Finite Subgroups of $F^*$

Mathematics 581, Fall 2012

In this note we give a proof that finite subgroups of the multiplicative group of a field are cyclic. Our approach is via elementary number theory and finite cyclic groups. Recall the Euler phi function, defined as

$$\phi(n) = |\{m \in \mathbb{N} : 1 \leq m \leq n, \gcd(m, n) = 1\}|$$

For example, $\phi(4) = 2$ and $\phi(6) = 2$ while $\phi(5) = 4$ and $\phi(12) = 4$. In addition, if $p$ is prime, then $\phi(p) = p - 1$ since the integers between 1 and $p$ and relatively prime to $p$ are $1, 2, \ldots, p - 1$.

The connection between the Euler phi function and finite cyclic groups is the following result.

**Lemma 1.** Let $A$ be a cyclic group of order $n$. Then $A$ has exactly $\phi(n)$ generators.

**Proof.** Let $A = \langle a \rangle$ be a cyclic group of order $n$. We have seen that $a^i$ is a generator for $A$ if and only if $\gcd(i, n) = 1$. Furthermore, $A = \{a^1, a^1, \ldots, a^n\}$. Thus, the generators of $A$ are the elements of the form $a^i$ with $1 \leq i \leq n$ and $\gcd(i, n) = 1$. Thus, $A$ has exactly $\phi(n)$ generators.

**Lemma 2.** Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be cyclic groups of orders $n$ and $m$, respectively. If $\gcd(n, m) = 1$, then $A \times B$ is cyclic, and the set of generators of $A \times B$ is $\{(a^i, b^j) : \gcd(i, n) = 1 = \gcd(j, m)\}$.

**Proof.** Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be cyclic groups of orders $n$ and $m$, respectively. Consider $C = A \times B$. We first show $C$ is a cyclic group by showing that it is generated by $(a, b)$. For, if $(x, y) \in C$, write $(x, y) = (a^i, b^j)$ for some $i, j$. Since $\gcd(n, m) = 1$, by the Chinese Remainder Theorem there is $r$ with $r \equiv i \pmod{n}$ and $r \equiv j \pmod{m}$. Then

$$(x, y) = (a^i, b^j) = (a^r, b^r) = (a, b)^r.$$ 

Thus, $C$ is cyclic. We next show that the set of generators of $C$ is

$$\{(a^i, b^j) : \gcd(i, n) = 1 = \gcd(j, m)\},$$
First, let \((a^i, b^j)\) be a generator of \(C\). Let \(a^k \in A\). Then \((a^k, 1) = (a^i, b^j)^l\) for some \(l\). Consequently, \(a^k = (a^i)^l\). This forces \(a^i\) to be a generator of \(A\), so \(\gcd(i, n) = 1\). Similarly, \(b^j\) is a generator of \(B\), so \(\gcd(j, m) = 1\). Conversely, let \(\gcd(i, n) = 1 = \gcd(j, m)\). Since \(\gcd(n, m) = 1\), we get \(\gcd(im, n) = 1\). Thus, there is \(t\) with \(imt \equiv 1 \pmod{n}\). Then \((a^i, b^j)^{mt} = (a^{imt}, b^{mnt}) = (a, 1)\). Similarly, \((1, b)\) is a power of \((a^i, b^j)\). Thus, \((a, b) = (a, 1) \cdot (1, b)\) is a power of \((a^i, b^j)\). Therefore \((a^i, b^j)\) generates \(C\). \(\Box\)

The assumption that \(\gcd(m, n) = 1\) is necessary in the result above. For example, \(\mathbb{Z}_2 \times \mathbb{Z}\) is not cyclic because each nonidentity element has order 2. More generally, if \(l = \text{lcm}(n, m)\), then \(l < nm\) if \(\gcd(n, m) \neq 1\), and \(A, B\) are cyclic of order \(n, m\), it is not hard to show that each element of \(A \times B\) has order dividing \(l\), so \(A \times B\) is not cyclic.

The following lemma gives two properties of the Euler phi function. The proof will show that they are really consequences of the structure of finite cyclic groups. Lemma 1 allows us to interpret \(\phi(n)\) as the number of generators of a cyclic group of order \(n\).

**Lemma 3.** Let \(\phi\) be the Euler phi function.

1. For each positive integer \(n\) we have \(\sum_{m|n} \phi(m) = n\).

2. If \(\gcd(n, m) = 1\), then \(\phi(nm) = \phi(n)\phi(m)\).

**Proof.** (a) Let \(A = \langle a \rangle\) be a cyclic group of order \(n\). We have seen that for each \(m \mid n\), the cyclic group \(A\) has a unique subgroup of order \(m\), and this is \(\langle a^d \rangle\) if \(n = md\). Each element of \(A\) of order \(m\) is then inside this cyclic subgroup. Thus, the number of elements of order \(m\) is the number of generators of \(\langle a^d \rangle\), which is \(\phi(m)\) by Lemma 1. Since \(|A|\) is the sum, over all \(m \mid n\) of the number of elements of order \(m\), we see that \(n = \sum_{m|n} \phi(m)\).

(b) Suppose that \(\gcd(n, m) = 1\). If \(A\) and \(B\) are cyclic groups of order \(n, m\), respectively, then by Lemma 2, \(A \times B\) is a cyclic group of order \(nm\). Also, by that lemma, the number of generators of \(A \times B\) is \(\phi(n)\phi(m)\). However, the number of generators is \(\phi(nm)\) by Lemma 1. Thus, \(\phi(nm) = \phi(n)\phi(m)\). \(\Box\)

**Lemma 4.** Let \(F\) be a field. Then \(F\) has at most \(n\) elements with \(a^n = 1\).

**Proof.** If \(a \in F\) satisfies \(a^n = 1\), then \(a\) is a root of \(x^n - 1\). Moreover, \(x - a\) then divides \(x^n - 1\). If there are distinct elements \(a_1, \ldots, a_m \in F\) with \(a_i^n = 1\) for each \(i\), then each \(x - a_i\) divides \(x^n - 1\). because these are distinct irreducible polynomials, we get \((x - a_1) \cdots (x - a_m)\) divides \(x^n - 1\). Comparing degrees, we get \(m \leq n\). \(\Box\)

**Theorem 5.** Let \(G\) be a finite subgroup of the multiplicative group \(F^*\) of a field \(F\). Then \(G\) is cyclic.

**Proof.** Set \(n = |G|\). For each integer \(m\), let \(S_m\) be the set of elements of \(G\) of order \(m\). Then \(S_1 = \{1\}\), and \(S_n \neq \emptyset\) if and only if \(G\) is cyclic. By Lagrange’s theorem, \(S_m = \emptyset\) when \(m\) does not divide \(n\). Since each element of \(G\) has order dividing \(n\), by Lagrange, we have

\[
G = \bigcup_{m|n} S_m.
\]
Because the sets $S_m$ are pairwise disjoint, we then have $n = |G| = \sum_{m \mid n} |S_m|$. Note also that since each element $a \in S_m$ is a root of $x^m - 1$. In fact, if we write $x^m - 1 = (x-1)g(x)$ for some $g(x)$, when $m > 1$, we see that each element of $S_m$ is a root of $g(x)$. Therefore, $|S_m| \leq m - 1$ by Lemma 4.

We prove, by induction, that $|S_m| \leq \phi(m)$. The case $m = 1$ holds since $|S_1| = 1 = \phi(1)$. The result also holds if $m$ is prime, since if so, then $\phi(m) = m - 1$ and we saw above that $|S_m| \leq m - 1$. Now, assume that $m > 1$ and that the result holds for all integers smaller than $m$. Again, if $m$ is prime, then the result holds. So, suppose that $m$ is not prime. We may write $m = kl$ for some integers $k, l$ with $\gcd(k, l) = 1$. Consider the function $\sigma : S_m \to S_k \times S_l$ defined by $\sigma(x) = (x^k, x^l)$. Note this is well defined because if the order of $x$ is $m$, then the order of $x^k$ (resp. $x^l$) is $k$ (resp. $l$). We next see that $\sigma$ is 1-1. For, if $x, y \in S_m$ with $(x^k, x^l) = (y^k, y^l)$, then $x^k = y^k$ and $x^l = y^l$. Because $\gcd(k, l) = 1$, we may write $1 = rl + sk$ for some integers $r, s$. Then

$$x = x^{rk+sl} = (x^k)^r (x^l)^s = (y^k)^r (y^l)^s = y.$$ 

Therefore, $|S_m| \leq |S_k \times S_l| = |S_k| \cdot |S_l|$. By induction, we then get $|S_m| \leq \phi(k)\phi(l) = \phi(kl) = \phi(m)$ by Lemma 3. Thus, the result follows by induction.

To finish the proof, we have $n = |G| = \sum_{m \mid n} |S_m|$. By what we just proved, $|S_m| \leq \phi(m)$. Thus,

$$n = \sum_{m \mid n} |S_m| \leq \sum_{m \mid n} \phi(m) = n$$

by Lemma 3. Thus, we must have equality everywhere, so $|S_m| = \phi(m)$ for each $m \mid n$. In particular, $|S_n| = \phi(n) > 0$, so $S_n$ is nonempty. Thus, $G$ has an element of order $n$. Because $|G| = n$, this means $G$ is cyclic. 

\[\square\]

An alternate approach

We give a different proof of the main theorem of this note. It is less number-theoretic in nature. It introduces a concept called the exponent of a group.

**Definition 6.** Let $G$ be a finite group. The exponent of $G$, denoted $\exp(G)$, is the least common multiple of the orders of all the elements of $G$.

**Example 7.** Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. The orders of elements of $G$ are either 1 or 2, so $\exp(G) = 2$. More generally, if $G = \mathbb{Z}_n \mathbb{Z}_n$, then $\exp(G) = n$.

**Example 8.** The orders of elements of $S_3$ are 1, 2, 3, so $\exp(S_3) = 6$. Similarly, the orders of elements of $D_4$ are 1, 2, 4, so $\exp(D_4) = 4$.

By Lagrange’s theorem, each element of a finite group $G$ has order dividing $|G|$. Thus, $\exp(G)$ divides $|G|$. If $G = \langle g \rangle$ is a cyclic group of order $n$, then $g$ has order $n$. This implies that $\exp(G) = n = |G|$. The main result of this section is a converse for Abelian groups.
That is, we will prove that an Abelian group $G$ is cyclic if and only if $\exp(G) = |G|$. Note that the Abelian hypothesis is necessary, since $\exp(S_3) = |S_3|$ but $S_3$ is not cyclic.

**Lemma 9.** Let $G$ be an Abelian group and let $a, b \in G$. Suppose that $o(a) = n$ and $o(b) = m$ with $\gcd(n, m) = 1$. Then $o(ab) = nm$.

**Proof.** Because $G$ is Abelian, $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e$. Thus, $o(ab)$ divides $nm$. Let $t = o(ab)$. Then $(ab)^t = e$, which yields $a^t = b^{-t}$. In particular, $a^{tm} = b^{-tm} = e$ since $o(b) = m$. Now, since $\gcd(n, m) = 1$, we may write $1 = rn + sm$ for some $r, s \in \mathbb{Z}$. Thus, $t = trn + stm$. Therefore, as $a^{tm} = e = a^n$, we see that $a^{stm} = e = a^{trn}$, so $a^t = e$. This forces $n \mid t$. Similarly, $m \mid t$. Thus, $nm \mid t$ because $\gcd(n, m) = 1$. We have thus proven that $nm$ divides $t$ and $t$ divides $nm$. Therefore, $t = nm$. \qed

**Lemma 10.** Let $G$ be an Abelian group and let $a, b \in G$. Suppose that $o(a) = n$ and $o(b) = m$. If $l = \text{lcm}(n, m)$, then there is $c \in G$ with $o(c) = l$.

**Proof.** We may write $n = p_1^{e_1} \cdots p_r^{e_r}$ and $m = p_1^{f_1} \cdots p_r^{f_r}$ for some distinct primes $p_1, \ldots, p_r$ and integers $e_i, f_i \geq 0$. If $s_i = \max\{e_i, f_i\}$, then $l = p_1^{s_1} \cdots p_r^{s_r}$. For each $i$ set $n_i = n/p_i^{e_i}$. Since $o(a) = n$, the order of $a^{n_i}$ is $p_i^{e_i}$. Similarly, an appropriate power of $b$ has order $p_i^{f_i}$. Thus, for each $i$, we may find an element $c_i$ of order $p_i^{s_i}$. Set $c = c_1 \cdots c_r$. Then by induction and the previous lemma, $o(c) = l$. \qed

**Theorem 11.** Let $G$ be a finite Abelian group. Then $G$ is cyclic if and only if $\exp(G) = |G|$.

**Proof.** One direction of this was noted earlier. For the converse, suppose that $\exp(G) = |G|$. By the previous lemma and induction, there is an element $g \in G$ of order $\exp(G)$. Thus, since $\exp(G) = |G|$, we see that $G = \langle g \rangle$, so $G$ is cyclic. \qed

**Corollary 12.** Let $F$ be a field and let $G$ be a finite subgroup of $F^*$. Then $G$ is cyclic.

**Proof.** Since $G$ is finite Abelian, the previous result applies, so it is enough to prove that $\exp(G) = |G|$. Let $\exp(G) = m$ and $|G| = n$. Then each element of $G$ has order dividing $m$, by definition of the exponent. Thus, $g^m = 1$ for each $g \in G$. Therefore, each element of $G$ is a root of $x^m - 1$. This forces $|G| \leq \deg(x^m - 1) = m$, so $n \leq m$. But, by Lagrange, $m$ divides $n$, so $m \leq n$. Thus, $m = n$. \qed