CRYPTOGRAPHY TOPIC IX
THE MULTIPLICATIVE GROUP
OF A FINITE FIELD

PAUL L. BAILEY

Abstract. We show that the multiplicative group of a finite field is cyclic.

1. Least Common Multiple

Definition 1. Let m and n be positive integers. The *least common multiple* of m and n, denoted $\operatorname{lcm}(m,n)$, is the unique positive integer l satisfying

(a) $m \mid l$ and $n \mid l$;
(b) $m \mid k$ and $n \mid k$ implies $l \mid k$.

Proposition 1. *Let m and n be positive integers. Then*

$$\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)}.$$

Proof. Let $d = \gcd(m,n)$ and $l = \frac{mn}{d}$; we wish to show that l is the least common multiple for m and n. Since $d = \gcd(m,n)$, $\frac{m}{d}$ and $\frac{n}{d}$ are integers, and $l = m\frac{n}{d} = n\frac{m}{d}$. Thus $m \mid l$ and $n \mid l$.

Now suppose that k is an integer such that $m \mid k$ and $n \mid k$; we wish to show that $l \mid k$. We have $k = mx$ and $k = ny$ for some $x, y \in \mathbb{Z}$. Thus $mx = ny$, and dividing by d gives $\frac{m}{d}x = \frac{n}{d}y$. Thus $\frac{n}{d} \mid \frac{m}{d}x$, and since $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$, we have $\frac{n}{d} \mid x$. Thus $x = \frac{n}{d}z$ for some $z \in \mathbb{Z}$, so $k = mx = \frac{mn}{d}z = lz$. Thus $l \mid k$, which shows that l is a least common multiple of m and n. □

2. The Order of Commuting Elements

Proposition 2. *Let G be a group with $a, b \in G$. Let $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$, where $m, n \in \mathbb{Z}$. Suppose that $ab = ba$ and $\gcd(m,n) = 1$. Then $\operatorname{ord}(ab) = mn$.*

Proof. Since a and b commute, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1^n \cdot 1^m = 1$; thus $\operatorname{ord}(ab) \mid mn$.

Since $\gcd(m,n) = 1$, there exist $x, y \in \mathbb{Z}$ such that $mx + ny = 1$. Now

$$(ab)^{ny} = a^{ny}b^{ny} = a^{ny} = a^{mx}a^{ny} = a^{mx+ny} = a,$$

a is a power of ab, so $m \mid \operatorname{ord}(ab)$. Similarly, $n \mid \operatorname{ord}(ab)$.

Thus $\operatorname{lcm}(m,n) \mid \operatorname{ord}(ab)$. By Proposition 1, $\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = mn$, so $mn \mid \operatorname{ord}(ab)$. Therefore $\operatorname{ord}(ab) = mn$. □

Date: December 11, 2007.

3. Cauchy's Theorem for Abelian Groups

Cauchy's Theorem states that if p is prime, then a finite group G has an element of order p if and only if p divides the order of G. That the order of an element divides the order of the group is a consequence of LaGrange's Theorem. It is the reverse direction we wish to show. Although this is true for finite groups in general, we will only show it for abelian groups, as the proof in general is significantly deeper.

Proposition 3. *Let G be a finite abelian group of order $m \in \mathbb{N}$.*
Let $m \in \mathbb{Z}$ with $\gcd(m, n) = 1$.
Then the power map $\phi : G \to G$ given by $g \mapsto g^n$ is bijective.

Proof. Suppose $\phi(g) = 1$, so that $g^n = 1$. Then the order of g divides n. Also the order of g divides the order of the group by LaGrange's Theorem. But this says that the order of g divides $\gcd(m, n) = 1$, so the order of g is 1, and $g = 1$.

Now suppose that $\phi(g_1) = \phi(g_2)$. Then $g_1^n = g_2^n$, and since G is abelian, $(g_1 g_2^{-1})^n = 1$. Thus $g_1 g_2^{-1} = 1$ by the previous paragraph, so $g_1 = g_2$. This shows that ϕ is injective, and since G is finite, ϕ is surjective. □

Proposition 4. *Let G be a finite abelian group and let p be a prime integer.*
If p divides the order of G, then G has an element of order p.

Proof. Suppose that p divides the order of G. By induction on $|G|$, we may assume that if p divides the order of any abelian group whose order is less than $|G|$, then that group has an element of order p.

Let the order of G be pm for some $m \in \mathbb{Z}$. Let $k \in G$ be a element which is not the identity. If $\text{ord}(k) = pn$ for some $n \leq m$, then then k^n has order p and we are done. Thus we suppose that p does not divide the order of k. Let H be the cyclic subgroup generated by k. Then p does not divide the order of H, and since G is abelian, H is normal.

Thus p divides the order of the group G/H. By induction, we assume that G/H has an element gH of order p. Then $(gH)^p = g^p H = H$, so $g^p k^n = 1$ for some $k^n \in H$. By Proposition 3, there exists $h \in H$ such that $h^p = k^n$. Then $(gh)^p = 1$. Since $g \notin H$, $gh \neq 1$. Thus $\text{ord}(gh) = 1$. □

4. p-Torsion Subgroups

Definition 2. Let G be an abelian group and let p be a positive prime integer. The *p-Torsion subgroup* of G is

$$T_p(G) = \{g \in G \mid g^{p^r} = 1 \text{ for some } r \in \mathbb{N}\}.$$

Proposition 5. *Let G be an abelian group, and let p be a positive prime integer. Then $T_p(G) \leq G$.*

Proof. We verify the three properties of being a subgroup.

(S0) Since $1^p = 1$, $1 \in T_p(G)$.

(S1) Let $a, b \in T_p(G)$. Then $a^{p^r} = 1$ and $b^{p^s} = 1$, for some $r, s \in \mathbb{N}$. Let $t = \max\{r, s\}$, and let $n = p^t$. Since a and b commute, $(ab)^{=}a^n b^n = 1 \cdot 1 = 1$, so $ab \in T_p(G)$.

(S2) Let $a \in T_{p^*}(G)$. Then $a^{p^r} = 1$ for some $r \in \mathbb{N}$. Let $n = p^r$. Then $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$, so $a^{-1} \in T_p(G)$.

Thus $T_p(G) \leq G$. □

Proposition 6. *Let G be a finite abelian group, and let p be a positive prime integer. Let p^r be the highest power of p which divides $|G|$. Then $|T_p(G)| = p^r$.*

Proof. By the Fundamental Theorem of Arithmetic, there exists $m, r \in \mathbb{Z}$ with $|G| = p^r m$ and $\gcd(m, p) = 1$. By LaGrange's Theorem, $|G| = |T_p(G)|[G : T_p(G)]$. We wish to show that $|T_p(G)| = p^r$.

Firstly, we show that $|T_p(G)|$ is a power of p. Let q be a prime which divides $|T_p(G)|$. Then by Proposition 4, $T_p(G)$ has an element of order q. But the order of this element is a power of p, so we must have $q = p$. Thus p is the only prime which divides the order of $T_p(G)$, so this order is a power of p.

Secondly, we show that $[G : T_p(G)]$ is relatively prime to p. Suppose that p divides $[G : T_p(G)]$. Since G is abelian, $T_p(G)$ is a normal subgroup of G, so $G/T_p(G)$ is a group. Clearly $|G/T_p(G)| = [G : T_p(G)]$, so p divides $|G/T_p(G)|$, so (again by Proposition 4), $G/T_p(G)$ has an element of order p, say $\overline{g} = gT_p(G)$ for some $g \in G \smallsetminus T_p(G)$. Then $\overline{g}^p = \overline{1}$, so $g^p \in T_p(G)$. Thus the order of g^p is a power of p, which implies that $g \in T_p(G)$, which in turn implies that $\operatorname{ord}(\overline{g}) = 1$. This contradiction proves the claim. □

Proposition 7. *Let F be a field and let G be a finite subgroup of F^*. Let p be a positive prime which divide $|G|$. Then $T_p(G)$ is cyclic.*

Proof. Let p^s be the highest power of p such that G contains an element of order p^s. If $g \in T_p(G)$, then $g^{p^s} = 1$. Moreover, there exists an elements $h \in T_p(G)$ such that $\operatorname{ord}(h) = p^s$, so $|T_p(G)| \geq p^s$.

Let $f \in F[x]$ be given by $f(x) = x^{p^s} - 1$. Every member of $T_p(G)$ is a zero of f. By the Bound on Roots Theorem, f has at most p^s zeros in F, so $|T_p(G)| \leq p^s$. Thus $|T_p(G)| = p^s$, so $T_p(G)$ is cyclic of order p^s generated by h. □

5. Finite Fields are Cyclic

Proposition 8. *Let F be a finite field. Show that F^* is cyclic.*

Proof. Let $G = F^*$. Now $|G| = n = \prod_{i=1}^k p_i^{r_i}$, where $p_1, \dots, p_k$ are distinct primes. By Proposition 6, $T_{p_i}(G) = p_i^{r_i}$. By Proposition 7, there exist elements $g_i \in G$ with $\operatorname{ord}(g_i) = p_i^{r_i}$. By Proposition 2 and induction, $g = \prod_{i=1}^k g_i$ has order n. Thus $G = \langle g \rangle$. □

As an application of Proposition 8, we prove Wilson's Theorem.

Proposition 9. *Let G be a cyclic group of even order. Then G contains exactly one element of order two.*

Proof. Let $n = \operatorname{ord}(g)$. Since n is even, $n = 2m$ for some $m \in \mathbb{Z}$, and $\gcd(m, n) = m$, so

$$\operatorname{ord}(g^m) = \frac{n}{\gcd(m,n)} = \frac{n}{m} = 2.$$

To show uniqueness, let $k \in \mathbb{Z}$ with $0 < k < n$. Suppose that $\operatorname{ord}(g^k) = 2$; Then $1 = (g^k)^2 = g^{2k}$, which implies that $n \mid 2k$, so $2m \mid 2k$, so $m \mid k$. But $m \leq k < 2m$ implies that $1 \leq \frac{k}{m} < 2$; since $\frac{k}{m}$ is an integer, we have $1 = \frac{k}{m}$, so $k = m$. □

Proposition 10 (Wilson's Theorem)**.** *Let p be a positive prime integer. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. In any finite abelian group G, only elements of order two are there own inverses. Thus, if we take the product of all element in G, we obtain the product of the elements of order two, because the other element cancel each other.

Note that $\mathbb{Z}_p$ is a field. By the previous problem, $G = \mathbb{Z}_p^*$ is cyclic. By Proposition 9, G has a unique element of order two. This element is $\overline{p-1}$. Every other element of G has an inverse which is distinct from it; thus $\prod_{g \in G} g = p - 1$. But $\prod_{g \in G} g = \overline{(p-1)!}$. The result follows. □

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: `plbailey@saumag.edu`