1-1 map from a finite set to itself is automatically also onto.

Proposition [cf Ch 16, 5.1(b)] *Assume $E \supset F$ is an algebraic extension where F is finite. Then E is separable over F.*

Proof Let $a \in E$ and $f(x) \in F[x]$ the minimal polynomial of a. We must show that $f(x)$ does not have multiple roots. Assume (for contradiction) it has multiple roots, then $f'(x) = 0$. So any coefficient a_j with j not a multiple of p is zero. So

$$f(x) = a_0 + a_p x^p + \ldots + a_{jp} x^{jp} + \ldots x^{pm}$$

By Lemma 4.0(b) every element in F is a p-th root. So we can write $a_{jp} = b_j^p$ for some $b_j \in F$. Then

$$f(x) = \sum_j b_j^p (x^j)^p = (\sum_j b_j x^j)^p$$

Therefore $f(x)$ is not irreducible, a contradiction.

Theorem 4.3 (Ch 16) *Let F be a field with $|F| = p^n$ for p prime. Then F is the SF of the polynomial*

$$f(x) = x^{p^n} - x \in \mathbb{Z}_p[x].$$

Hence any two finite fields of the same size are isomorphic. Furthermore, $f(x)$ does not have multiple roots.

Proof The multiplicative group $F^* = F \setminus \{0\}$ has order $p^n - 1$. So if $0 \neq a \in F$ then $a^{p^n - 1} = 1$ (by Lagrange's Theorem). Therefore $a^{p^n} = a$ and a is a root of $f(x)$. Also 0 is a root. So all elements of F are roots. The degree is p^n, so these are precisely the roots.

This shows that F is a splitting field of $f(x)$. More generally, any two splitting fields are isomorphic, so any two fields of size p^n must be isomorphic.

As well we see that $f(x)$ cannot have multiple roots.

Corollary 4.4 *The set of roots of $x^{p^n} - x$ over characteristic p is a field.*

Galois groups for finite fields

Let E be a finite field. Then it has size p^n for p a prime, and contains $\mathbb{Z}_p$ (the subfield generated by 1).

Notation: $E = GF(p^n)$ (unique field of this size).

- E is a Galois extension of $\mathbb{Z}_p$: separable, see 5.1(b) of Ch. 16.

Normal: $E =$ set of roots of $x^{p^n} - x$ and hence is the SF of this over $\mathbb{Z}_p$.

So we have $G = G(E|\mathbb{Z}_p)$, the Galois group of this extension.

We have seen (Lemma 4.0) that E has the automorphism

$$\sigma(x) = x^p$$

(known as 'Frobenius automorphism').

Lemma *Assume $E \supset \mathbb{Z}_p$ and $(E : \mathbb{Z}_p) = n$. Then $G(E|\mathbb{Z}_p) = \langle\sigma\rangle$, cyclic of order n.*

Proof Let $G = G(E|\mathbb{Z}_p)$.

(1) We claim that σ is in G, i.e. σ is the identity on $\mathbb{Z}_p$: If $a \in \mathbb{Z}_p$ then a is a root of $x^p - x$ (special case of). So $\sigma(a) = a$.

Therefore $\langle\sigma\rangle \leq G$. We are done if we show that σ has order n, i.e. $\sigma^n = e$ and if $\sigma^k = e$ then $k \geq n$.

(a) Recall $E =$ set of roots of $x^{p^n} - x$. So for each $a \in E$ we have

$$\sigma^n(a) = \sigma^{n-1}(a^p) = \ldots = a^{p^n} = a$$

and $\sigma^n = e$.

(b) Suppose $\sigma^k = e$. Then for all $a \in E$ we have $a^{p^k} = a$. So all elements of E are roots of the polynomial $x^{p^k} - x$. There are p^n such elements, so $p^k \geq p^n$ and $k \geq n$.

□

With the FTGT we can now classify all intermediate fields.

Corollary *Let $E \supset \mathbb{Z}_p$ with $(E : \mathbb{Z}_p) = n$.*
(a) If $E \supset K \supset \mathbb{Z}_p$ then $(E : K) = m$ where m divides n.
(b) For each divisor m of n there is a unique intermediate field $E \supset K \supset \mathbb{Z}_p$ with $(E : K) = m$.

Proof Part (a) follows from the Tower theorem.

(b) G is cyclic of order n. Let $n = mr$, then G has a unique subgroup of order m. (this subgroup is $\langle \sigma^r \rangle$). Let $K =$ the fixed field of this group, then $(E : K) = m$ by the FTGT.

Note also that then $\langle \sigma^r \rangle = G(E|K)$. We can also describe K, it is the set of roots of $x^{p^r} - x$.

By uniqueness of field of a fixed size we also have: Let E, K be fields of sizes p^n and p^k. Then K is (isomorphic to) a subfield of E if and only if k divides n.

Exercise Draw diagram of intermediate fields when $|E| = 2^{12}$.

Theorem 4.8 *Assume F is a finite field. Then for all $n \geq 1$ there is an irreducible polynomial in $F[x]$ of degree n.*

Proof Assume $|F| = p^m$. Let $E =$ the field of size p^{nm}, then $F \subseteq E$ and $(E : F) = p^n$ by the Corollary (and uniqueness) If $E = F(\theta)$ then the minimal polynomial of θ in $F[x]$ is irreducible of degree n. Such θ exists, for example take a generator of the (cyclic) group E^*.

This can be used to count irreducible polynomials over finite fields.

Example How many monic irreducible polynomials of degree 4 are there over $\mathbb{Z}_3$?