

THE PRIMITIVE ROOT THEOREM

MATH 336, KEN BROWN

The proof of the primitive root theorem (Section 23A, p. 348) is hard to read because it relies on Section 9F, which we skipped. This handout gives a self-contained proof. We begin with some examples to illustrate the ideas.

Example 1. You learned about the field \mathbb{F}_9 in Section 8B, Exercise 7, where you showed by direct computation that $1 + i$ has order 8 and so is a primitive element. Here's a conceptual proof that a field F with 9 elements has to have an element of order 8. By the abstract Fermat theorem, every nonzero element $a \in F$ satisfies $a^8 = 1$; the possible orders of elements are therefore 1, 2, 4, and 8. The elements of order 1, 2, and 4 satisfy $a^4 = 1$, so there can't be more than 4 of them (they are roots of the polynomial $x^4 - 1$). The remaining nonzero elements have order 8.

This example was easy because the number of units was a prime power. The following lemma will help us handle more complicated cases.

Lemma 1. *Suppose a has order m and b has order n , with $(m, n) = 1$. Then ab has order mn .*

Proof. We're given $a^m = 1$ and $b^n = 1$, so $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1$. To see that there can't be a smaller exponent e such that $(ab)^e = 1$, observe that

$$(ab)^e = 1 \implies (ab)^{em} = 1 \implies b^{em} = 1 \implies n \mid em \implies n \mid e.$$

Similarly, $m \mid e$. So $mn \mid e$ and therefore $mn \leq e$. \square

Example 2. We will see later in the course that there is a field \mathbb{F}_{64} with 64 elements. Without knowing anything about how this field is constructed, let's show that it has to have an element of order 63. In view of the lemma, it suffices to find an element of order 9 and an element of order 7. We will get an element a of order 9 by setting $a = b^7$ for a suitably chosen $b \neq 0$. Regardless of how b is chosen, we will have $a^9 = b^{63} = 1$, so a will have order 1, 3, or 9. To make sure it has order 9, we need $a^3 \neq 1$, i.e., $b^{21} \neq 1$. This is easy to achieve, since no more than 21 of the 63 nonzero elements b can satisfy $b^{21} = 1$. A similar argument produces an element of order 7 as c^9 , where c is any nonzero element such that $c^9 \neq 1$.

The same method works in complete generality, once we observe that Lemma 1 extends to several factors:

Lemma 2. *Suppose a_1, a_2, \dots, a_n are elements whose orders m_1, m_2, \dots, m_n are pairwise relatively prime. Then $a_1 a_2 \cdots a_n$ has order $m_1 m_2 \cdots m_n$.*

Proof. We argue by induction on n . There's nothing to prove if $n = 1$, and we've already done the case $n = 2$. So assume that $n > 2$ and that the result is known for $n - 1$ factors. Then $a_1 \cdots a_{n-1}$ has order $m_1 \cdots m_{n-1}$, so $a_1 \cdots a_n = (a_1 \cdots a_{n-1})a_n$ has order $(m_1 \cdots m_{n-1})m_n$ by Lemma 1. \square

Date: April 2001.

We can now prove the primitive root theorem for any finite field by imitating the method of Example 2.

Theorem 1. *Every finite field F has a primitive root.*

Proof. Let N be the number of nonzero elements in F . In view of Lemma 2, it suffices to produce an element of order p^e for each prime power $q = p^e$ occurring in the prime factorization of N . Choose $b \neq 0$ in F so that $b^{N/p} \neq 1$; this is possible because the polynomial $x^{N/p} - 1$ can't have more than N/p roots. Let $a = b^{N/q}$. Then $a^q = 1$ by the abstract Fermat theorem, so a has order p^f for some $f \leq e$. We can't have $f < e$, because then p^f would divide $p^{e-1} = q/p$, implying $a^{q/p} = 1$; but $a^{q/p} = b^{N/p} \neq 1$. So $f = e$ and a has order $q = p^e$ as desired. \square

Note that this proof used very little from the theory of fields. The same method proves the following result:

Theorem 2. *Let G be a finite abelian group with the following property: For any positive integer m , there are at most m solutions of the equation $x^m = 1$. Then G is cyclic.* \square

Exercise. Where in the proof does one need the assumption that G is abelian?