Notes on finite fields

1. The order of a finite field

Recall (Goodman 6.4.9) that the subring generated by 1 in any integral domain R is isomorphic either to $\mathbb{Z}$, in which case we say R has characteristic zero, or to $\mathbb{Z}_p$, in which case we say R has characteristic p. If F is a field of characteristic zero, then F is clearly infinite. In fact, since F is a field, it not only contains a copy of $\mathbb{Z}$, but a copy of the fraction field $\mathbb{Q}$ of $\mathbb{Z}$.

A finite field F must therefore have characteristic p for some prime p, that is, the subring of F generated by 1 is isomorphic to $\mathbb{Z}_p$. Note that this subring is already a subfield. We can identify it with $\mathbb{Z}_p$ and think of $\mathbb{Z}_p \subseteq F$ as a field extension.

In particular, F is a vector space over $\mathbb{Z}_p$, and since F is finite, $d = \dim_{\mathbb{Z}_p}(F)$ is finite. Then F is isomorphic as a vector space (and as an abelian group, but not as a ring!) to $(\mathbb{Z}_p)^d$. Hence F has p^d elements.

Our main goal in these notes will be to prove

Theorem 1.

(i) For every prime power $q = p^d$, there exists a finite field $\mathbb{F}(q)$ of order q.

(ii) $\mathbb{F}(q)$ is unique up to isomorphism.

(iii) $\mathbb{F}(q)$ can be constructed as $\mathbb{Z}_p(\alpha)$, where α is a root of an irreducible polynomial $f(x)$ of degree d in $\mathbb{Z}_p[x]$.

In the process we will also learn something about the structure of the finite fields $\mathbb{F}(q)$, and use this knowledge to discover an algorithm for testing whether a polynomial $f(x)$ over $\mathbb{Z}_p$ is irreducible in $\mathbb{Z}_p[x]$.

2. The Frobenius automorphism

Proposition (Goodman 9.3.3). *If F is a field of characteristic p, the map $\Phi\colon F \to F$ given by $\Phi(x) = x^p$, called the Frobenius homomorphism, is a ring homomorphism. The Frobenius homomorphism is always injective. If F is finite, then Φ is bijective, that is, it is an automorphism.*

Proof. It is clear that $\Phi(xy) = x^p y^p = \Phi(x)\Phi(y)$. We also need to prove that $\Phi(x + y) = \Phi(x) + \Phi(y)$. By the binomial theorem,

$$\Phi(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}. \tag{1}$$

Recall that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

For $0 < k < p$, $k!$ and $(p-k)!$ are products of positive integers less than p. Hence p does not divide the denominator in the above fraction. Since p divides the numerator, we see that p divides $\binom{p}{k}$. Bearing in mind that $p\,z = 0$ for every element z in a field of characteristic p, we see that the terms for $0 < k < p$ on the right hand side in (1) are all zero. The remaining terms, for $k = 0$ and $k = p$, are x^p and y^p. This gives

$$\Phi(x + y) = (x + y)^p = x^p + y^p = \Phi(x) + \Phi(y).$$

We have now shown that Φ is a ring homomorphism. It is not zero, since $\Phi(1) = 1$, so its kernel is an ideal $I \subset F$, $I \neq F$. But since F is a field, the only such ideal is $I = \{0\}$. Hence Φ is injective. (This argument actually shows that every unital ring homomorphism $\phi\colon F \to R$ from a field to any ring with identity is injective.)

If F is finite, then Φ, being an injective map from F to F, is also surjective. $\square$

We will now prove part (i) of Theorem 1, that for every prime power $q = p^d$, a finite field of order q exists.

Given $q = p^d$, let F be the splitting field (Goodman 9.2.3) over $\mathbb{Z}_p$ of the polynomial $P(x) = x^q - x$ in $\mathbb{Z}_p[x]$. Since p divides q, the formal derivative of $P(x)$ is $P'(x) = -1$, which is (obviously) relatively prime to $P(x)$. By the derivative criterion (Goodman 9.3.5), $P(x)$ has no multiple roots in any extension field of $\mathbb{Z}_p$. In particular, $P(x)$ has q distinct roots in its splitting field F.

For an element $\alpha \in F$ to be a root of $P(x)$ means that $\alpha^{p^d} = \alpha$, or, since $\alpha^{p^d} = \Phi^d(\alpha)$, that the d-th power Φ^d of the Frobenius automorphism fixes α.

Since F is generated by roots of $P(x)$, this implies that Φ^d fixes *every* element of F. In other words, every element of F is a root of $P(x)$. Since $P(x)$ has q roots in F, this shows that $|F| = q$.

Now we prove part (ii) of Theorem 1, that all finite fields of order q are isomorphic. We know (Goodman 9.2.5) that the splitting field of $P(x)$ over $\mathbb{Z}_p$ is unique up to isomorphism, but we still need to show that if E is another field of order q, then E is a splitting field for $P(x)$.

So, suppose $|E| = q$, without assuming in advance that E is a splitting field for $P(x)$. The multiplicative group $E^\times = E \setminus \{0\}$ has order $q - 1$, so by Lagrange's Theorem, every $x \in E^\times$ satisfies $x^{q-1} = 1$, and consequently $x^q = x$. But of course $x = 0$ also satisfies $x^q = x$. This shows that every element of E is a root of $P(x) = x^q - x$. Since $|E| = q$, it follows that E is a splitting field for $P(x)$.

From now on we write $\mathbb{F}(q)$ for the splitting field of $P(x)$, which we have just shown is the unique finite field of order q, up to isomorphism.

To prove part (iii) of Theorem 1, we just have to show that $\mathbb{F}(q)$ can be generated over $\mathbb{Z}_p$ by a single element α. Then by the basic theory of field extensions, we have $\mathbb{F}(q) = \mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(f(x))$, where $f(x) \in \mathbb{Z}_p[x]$ is the minimal polyonomial of α, which will be a polynomial of degree $d = \dim_{\mathbb{Z}_p}(\mathbb{F}(q))$.

It follows from the structure theorem for finite abelian groups that the multiplicative group $F^\times$ of any finite field is cyclic. This is shown in Goodman, Theorem 3.6.25. I'll remind you what the essential point there is. Since $F^\times$ is a finite abelian group, it has an invariant factor decomposition $F^\times \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, where each n_i divides the one before. Then every element $x \in F^\times$ satisfies $x^{n_1} = 1$. However, since F is a field, the equation $x^{n_1} - 1 = 0$ cannot have more than n_1 roots, giving $|F^\times| \leq n_1$. But $|F^\times| = n_1 \cdots n_k$, so this implies that $F^\times$ has just one factor in its invariant factor decomposition, that is, $F^\times$ is cyclic.

Now let $\alpha \in F$ be a generator of $F^\times$ as a cyclic group. Then α also generates F as an extension of $\mathbb{Z}_p$.

Just to be clear, I should point out that the above is just one possible way to find a generator of $\mathbb{F}(q)$ over $\mathbb{Z}_p$. There are often other elements α such that $\mathbb{F}(q) = \mathbb{Z}_p(\alpha)$, but α does not generate the group $\mathbb{F}(q)^\times$. For example, in $\mathbb{F}(9)$, we have $\mathbb{F}(9)^\times \cong \mathbb{Z}_8$, which has four elements that generate it as a cyclic group. But since $\dim_{\mathbb{Z}_3} \mathbb{F}(9) = 2$, the only subfields of $\mathbb{F}(9)$ are itself and $\mathbb{Z}_3 = \mathbb{F}(3)$. Hence any element $\alpha \in \mathbb{F}(9)$ which is not in $\mathbb{Z}_3$ is a generator. There are six such elements, but only four of them are generators of $\mathbb{F}(9)^\times$.

3. Extensions of finite fields

Let us now work out for which q and r there can be an extension of finite fields $\mathbb{F}(r) \subseteq \mathbb{F}(q)$.

Of course both fields must have the same characteristic, so q and r must be powers of the same prime, say $q = p^d$ and $r = p^e$. Also, since $\dim_{\mathbb{F}(r)}(\mathbb{F}(q)) = \dim_{\mathbb{Z}_p}(\mathbb{F}(q))/\dim_{\mathbb{Z}_p}(\mathbb{F}(r)) = d/e$, we must have e dividing d.

We will now prove that these conditions are sufficient, that is, if e divides d then $\mathbb{F}(p^d)$ has a subfield E of order p^e, and moreover this subfield is unique. (We know that E is unique up to isomorphism, being isomorphic to $\mathbb{F}(p^e)$, but that is not sufficient to conclude that $\mathbb{F}(p^d)$ has only one such subfield E.)

For this we consider the polynomials $P(x) = x^q - x = x^{p^d} - x$ and $Q(x) = x^r - x = x^{p^e} - x$ in $\mathbb{Z}_p[x]$. We will show that if e divides d, then $Q(x)$ divides $P(x)$, or in other words, $x^q - x$ belongs to the ideal $(x^r - x) \subseteq \mathbb{Z}_p[x]$. Let $d = k\,e$, so $q = r^k$. In the quotient ring $\mathbb{Z}_p[x]/(x^r - x)$ we have $x^r \equiv x$ and therefore $x^{r^2} = (x^r)^r \equiv x^r \equiv x$, $x^{r^3} = (x^{r^2})^r \equiv x^r \equiv x$, and so on. In particular, $x^q \equiv x$, which means that $x^q - x \in (x^r - x)$.

Now, since $\mathbb{F}(q)$ is a splitting field of $P(x)$, and $Q(x)$ is a factor of $P(x)$, $\mathbb{F}(q)$ contains r roots of $Q(x)$, that is, it contains a splitting field E of $Q(x)$, which we have already seen is isomorphic to $\mathbb{F}(r)$. Furthermore, any subfield $E' \subseteq \mathbb{F}(q)$ of order r is a splitting field of $Q(x)$ and therefore contains all the roots of $Q(x)$ in $\mathbb{F}(q)$. In other words, $E \subseteq E'$, and therefore $E = E'$ since $|E| = |E'| = r$. This shows that E is unique.

Looking ahead a bit, the picture we have just worked out can be understood nicely in terms of Galois theory. Since $\mathbb{F}(q)$ is the splitting field of the separable polynomial $P(x)$ over $\mathbb{Z}_p$, the extension $\mathbb{Z}_p \subseteq \mathbb{F}(q)$ is a Galois extension.

The Frobenius automorphism Φ is an element of the Galois group G of $\mathbb{F}(q)$ over $\mathbb{Z}_p$. Its fixed field consists of the roots of the equation $x^p - x = 0$ in $\mathbb{F}(q)$. But this equation has only p roots, so the fixed field of Φ, or of the cyclic subgroup $\langle \Phi \rangle \subseteq G$, is just $\mathbb{Z}_p$. By the Galois correspondence, this implies that $G = \langle \Phi \rangle$.

In other words, the Galois group G of $\mathbb{F}(q)$ over $\mathbb{Z}_p$ is cyclic of order d (where $q = p^d$), and generated by Φ. Now $G \cong \mathbb{Z}_d$ has one subgroup for each divisor e of d, namely the cyclic subgroup generated by Φ^e. These subgroups are in one-to-one correspondence with the subfields of $\mathbb{F}(q)$: specifically, the fixed field of the subgroup $\langle \Phi^e \rangle$ is the unique subfield $E \subseteq \mathbb{F}(q)$ of order p^e.

4. Irreducibility of polynomials over $\mathbb{Z}_p$

Part (iii) of Theorem 1 implies that there exist irreducible polynomials in $\mathbb{Z}_p$ of every degree $d > 0$. Actually, we can say much more:

Proposition. *For $q = p^d$, the polynomial $P(x) = x^q - x$ is exactly the product of all monic irreducible polynomials $f(x)$ in $\mathbb{Z}_p[x]$ of degree dividing d.*

Proof. Since $P(x)$ does not have repeated roots, it is a product of distinct irreducible factors, which we can take to be monic, since $P(x)$ is monic. Since the roots of $P(x)$ in its splitting field $\mathbb{F}(q)$ are all the elements of $\mathbb{F}(q)$, the irreducible factors are precisely the minimal polynomials of elements of $\mathbb{F}(q)$. In particular, their degrees are the dimensions over $\mathbb{Z}_p$ of subfields $E \subseteq \mathbb{F}(q)$, so they divide d.

Conversely, if $f(x) \in \mathbb{Z}_p$ is irreducible of degree e dividing d, then it has a root in $\mathbb{F}(p^e) \cong \mathbb{Z}_p[x]/(f(x))$. We saw in the previous section that that $\mathbb{F}(p^e)$ is isomorphic to a subfield of $\mathbb{F}(q)$, so $f(x)$ has a root in $\mathbb{F}(q)$, and is therefore an irreducible factor of $P(x)$. □

Using this proposition, we can determine the exact number of irreducible polynomials of each degree in $\mathbb{Z}_p[x]$. For $d = 1$, $P(x) = x^p - x$ must have p irreducible factors all of degree 1, which are of course just the polynomials $x - a$ for each of the p residue classes $a \in \mathbb{Z}_p$. For $d = 2$, $P(x) = x^{p^2} - x$ has the p linear factors we just found, together with $(p^2 - p)/2$ quadratic factors, since its total degree is p^2. Hence there are $(p^2 - p)/2$ distinct monic irreducible quadratic polynomials over $\mathbb{Z}_p$, for every prime p. In the case $p = 2$, we have $(2^2 - 2)/2 = 1$. Of the four monic quadratic polynomials in $\mathbb{Z}_2[x]$, the unique irreducible one is $x^2 + x + 1$, since the other three have roots in $\mathbb{Z}_2$.

Continuing in this manner, we find that for $d = 3$, $P(x)$ must have p linear factors and $(p^3 - p)/3$ factors of degree 3; for $d = 4$, it must have the p linear factors and $(p^2 - p)/2$ quadratic factors that we already discovered, together with $(p^4 - p^2)/4$ factors of degree 4, and so on.

Another, more important, application of the above proposition is to test whether a given polynomial $f(x) \in \mathbb{Z}_p[x]$ is irreducible. Suppose the degree of $f(x)$ is d. If it is not irreducible, $f(x)$ must have an irreducible factor $g(x)$ of degree at most $d/2$. Then $g(x)$ is a factor of $x^{p^e} - x$ for some $e \leq d/2$, so we can discover whether $f(x)$ is irreducible by computing its gcd with each of these polynomials. If $f(x)$ turns out to relatively prime to $x^{p^e} - x$ for all $e \leq d/2$, then it is irreducible; otherwise $f(x)$ is reducible.

Note that, although the degree p^e of $x^{p^e} - x$ might be quite large, the first step in computing $\gcd(f(x), x^{p^e} - x)$ is to find the remainder of $x^{p^e} - x$ modulo $f(x)$. This remainder is a polynomial of degree less than d, easily computed by starting with x and taking repeated p-th powers modulo $f(x)$.

Example. We'll test $f(x) = x^4 + x + 2$ for irreducibility in $\mathbb{Z}_3[x]$. It has no root in $\mathbb{Z}_3[x]$, hence no linear factor, so if $f(x)$ is reducible it must be a product of quadratic factors, and therefore have a common divisor with $x^9 - x$ (here $9 = p^2$). Modulo $f(x)$ (and reducing all coefficients modulo 3) we have $x^4 \equiv -x + 1$, $x^8 \equiv x^2 - 2x + 1 \equiv x^2 + x + 1$, $x^9 \equiv x^3 + x^2 + x$, and $x^9 - x \equiv x^3 + x^2$. Therefore $\gcd(f(x), x^9 - x) = \gcd(f(x), x^3 + x^2)$. Now $x^3 + x^2$ factors as $(x + 1)\, x^2$, and we already saw that $f(x)$ has no linear factors, so $f(x)$ is relatively prime to $x^3 + x^2$. It follows that $x^4 + x + 2$ is irreducible in $\mathbb{Z}_3[x]$. Note that this also implies that $x^4 + x + 2$ is irreducible in $\mathbb{Z}[x]$, and therefore in $\mathbb{Q}[x]$, by Gauss' Lemma.