Lecture Notes, Week 4

Math 480A2: Mathematics of Blockchain Protocols, Fall 2022

Lecturer: Bryan Gillespie

Finite Fields

We are now ready to present the construction and full classification of finite fields.

Proposition 1. *Let K be a finite field. Then K is a field extension of $\mathbb{Z}/p\mathbb{Z}$ for some prime number p.*

Proof. Let $\varphi : \mathbb{Z} \to K$ be the ring homomorphism which maps a positive integer n to the sum $1 + 1 + \cdots + 1$ of n copies of 1 in K, and a negative integer n to $-\varphi(-n)$. Then by the first isomorphism theorem, $\operatorname{im}\varphi$ is isomorphic to $\mathbb{Z}/\ker\varphi$. Since K is finite, the quotient $\mathbb{Z}/\ker\varphi$ must be finite, so $\ker\varphi \neq \{0\}$, and must be equal to (m) for a positive integer m. Then m cannot be 1 since this would imply that $\varphi(1) = 1 = 0$, but this is never the case in a field. If m is composite, say $m = ab$ with $a, b < m$, then this implies that $\phi(ab) = \phi(a)\phi(b) = 0$ in K, which contradicts that the nonzero elements $\phi(a)$ and $\phi(b)$ have multiplicative inverses in K. Thus we must have $m = p$ for somep rime number p, so $\operatorname{im}\varphi$ is a subfield of K isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

□

If K is any field, the ring homomorphism $\mathbb{Z} \to K$ mapping the integer 1 to the field element 1 has kernel equal to an ideal $(m) \subseteq \mathbb{Z}$. The number m is called the **characteristic** of the field K. If $m > 0$ then $m = p$ for some prime number p by the above reasoning, and K contains a copy of $\mathbb{Z}/p\mathbb{Z}$. If $m = 0$, then instead K contains a copy of $\mathbb{Q}$. In each case this subfield is called the **prime subfield** of K.

Proposition 2. *Let K be a finite field with prime subfield $F = \mathbb{Z}/p\mathbb{Z}$. Then $|K| = p^r$ for some positive integer r.*

Proof. The set K with addition operation inherited from its field structure is an additive abelian group, and with field multiplication by elements of F, it is a vector space over F. Since K is finite, it must be a finite-dimensional vector space, since otherwise an F-basis of K must be an infinite subset. Thus K is isomorphic to (and in particular in bijection with) the vector space F^r for some positive integer r. The result follows because F^r has p^r elements. □

The integer r in the above result is called the **degree** of K over F, written $[K : F]$, and is generally defined as the dimension of K as an F-vector space. In the following, we will let $q = p^r$ denote a positive power of a prime number p.

Lemma 3. *In a field K of order q, every element is a root of the polynomial $x^q - x$.*

Proof. Since K is a field, the nonzero elements of K form a multiplicative group of order $q-1$. In particular, a nonzero element α has multiplicative order dividing $q-1$ by Lagrange's Theorem, and thus satisfies $\alpha^{q-1} = 1$, implying that α is a root of $x^q - x$. The zero element of K is also clearly a root. □

We will need the following lemma for the next argument.

Lemma 4. *Let $F = \mathbb{Z}/p\mathbb{Z}$. Then in $F[x, y]$, $(x + y)^q = x^q + y^q$ for any $q = p^r$, $r \geq 0$.*

Proof. First note that for $1 \leq k \leq p - 1$, the binomial coefficient $\binom{p}{k} \in \mathbb{Z}$ is divisible by p. This is because it can be written as $p!/k!(p-k)!$, and p clearly divides $p!$ but not $k!$ or $(p-k)!$, so p must divide the whole expression.

In particular, this implies that the polynomial identity holds for $q = p$: by the binomial theorem, we have

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p = x^p + y^p$$

Here, the last equality holds because each of the intermediate coefficients $\binom{p}{k}$ is divisible by p, and thus is equal to 0 as an element of F.

Now we complete the proof by induction on r. For $r = 0$, this is a trivial statement: $(x + y)^1 = x^1 + y^1$. For $r > 0$, we write

$$(x+y)^{p^r} = \big((x+y)^{p^{r-1}}\big)^p = \big(x^{p^{r-1}} + y^{p^{r-1}}\big)^p = (x^{p^{r-1}})^p + (y^{p^{r-1}})^p = x^{p^r} + y^{p^r}$$

The second-to-last equality holds because $(x + y)^p = x^p + y^p$ is an identity of polynomials, and so it also holds after substituting $x^{p^{r-1}}$ and $y^{p^{r-1}}$ for x and y. □

Proposition 5. *There exists a finite field of order q for any prime power $q = p^r$.*

Proof. Let L be an extension field of $F = \mathbb{Z}/p\mathbb{Z}$ in which $x^q - x$ splits into a product of linear factors. Then L has characteristic p, so the derivative of $x^q - x$ in L is

$$\mathrm{d}/\mathrm{d}x\big(x^q - x\big) = qx^{q-1} - 1 = -1$$

This implies that $x^q - x$ has no multiple root in L, and thus that the set K of roots of this polynomial in L contains x^q distinct elements. We now show that K is a subfield of L.

We need to show that K is closed under sums, products, additive and multiplicative inverses, and contains 1. We see that $1 \in K$ because $1^q = 1$. We also have $-1 \in K$: if $p = 2$, this is because $-1 = 1$ in F, and if $p > 2$, then this is because q is odd, so $(-1)^q = -1$.

Now let $\alpha, \beta \in K$, so that $\alpha^q = \alpha$ and $\beta^q = \beta$. Then we have

- (Sums) $(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta$ by previous lemma
- (Products) $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$
- (Additive inverses) $(-\alpha)^q = (-1)^q\alpha^q = (-1) \cdot \alpha = -\alpha$
- (Multiplicative inverses) $(\alpha^{-1})^q = \alpha^{-q} = (\alpha^q)^{-1} = \alpha^{-1}$ when $\alpha \neq 0$

□

Remark 6. The above argument that the roots of $x^q - x$ in L form a subfield does not rely on the fact that the polynomial splits into linear factors. More generally, in any field of characteristic p, the same argument shows that the roots of $x^q - x$ (whichever ones are present) will form a finite subfield of L.

Our next result will apply the structure theorem for finitely generated abelian groups, a basic algebra result which we now state, but whose proof we will omit.

Theorem 7 (Structure Theorem for Finitely Generated Abelian Groups)**.** *Let G be an abelian group admitting a finite set of generators. Then G can be uniquely expressed as a direct sum*

$$G \cong \mathbb{Z}^r \oplus (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_k\mathbb{Z})$$

where each of the cyclic components has order at least 2, and d_i divides d_{i+1} for each i. The number r is called the rank *of G, and the numbers $d_1, \ldots, d_k$ are called the* invariant factors*.*

Proposition 8. *The multiplicative subgroup of a finite field K is cyclic.*

Proof. Suppose K has order q. Then the multiplicative subgroup $K^\times$ of nonzero elements of K is an abelian group of order $q-1$. The structure theorem for finitely generated abelian groups implies that $K^\times$ can be written (additively) as a direct sum of nontrivial cyclic subgroups:

$$K^\times \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_k\mathbb{Z})$$

where the order d_i of each cyclic component divides the order d_{i+1} of the next. Let $\alpha \in K^\times$, and write $\alpha = (h_1, \ldots, h_k)$ as an element of the above direct sum. Then writing $d = d_k$, we have

$$\alpha^d = (dh_1, \ldots, dh_k)$$

Since each of the components h_i is an element of a cyclic group of order dividing d, we conclude that dh_i is the identity element 0 in $\mathbb{Z}/d_i\mathbb{Z}$, and so α^d is the identity element 1 of $K^\times$. In particular, we see that every $\alpha \in K^\times$ is a root of the polynomial $x^d - 1$. However, a polynomial of degree d has at most d roots, so $|K^\times| = q - 1 \leq d$.

However, since $K^\times \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_k\mathbb{Z})$, the order of $K^\times$ is given by $d_1 d_2 \cdots d_k$. We can therefore conclude that $d_1 d_2 \cdots d_k = q - 1 \leq d_k$, so the only valid choice for the invariant factors of $K^\times$ is $k = 1$ and $d_k = q - 1$. Thus $K^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$, which is cyclic. □

Proposition 9. *There exist irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ of any positive degree.*

Proof. Let K be a finite field with degree r over its prime subfield $F = \mathbb{Z}/p\mathbb{Z}$, and let f be the irreducible polynomial over F of a cyclic generator α of $K^\times$. Then $F[x]/(f) \cong F[\alpha] = K$. However, $F[x]/(f)$ is a vector space of dimension $\deg f$ over F, so $|F|^{\deg f} = |F[x]/(f)| = |K| = |F|^r$, and we conclude that $\deg f = r$. □

Proposition 10. *Any two finite fields of equal order are isomorphic.*

Proof. Let K and K' be two finite fields of equal order $q = p^r$, let F be their common prime subfield, and let α be a generator for $K^\times$ with irreducible polynomial f over F. We can see that f divides $x^q - x$ because α is a root of the latter. In K', the polynomial $x^q - x$ splits into a product of linear factors, so f does as well. In particular, f has a root $\alpha' \in K'$, and f is the irreducible polynomial of α' over F by uniqueness. Then we have

$$K = F[\alpha] \cong F[x]/(f) \cong F[\alpha'] \subseteq K'$$

Comparing cardinalities gives us equality in the last inclusion, so the result follows. □

Proposition 11. *A field of order p^r contains a subfield of order p^k if and only if $k \mid r$.*

Proof. Let K/K' be a field extension of degree d with $|K| = p^r$ and $|K'| = p^k$. Then K is a K'-vector space of dimension d, and thus is isomorphic to $(K')^d$ as a vector space. In particular, its cardinality is $|K'|^d = (p^k)^d = p^{kd}$, so $r = kd$ and k divides r.

Now suppose $r = kd$ for some d. Then we have

$$p^r - 1 = p^{kd} - 1 = (p^k - 1)(p^{(d-1)k} + p^{(d-2)k} + \cdots p^k + 1)$$

so that $q' - 1$ divides $q - 1$. Since the multiplicative group of K is cyclic of order $q - 1$, it has an element β of order $q' - 1$, and the $q' - 1$ powers of β give $q' - 1$ roots of the polynomial $x^{q'-1} - 1$. Thus these powers along with 0 give the collection of q' roots of the polynomial $x^{q'} - x$ in K. By the previous argument proving the existence of finite fields of all orders, this collection of roots is a subfield of K of order q', as required. □

Proposition 12. *The irreducible factors of $x^q - x$ over $F = \mathbb{Z}/p\mathbb{Z}$ are the irreducible polynomials in $F[x]$ whose degree divides r, each with multiplicity 1.*

Proof. Let K be a finite field of order q, and let $g \in F[x]$ be an irreducible polynomial of degree k. Suppose first that g divides $x^q - x$. Then in particular, g can be represented as a product of linear factors in K, since this is the case for $x^q - x$. In particular, g has a root $\beta \in K$, and g is the irreducible polynomial of β over F. This implies that $F[\beta]$ is a subfield of K of order p^k, and so as we have seen, k divides r.

Conversely, suppose that k divides r. Then $F[x]/(g)$ is a field of order p^k such that the image of x under the quotient map is a root of g. By the previous proposition, K has a subfield K' of order p^k, and since all fields of order p^k are isomorphic, there is an isomorphism from $F[x]/(g)$ to K'. In particular, the image β of x in K' is an element of K with irreducible polynomial g. Since β is a root of $x^q - x$ in K, we see that the irreducible polynomial g of β divides $x^q - x$.

Lastly, each irreducible polynomial dividing $x^q - x$ has multiplicity 1 because any irreducible having higher multiplicity would result in $x^q - x$ having a multiple root over K, which is not the case since $x^q - x$ has q distinct roots in K. □

Example 13. Over $F = \mathbb{Z}/3\mathbb{Z}$, the polynomial $x^9 - x$ factors as:

$$x^9 - x = x(x + 1)(x - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1)$$

In particular, this factorization gives a list of all of the irreducible polynomials of degrees 1 and 2 over F. Letting $K = F[x]/(x^2+1)$, we have that K is a finite field with 9 elements, given by

$$0, \quad 1, \quad -1, \quad \bar{x}, \quad \bar{x}+1, \quad \bar{x}-1, \quad -\bar{x}, \quad -\bar{x}+1, \quad -\bar{x}-1$$

The multiplicative subgroup $K^\times$ is cyclic of order 8. However, it is not generated by the underlying variable $\bar{x}$, as can be seen by the computation: $\bar{x}^4 = (\bar{x}^2)^2 = (-1)^2 = 1$. We can see then that the multiplicative order of $\bar{x}$ is 4, so it doesn't generate the entire multiplicative group. However, we can check that $(\bar{x}+1)^4 = ((\bar{x}+1)^2)^2 = (-\bar{x})^2 = -1 \neq 1$. Since the multiplicative order of an element divides the order of $K^\times$, the order of $\bar{x}+1$ must be 8.

The irreducible polynomial of a multiplicative generator of the multiplicative group of K has degree equal to the dimension of K over F. Thus $\bar{x}+1$ must be a root of (exactly) one of the three quadratic factors of $x^9 - x$. We can check that this is the case for the polynomial $x^2 + x - 1$:

$$(\bar{x}+1)^2 + (\bar{x}+1) - 1 = -\bar{x} + \bar{x} + 1 - 1 = 0$$

Thus $\bar{x}+1$ has irreducible polynomial $x^2 + x - 1$ over F. Now let $L = F[y]/(y^2 + y - 1)$. Since K and L are finite fields of equal order 9, they are isomorphic as fields. As usual, the image $\bar{y}$ of y in L is a root of the quotient polynomial $y^2 + y - 1$, and so this is the irreducible polynomial of $\bar{y}$. From the previous proof that finite fields of equal order are isomorphic, we know that homomorphism taking $\bar{x}+1$ to $\bar{y}$ (an element of L with the same irreducible polynomial) is therefore an isomorphism. In particular, since we found $\bar{x}+1$ to be a generator of $K^\times$, it should be the case that $\bar{y}$ is a generator of $L^\times$. Indeed, $\bar{y}^4 = (\bar{y}^2)^2 = (-\bar{y}+1)^2 = (-\bar{y}+1) + \bar{y} + 1 = -1$, so the multiplicative order of $\bar{y}$ is 8.

To compute this isomorphism explicitly, express a nonzero element α in K as a polynomial using powers of $\bar{x}+1$. This is always possible, at the very least by expressing α as a power of $\bar{x}+1$ using the fact that $\bar{x}+1$ is a multiplicative generator of $K^\times$. Then the image of this element is obtained by replacing all powers of $\bar{x}+1$ in this polynomial representation with a corresponding power of $\bar{y}$, keeping all coefficients the same.