7 Finite fields

If p is a prime number, we write $\mathbb{F}_p := \mathbb{Z}/(p)$. Warning: later we shall define $\mathbb{F}_q$ for more values of q, but in these cases it is not $\mathbb{Z}/(q)$.

Let K be a finite field. Then its characteristic is a prime number p because otherwise K would contain a copy of $\mathbb{Q}$. So the prime subfield of K is isomorphic to $\mathbb{F}_p$. Let us assume it *is* $\mathbb{F}_p$.

Write $[K : \mathbb{F}_p] = n$. Then K has precisely p^n elements. The reason is that, as we learned in linear algebra, there exists an isomorphism of vector spaces over $\mathbb{F}_p$ between K and $(\mathbb{F}_p)^n$. The latter has p^n elements.

We shall prove that for every power q of a prime number there exists a field of q elements and, conversely, any two such fields are isomorphic. The main step is in the following.

Proposition 106. Let p be a prime number and $K/\mathbb{F}_p$ an extension. Let $n \geq 1$ and write $q = p^n$. Then $\#K = q$ if and only if $K/\mathbb{F}_p$ is a splitting field of the polynomial $g = X^q - X$.

Proof. Proof of $\Leftarrow$. Recall from exercise 2.6 the Frobenius endomorphism $F\colon K \to K$ defined by $F(a) = a^p$. Let $A = \{a \in K \mid F^n(a) = a\}$. Then A is a subfield of K because if $a, b \in A$ then $F^n(a+b) = F^n(a) + F^n(b) = a + b$ and likewise for multiplication of a, b or inverting a. Also, A contains the roots of g. Therefore, A contains the subfield of K generated by the roots of g. Since K is a splitting field of g, we find $K \subset A$. It follows that $K = A$, and that every element of K is a root of g. But g has no multiple roots in K by proposition 93 and the observation that $g' = -1$. Therefore $\#K = \deg g = q$.

Proof of $\Rightarrow$. Let $\#K = q$. Then the multiplicative group $K^\times$ has order $q-1$. Therefore $u^{q-1} = 1$ for all $u \in K^\times$. Therefore $u^q = u$ for all $u \in K$. Every element of K is a root of g. But $\deg g = \#K$ so we must have $g = \prod(X - a)$, the product being over the elements a of K. This shows that $K/\mathbb{F}_p$ is a splitting field of g as required. □

We know that splitting fields exist and are unique up to isomorphism. This proves the following.

Proposition 107. Let $q > 1$ be a power of a prime number. Then there exists a field of q elements. Any two such are isomorphic. □

A field of q elements is usually written $\mathbb{F}_q$. This is justified by the fact that such a field depends only on q up to isomorphism; but no particular field in its isomorphism class is meant specifically.

Next we consider what Galois theory says about a finite extension of a finite field.

Proposition 108. Let $K \subset L$ be finite fields. Then L/K is Galois and its Galois group is cyclic.

Proof. We may assume $\mathbb{F}_p \subset K \subset L$. Let $F\colon L \to L$ be Frobenius, $F(a) = a^p$. You proved in exercise 2.6 that F is an injective ring endomorphism. As L is

finite, F is surjective as well. Therefore F is an element of the Galois group $G = \mathrm{Gal}(L/\mathbb{F}_p)$.

Write $p^n = \#L = q$ and $g = X^q - X$. By proposition 106, $L/\mathbb{F}_p$ is a splitting field of g. This proves that $F^n = 1$. No lower power of F is the identity because if $F^k = 1$, $k \geq 1$ then L is contained in the splitting field of $X^{p^k} - X$ and $k \geq n$.

In exercise 4.10 you proved that $[L : \mathbb{F}_p] \geq \#G$ and that equality implies that $L/\mathbb{F}_p$ is Galois. But we have just seen that $\#G \geq \#\langle F\rangle = [L : \mathbb{F}_p]$. This proves that $L/\mathbb{F}_p$ is Galois and that its Galois group is the cyclic group $\langle F\rangle$.

Now K is an intermediate field for $L/\mathbb{F}_p$ hence closed by the main theorem of Galois theory. Thus L/K is also Galois. Its Galois group is a subgroup of the cyclic group $\mathrm{Gal}(L/\mathbb{F}_p)$ and is therefore itself cyclic. □

Proposition 109. Let K be a field. Let $G \subset K^\times$ be a finite subgroup of the multiplicative group of K. Then G is cyclic.

Proof. Suppose that G is not cyclic. The theory of finite abelian groups tells us that then G contains a subgroup H isomorphic to $C_p \times C_p$ with p a prime number. Then all elements of H are roots of $X^p - 1$, so H has at most p elements, a contradiction. □

In particular, if K is a finite field then $K^\times$ is a finite group and therefore cyclic by proposition 109.

Exercises

(7.1) Let $K \subset L$ be finite fields. Prove that L is separable over K.

(7.2) Let p be a prime number and $a, b \geq 1$. Prove that $\mathbb{F}_{p^a}$ can be embedded into $\mathbb{F}_{p^b}$ if and only if $a \mid b$.

(7.3) Find a generator of the multiplicative group $\mathbb{F}_{31}^*$.

(7.4) For each $d \in \{3, 5, 7, 9\}$, find at least one irreducible $f \in \mathbb{F}_2[x]$ such that if α is a root of f in an extension of $\mathbb{F}_2$, then $\#\langle\alpha\rangle = d$, where $\langle\alpha\rangle$ is the multiplicative group generated by α.

(7.5) Let $\mathbb{F}_q$ be a finite field of q elements and let $a \geq 1$.

(a) Prove that $\mathbb{F}_{q^a}/\mathbb{F}_q$ is primitive (that is, $\mathbb{F}_{q^a} = \mathbb{F}_q(\alpha)$ for some $\alpha \in \mathbb{F}_{q^a}$) and deduce that there exists an irreducible polynomial in $\mathbb{F}_q[X]$ of degree a.

(b) Prove that $X^{q^a} - X \in \mathbb{F}_q[X]$ has no multiple roots in any field extension.

(c) Let $a \geq 1$. Prove that $X^{q^a} - X$ is the product of all irreducible monic polynomials in $\mathbb{F}_q[X]$ whose degree divides a.

(d) Let $h_d(q)$ be the number of monic irreducible $f \in \mathbb{F}_q[x]$ of degree d. Prove

$$\sum_{d|a} d\, h_d(q) = q^a. \tag{110}$$

(e) Prove that there exists a polynomial $H_a \in \mathbb{Q}[y]$ such that $h_a(r) = H_a(r)$ for all prime powers r.

(f) Let $f \in \mathbb{F}_q[x]$ be of degree d. Prove that f is irreducible if and only if f does not divide $x^{q^a} - x$ whenever $a < d$. (This gives a fast algorithm to check irreducibility.)

(7.6) Let K be a field of characteristic $p > 0$. Let $f = X^p - X - a \in K[X]$.

(a) Prove $f(X) = f(X+1)$.

(b) Prove: f has no multiple roots in any field extension.

(c) Suppose f has no root in K. Then f is irreducible.

8 Added later

Here are a few easy details that I didn't write up earlier.

8.1 On K-homomorphisms

This should be put directly before proposition 60.

For clarity here is an easy observation. Notice the analogy between parts (a) and (b).

Lemma 111.

(a) Let $s\colon A \to B$ be a homomorphism of rings and $f \in \mathbb{Z}[X]$ a polynomial. Then $s(f(a)) = f(s(a))$ for all $a \in A$.

(b) Let L_1/K and L_2/K be field extensions. Let $s\colon L_1 \to L_2$ be a K-homomorphism and let $f \in K[X]$ be a polynomial. Then $s(f(a)) = f(s(a))$.

(c) Let $K(\alpha)/K$ and $K(\beta)/K$ be field extensions with α and β algebraic over K. Let $s\colon K(\alpha) \to K(\beta)$ be a K-isomorphism such that $s(\alpha) = \beta$. Then α and β have the same minimum polynomial over K.

Proof. (a). Write $f = \sum_i c_i X^i$ with $c_i \in \mathbb{Z}$. Then

$$\begin{aligned} s(f(a)) &= s\sum_i c_i\, a^i = \sum_i s(c_i\, a^i) = \sum_i s(c_i)\, s(a^i) \\ &= \sum_i c_i\, s(a^i) = \sum_i c_i\, s(a)^i = f(s(a)). \end{aligned}$$

(b). Write $f = \sum c\, X^i$ with $c \in K$. Then

$$\begin{aligned} s(f(a)) &= s\sum c\, a^i = \sum s(c\, a^i) && \text{because } s \text{ is a ring homomorphism} \\ &= \sum s(c)\, s(a^i) && \text{because } s \text{ is a ring homomorphism} \\ &= \sum c\, s(a^i) && \text{because } s \text{ is a } K\text{-homomorphism} \\ &= \sum c\, s(a)^i && \text{because } s \text{ is a ring homomorphism} \\ &= f(s(a)). \end{aligned}$$

(c). Let f be the minimum polynomial of α over K. By (b) we have $0 = s(0) = s(f(\alpha)) = f(s(\alpha)) = f(\beta)$. Thus f is the minimum polynomial of β as well. □

A strong converse to (c) is proposition 60b.

8.2 Group actions

Here is some simple background on group actions.

Definition 112. Let G be a group and X a set. A **left G-action on X** is a map $G \times X \to X$ written $(g,x) \mapsto g(x) = gx$ such that $(gh)x = g(hx)$ for all $g,h \in G$, $x \in X$.

Similarly, a **right G-action on X** is a map $X \times G \to X$ written $(x,g) \mapsto (x)g = xg$ such that $x(gh) = (xg)h$ for all $g,h \in G$, $x \in X$.

If $(g,x) \mapsto gx$ is a left G-action then $(x,g) \mapsto xg$ is *not* a right action; but $(x,g) \mapsto xg^{-1}$ is.

Let X be a set. A bijective map $X \to X$ is sometimes called a **permutation** of X. The set of permutations of X forms a group $\mathrm{Sym}(X)$ called the **symmetric group on X**. Analogous to the distinction between left and right actions, one can and should choose whether to write sx or xs for all $x \in X$ and $s \in \mathrm{Sym}(X)$.

We write S_n for $\mathrm{Sym}(\{1,\ldots,n\})$. Thus $\mathrm{Sym}(X)$ is isomorphic to S_n if X has n elements.

The proposition says that G-actions on X are 'the same' as homomorphisms $G \to \mathrm{Sym}(X)$.

Proposition 113. Let G be a group and X a set. There exists a unique bijection between the set of left G-actions on X and the set of homomorphisms $G \to \mathrm{Sym}(X)$ (with permutations of X acting on the left) such that whenever the action $(g,x) \mapsto g \circ x$ corresponds to the homomorphism $s\colon G \to \mathrm{Sym}(X)$ then $(sg)x = g \circ x$ for all $g \in G$, $x \in X$.

Proof. Exercise. □

A G-action on X is said to be **faithful** if the corresponding homomorphism $G \to \mathrm{Sym}(X)$ is injective.

Exercise (8.1) Prove that a left G-action on X is faithful if and only if for all nontrivial $g \in G$ there exists $x \in X$ such that $gx \neq x$.

8.3 Actions of Galois groups

This should be amended to chapter 6.

In order to determine the structure of a Galois group in practice, it is useful to embed it into S_n. This can be done as follows.

Lemma 114. Let L/K be an extension and write $G = \mathrm{Gal}(L/K)$. Let $U \subset L$ be a G-invariant subset of L; then the G-action on L restricts to a G-action on U, that is, to a homomorphism $s\colon G \to \mathrm{Sym}(U)$.

(a) Suppose that $L = K(U)$, that is, L is generated over K by U. Then s is injective.

(b) Suppose that L/K is a splitting field for $f \in K[X]$ and that U is the set of roots in L of f. Then U is G-invariant and $L = K(U)$. In particular, G acts faithfully on U.

Proof. (a). Suppose that $g \in G$ is such that $s(g) = 1$. Then g preserves U

pointwise. Therefore g preserves any element in the ring $K[U]$ by proposition 111b and indeed any element in the field $K(U) = L$. This shows that $g = 1$ and that s is injective.

(b). Proof that U is G-invariant. Let $u \in U$, $s \in G$. Then $f(s(u)) = s(f(u)) = s(0) = 0$ where the first equality is by lemma 111b. This shows $s(u) \in U$ as required.

Proof that the G-action on U is faithful. Note that this means by definition that the corresponding homomorphism $G \to \mathrm{Sym}(U)$ is injective. It is true by part (a) and the fact that $L = K(U)$. □

Example 115. Let $K \subset \mathbb{C}$ be the complex splitting field for $f = X^3 - 2$ over $\mathbb{Q}$ and put $G = \mathrm{Gal}(K/\mathbb{Q})$.

(a) Prove that $K/\mathbb{Q}$ is Galois.

(b) Prove that f is irreducible over $\mathbb{Q}$.

(c) Prove $[K : \mathbb{Q}] = 6$.

(d) Prove that $\#G = 6$.

(e) Prove $G \cong S^3$.

(f) List the subgroups of G and the intermediate fields.

Solution. (a). By assumption $K/\mathbb{Q}$ is a splitting field. It is also separable because the characteristic is 0. Now apply (2) ⇒ (1) in theorem 97.

(b). The polynomial $f \in \mathbb{Z}[X]$ is Eisenstein at 2. Apply proposition 47.

(c). Put $\alpha = \sqrt[3]{2}$, $\omega = \exp(2\pi i/3)$. Then $K = \mathbb{Q}(\alpha, \omega)$. Also $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ because f is irreducible of degree 3 by (b) and α is a root of f. Moreover $[K : \mathbb{Q}(\alpha)] = 2$ because ω is a root of $X^2 + X + 1$ but is not in $\mathbb{R}$ while $\mathbb{Q}(\alpha) \subset \mathbb{R}$. Using the tower law we find $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6$.

(d). Immediate from (a), (c) and the main theorem of Galois theory, theorem 78.

(e). The Galois group G acts faithfully on the set of roots of f, which is a set of three elements. That gives us an injective homomorphism ϕ: $G \to S_3$. But G has 6 elements by (d), and S_3 has 6 elements too. So ϕ is bijective.

(f). Inspection of the isomorphism from (e) suggests that we define $s, t \in G$ by $s(\omega) = t(\omega) = \omega^2$, $s(\alpha) = \alpha$, $t(\alpha) = \alpha\omega^2$. We find the following intermediate fields.

subgroup	1	$\langle s \rangle$	$\langle t \rangle$	$\langle sts \rangle$	$\langle st \rangle$	G
field	K	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\alpha\omega)$	$\mathbb{Q}(\alpha\omega^2)$	$\mathbb{Q}(\omega)$	$\mathbb{Q}$

As an example we prove that $K^{\langle s \rangle} = \mathbb{Q}(\alpha)$. We have $s(\alpha) = \alpha$ so $K^{\langle s \rangle} \supset \mathbb{Q}(\alpha)$. Also

$$[K^{\langle s \rangle} : \mathbb{Q}] = [G : \langle s \rangle] = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

which proves $K^{\langle s \rangle} = \mathbb{Q}(\alpha)$. □