

33. FINITE FIELDS

We will discuss the basic theoretical properties of finite fields, prove most of these properties and use them to deduce the precise structure of finite fields and to construct some of the classical finite simple groups.

The two basic properties of finite fields are the following. The first concerns the number of elements in a finite field.

- Theorem 33.1.** (1) *The number of elements of any finite field is a power of a prime number: $|F| = p^k$.*
 (2) *Every power of every prime is the order of some finite field.*
 (3) *Two finite fields with the same order are isomorphic.*

We will prove (1) using group theory.

This theorem tells us that there is a unique finite field for any power of any prime (up to isomorphism). This field is called the **Galois fields** $GF(q)$ where $q = p^k$. Today, we will deduce the exact structure of $GF(16)$ from the general theory.

The second main property of finite fields is Fermat's little theorem in the case of $GF(p) = \mathbb{Z}_p$.

- Theorem 33.2.** *The group of units of any finite field of order q is a cyclic group of order $q - 1$.*

We will prove this using polynomials with coefficients in the field F .

Problem: Using this theorem show that $GF(9)$ is not a subfield of $GF(27)$.

33.1. order of a field. I will explain the proof and the consequences of Theorem 33.1

Recall that the *characteristic* of a field is either prime or 0. A finite field F cannot have characteristic 0 so it has prime characteristic p . This means that

$$p \cdot x = \underbrace{x + x + \cdots + x}_p = 0$$

for every $x \in F$. In other words, every element of the additive group $(F, +)$ has order p (except for 0 which has order 1).

Lemma 33.3. *Suppose that G is a finite abelian group in which every nontrivial element has order p where p is a fixed prime. Then the order of G is a power of a prime.*

This is a simple induction on the order of G using the factor group

$$G/\langle g \rangle$$

for any nontrivial element $g \in G$.

Proof. The proof is by induction on $n = |G|$. Suppose that $|G| = n = 1$. Then $1 = p^0$ is a power of p so the theorem holds.

Now suppose that $n > 1$ and the theorem holds for all groups with fewer than n elements. Take $g \neq e$ in G . Then by assumption we have $o(g) = \langle g \rangle = p$. Since G is abelian, every subgroup is normal. So, we have a factor group $G/\langle g \rangle$ with order

$$|G/\langle g \rangle| = \frac{n}{p}$$

Claim Every nontrivial element of the factor group has order p .

Proof of Claim: Any element of the factor group has the form $hN = h\langle g \rangle$. So,

$$(h\langle g \rangle)^p = h^p \langle g \rangle = e \langle g \rangle = \langle g \rangle$$

which is the identity of $G/\langle g \rangle$. Since $g^n = e$ implies that $o(g)|n$, the calculation above implies that $o(h\langle g \rangle)$ is either p or 1. So, every nontrivial element of $G/\langle g \rangle$ has order p .

Getting back to the proof of the lemma,

$$|G/\langle g \rangle| = \frac{n}{p} = p^k \Rightarrow n = p^{k+1}$$

So, the lemma holds for G and we are done. \square

33.2. example: $GF(16)$. I will prove Theorem 33.2 next time. Today, I used it to construct $F = GF(16)$. Since $16 = 2^4$, we have $p = 2$. This implies that $x + x = 0$ for all $x \in F$. In other words, $x = -x$.

The theorem says that $GF(16)^\times = \langle x \rangle$ where x has multiplicative order 15: $x^{15} = 1$. Let $\alpha = x^3$. Then $\alpha^5 = 1$. Now, we represent elements of F as binary sequences with 4 binary digits. For example:

$$1010 = \alpha^3 + \alpha^2$$

This is *base* α . If we have more than 4 digits, we can contract using the formula:

Lemma 33.4.

$$\boxed{\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1}$$

Proof. We put everything on one side of the equation and multiply by $\alpha - 1 = \alpha + 1$:

$$(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)(\alpha - 1) = \alpha^5 - 1 = 0$$

This is a product of two elements of the field F . But $\alpha - 1 \neq 0$ since $\alpha = x^3$ and x has order 15. Therefore, the other factor must be zero since F has no zero divisors:

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$$

This implies that

$$\alpha^3 + \alpha^2 + \alpha + 1 = -\alpha^4 = +\alpha^4$$

since $+$ and $-$ are the same thing in characteristic 2. \square

Addition and multiplication of 4 digit sequences works like this:

$$\begin{array}{r} 1\ 0\ 1\ 0 \\ +\ 0\ 1\ 1\ 1 \\ \hline 1\ 1\ 0\ 1 \end{array}$$

The rule is: we add digits without carrying. These digits represent:

$$\begin{array}{r} \alpha^3 \qquad \qquad +\alpha \\ + \qquad \alpha^2 \quad +\alpha \quad +1 \\ = \alpha^3 \quad +\alpha^2 \qquad \quad +1 \end{array}$$

since $\alpha + \alpha = 0$.

Multiplication uses the boxed formula:

$$\begin{array}{r|l} & 1\ 0\ 1\ 0 \\ \times & 0\ 1\ 1\ 1 \\ \hline & 1\ 0\ 1\ 0 \\ 1 & 0\ 1\ 0 \\ 1\ 0 & 1\ 0 \\ \hline \alpha^4 & 1\ 1\ 1\ 1 \\ \alpha^5 & 0\ 0\ 0\ 1 \\ \hline & 1\ 0\ 0\ 0 \end{array}$$

Any digit beyond the first four can be shifted to the right since

$$1,0000 = \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1 = 1111$$

$$10,0000 = \alpha^5 = 1 = 0001$$

$$100,0000 = \alpha^6 = \alpha = 0010$$

Problem: Show that $1010^3 = 0010 = \alpha$ and 1010 has order 15.