The Multiplicative Group of a Finite Field

Math 430

The purpose of these notes is to give a proof that the multiplicative group of a finite field is cyclic, without using the classification of finite abelian groups. We need the following lemma, the proof of which we omitted from class.

**Lemma 1.** Suppose $G$ is an abelian group, $x, y \in G$, and $|x| = r$ and $|y| = s$ are finite orders. Then there exists an element of $G$ which has order $\text{lcm}(r, s)$.

**Proof.** Suppose first that $\gcd(r, s) = 1$, so that $\text{lcm}(r, s) = rs$. Given $x, y \in G$ such that $|x| = r$ and $|y| = s$, consider $z = xy \in G$. Since $z^rs = x^ry^s = e$, then $|z| \leq rs$. If $|z| = m$, then $z^m = e$, so $e = e^s = z^ms = x^msy^ms = x^ms$, since $y^s = e$. Since $x^ms = e$ and $|x| = r$, then $r|ms$, and $\gcd(r, s) = 1$, so $r|m$. Also $e = e^r = z^mr = x^my^mr = y^mr$, since $x^r = e$. Then since $|y| = s$ and $y^mr = e$, then $s|m$, so $s|m$. Now $r|m$ and $s|m$ implies $rs|m$ since $\gcd(r, s) = 1$. So $|z| = m \geq rs$. Now $|z| = rs = \text{lcm}(r, s)$.

We now consider the general case, where $\text{lcm}(r, s)$ is not necessarily $rs$. Given $|x| = r$ and $|y| = s$ in the abelian group $G$, it is not true in general that $xy$ will have order $\text{lcm}(r, s)$ (try to find a counterexample). We decompose the positive integer $r$ as a product $r = r_1r_2r_3r_4$ as follows:

- $r_1$ = the product of all prime factors of $r$ which are not prime factors of $s$,
- $r_2$ = the product of all prime factors which occur with equal powers in $r$ and $s$,
- $r_3$ = the product of all prime factors of $r$ which occur in $r$ and $s$, but in $r$ with higher powers,
- $r_4$ = the product of all prime factors of $r$ which occur in $r$ and $s$, but in $s$ with higher powers.

Define $s = s_1s_2s_3s_4$ analogously, with $r$ and $s$ in exchanged roles. Note that this means $s_2 = r_2$, and $\text{lcm}(r, s) = r_1r_2r_3s_1s_3$. If we define $\tilde{r} = r_1r_2r_3$ and
s = s_1s_3, then gcd(\tilde{r}, \tilde{s}) = 1, and lcm(\tilde{r}, \tilde{s}) = \tilde{r}\tilde{s} = r_1r_2r_3s_1s_3 = \text{lcm}(r, s).

For example, if r = 2^73^54^7 and s = 2^63^75^411^4, then r_1 = 7^4, r_2 = s_2 = 5^4, r_3 = 2^7, r_4 = 3^5, s_1 = 11^4, s_3 = 3^7, s_4 = 2^6, and so \tilde{r} = 7^45^42^7 and \tilde{s} = 11^43^7.

Now |x^{r_4}| = r/r_4 = r_1r_2r_3 = \tilde{r} and |y^{s_2s_4}| = s/s_2s_4 = s_1s_3 = \tilde{s}. If we take \tilde{x} = x^{r_4} and \tilde{y} = y^{s_2s_4}, then |\tilde{x}| = \tilde{r} and |\tilde{y}| = \tilde{s}, where gcd(\tilde{r}, \tilde{s}) = 1, so by the first part of the proof, |\tilde{x}\tilde{y}| = \tilde{r}\tilde{s}. That is, taking \tilde{z} = \tilde{x}\tilde{y}, we have \tilde{z} \in G with |\tilde{z}| = \tilde{r}\tilde{s} = \text{lcm}(r, s).

The above lemma is enough to prove the desired statement.

**Theorem 1.** Suppose \( F \) is a finite field. Then \( F^\times = F \setminus \{0\} \) is a cyclic group under multiplication.

**Proof.** Let \( |F^\times| = m \). Suppose \( \alpha \in F^\times \) has maximal possible order under multiplication over all elements of \( F^\times \), and call this order \( |\alpha| = k \). By Lagrange’s Theorem, \( k|m \), so in particular \( k \leq m \).

Let \( \beta \in F^\times \) be any element of \( F^\times \). If \( |\beta| = r \), then by Lemma ??, \( F^\times \) has some element of order \( \text{lcm}(r, k) \geq k \). Since \( k \) is the maximal order of all elements in \( F^\times \), then we must have \( \text{lcm}(r, k) = k \), which implies \( r|k \). Since \( |\beta| = r \) and \( r|k \), then we have \( \beta^k = 1 \). Since \( \beta \) was arbitrary, this means every element of \( F^\times \) is a zero of the polynomial \( x^k - 1 \in F[x] \), that is, \( x^k - 1 \) has \( m \) roots in \( F \). However, we’ve shown that a polynomial of degree \( d \) over some field has at most \( d \) roots in that field. That is, we must have \( m \leq k \).

That is, we have \( m = k \).

Now \( |\alpha| = m = |F^\times| \). Thus \( \langle \alpha \rangle = F^\times \) and \( F^\times \) is a cyclic group under multiplication. \( \square \)