CYCLIC UNIT GROUPS

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

The goal of this handout is to prove that if p is a prime, then the unit group $U_p = \left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\}$ is a cyclic group. Its generators are called *primitive elements*.

1. Orders

Let U_m be the unit group modulo m.

Definition 1. The *order* of an element $\overline{a} \in U_m$ is defined to be the smallest positive integer k such that $\overline{a}^k = \overline{1}$. Such integers exist since $\overline{a}^{\varphi(n)} = \overline{1}$ by Euler's Theorem, so there is a smallest such integer.

Remark. There are two *order* concepts used in this class, and they are much different. One concerns the power of p occurring in $a \in \mathbb{Z}$, while the other concerns $\overline{a} \in U_m$. So when we are talking about units in U_m you can be sure that we mean Definition 1. Definition 1 is used in more generally in group theory.

Proposition 1. *Let $\overline{a} \in U_m$ have order k. Then $\overline{a}^n = \overline{1}$ if and only if $k \mid n$. (This is valid for any $n \in \mathbb{Z}$, not just $n > 0$).*

Proof. First suppose $\overline{a}^n = \overline{1}$. Write $n = qk + r$ where $0 \le r < k$. Then

$$\overline{1} = (\overline{a})^n = (\overline{a})^{qk+r} = (\overline{a})^{qk}(\overline{a})^r = \left(\overline{a}^k\right)^q(\overline{a})^r = \overline{1}^q\overline{a}^r = \overline{a}^r.$$

But k is defined as the smallest positive integer with the desired property. So $r = 0$. Thus k divides n.

Now suppose $k \mid n$. Then $n = qk$ for some q. So $\overline{a}^n = (\overline{a}^k)^q = \overline{1}^q = \overline{1}$. $\square$

By Euler's Theorem we get the following.

Corollary 1. *Let $\overline{a} \in U_m$ have order k. Then $k \mid \varphi(m)$.*

If an element $\overline{a} \in U_m$ has order exactly $\varphi(m)$ then we say that $\overline{a}$ is a *generator* or *primitive element* modulo m, and U_m is called a *cyclic group*.

Proposition 2. *Let $\overline{a} \in U_m$ have order k. Then $\overline{a}^s = \overline{a}^t$ if and only if $s \equiv t \bmod k$.*

Proof. If $\overline{a}^s = \overline{a}^t$ then $\overline{a}^{s-t} = \overline{1}$. Then $k \mid s - t$ by Proposition 1. So $s \equiv t \bmod k$.

Conversely, if $s \equiv t \bmod k$ then $k \mid s - t$. So $\overline{a}^{s-t} = \overline{1}$ by Proposition 1. Multiply both sides of the equation by $\overline{a}^t$. This results in $\overline{a}^s = \overline{a}^t$. $\square$

Date: Fall 2005. Version of November 4, 2005.

2. An Application

In class we proved the following:

Theorem 1. *Let a/b be a rational number in lowest terms with $(b, 10) = 1$ and $b > 1$. Then the decimal expansion of a/b is periodic (after the decimal point) with period equal to the order of $\overline{10}$ in U_b.*

Remark. The element $\overline{10}$ occurs because we use base 10. We could generalize the above to base B by changing $\overline{10}$ to $\overline{B}$, and by making other obvious changes.

This theorem generalizes to denominators with $(b, 10) > 1$.

Theorem 2. *Let a/b be a rational number in lowest terms with positive b. Write $b = 2^s 5^t b_0$ where $(b_0, 10) = 1$. If $b_0 = 1$ then a/b has a finite decimal expansion. If $b_0 > 1$ then the decimal expansion of a/b is periodic (after some digit) with period equal to the order of $\overline{10}$ in U_{b_0}.*

3. Some Basic Facts

Let U_m be the unit group modulo m. Below are some basic facts about orders of elements of U_m. Actually these results apply to any Abelian group.

Proposition 3. *If $\overline{a} \in U_m$ has order k, and if $d \mid k$, then $\overline{a}^d$ has order k/d.*

Proof. Let k' be the order of $\overline{a}^d$. Observe that $\overline{1} = \left(\overline{a}^d\right)^{k'} = (\overline{a})^{k'd}$. Since k is the order of $\overline{a}$, this implies that $k \le k'd$. So $k' \ge k/d$.

Observe that $\left(\overline{a}^d\right)^{k/d} = \overline{a}^k = \overline{1}$. So $k' \le k/d$ since k' is the order of $\overline{a}^d$. Thus $k' = k/d$. □

Proposition 4. *Suppose $\overline{a} \in U_m$ has order k_1 and $\overline{b} \in U_m$ has order k_2. If $(k_1, k_2) = 1$ then $\overline{ab}$ has order $k_1 k_2$*

Proof. Let k be the order of $\overline{ab}$. First observe that

$$\left(\overline{ab}\right)^{k_1k_2} = (\overline{a})^{k_1k_2}\left(\overline{b}\right)^{k_1k_2} = \left(\overline{a}^{k_1}\right)^{k_2}\left(\overline{b}^{k_2}\right)^{k_1} = \left(\overline{1}\right)^{k_2}\left(\overline{1}\right)^{k_1} = \overline{1}.$$

By Proposition 1, $k | k_1 k_2$.

Now observe that

$$\left(\overline{ab}\right)^{k_1k} = (\overline{a})^{k_1k}\left(\overline{b}\right)^{k_1k} = \left(\overline{a}^{k_1}\right)^{k}\left(\overline{b}\right)^{k_1k} = \left(\overline{1}\right)^{k_2}\left(\overline{b}\right)^{k_1k} = \left(\overline{b}\right)^{k_1k}$$

and

$$\left(\overline{ab}\right)^{k_1k} = \left(\overline{ab}^{k}\right)^{k_1} = \overline{1}^{k_1} = \overline{1}.$$

So $\left(\overline{b}\right)^{k_1k} = \overline{1}$. Again, by Proposition 1, $k_2 \mid k_1 k$. Since $(k_1, k_2) = 1$, it follows that $k_2 \mid k$. By a similar argument $k_1 \mid k$.

Since $k_1 \mid k$ and $k_2 \mid k$, and since $(k_1, k_2) = 1$, it follows that $k_1 k_2 | k$.

Since $k_1 k_2 \mid k$ and $k \mid k_1 k_2$, it follows that $k = k_1 k_2$. □

Remark. Bezout's Identity can be used to prove that if $k_2 \mid k_1 k$ and $(k_1, k_2) = 1$, then $k_2 \mid k$.

See the handout on the Chinese Remainder Theorem for the proof that that $k_1 \mid k$ and $k_2 \mid k$, together with $(k_1, k_2) = 1$, imply $k_1 k_2 \mid k$.

Proposition 5. *Suppose $\overline{a_1}, \ldots, \overline{a_r} \in U_m$ have orders $n_1, \ldots, n_r$ respectively. Suppose also that the n_i are pairwise relatively prime. Then $\overline{a_1 \cdots a_r}$ has order $n_1 \cdots n_r$.*

Proof. This follows from Proposition 4 with the use of a short induction proof (in r). I will leave the details to you. □

4. The Primitive Element Theorem

Lemma 1. *Let $p > 2$ be a prime, and let $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of $p-1$ into powers of distinct primes. Then the order of each element $\overline{a} \in U_p$ is $q_1^{c_1} \cdots q_r^{c_r}$ where $c_i \le e_i$ for each i.*

Proof. This follows from Corollary 1. □

Lemma 2. *Let $p > 2$ be a prime, and let $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of $p-1$ into powers of distinct primes. Then for each i there is an element $\overline{a_i} \in U_p$ whose order is a multiple of $q_i^{e_i}$.*

Proof. We prove this for $i = 1$, the argument for general i is similar. So suppose the lemma fails for $i = 1$. Then every element of U_p has order $q_1^{c_1} \cdots q_r^{c_r}$ with $c_1 \le e_1 - 1$ and $c_j \le e_j$ for $j > 1$. In other words, every element has order dividing $(p-1)/q_1 = q_1^{e_1 - 1} \cdots q_r^{e_r}$. Let $d = (p-1)/q_1$. Then every element of U_p is a root of $x^d - \overline{1}$. However, by Lagrange's theorem on roots of polynomials, there are at most d roots. This is a contradiction since U_p has $p-1$ elements and $p - 1 > d$. □

Lemma 3. *Let $p > 2$ be a prime, and let $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of $p-1$ into powers of distinct primes. Then for each i there is an element $\overline{a_i} \in U_p$ of order $q_i^{e_i}$.*

Proof. By the previous lemma there is an element $\overline{b_i} \in U_p$ of order $q_i^{e_i} k$ for some k. Let $\overline{a_i} = \overline{b_i}^k$. By Proposition 3, $\overline{a_i}$ has order $q_1^{e_1}$. □

Theorem 3. *Let p be a prime. Then U_p has an element of order $\varphi(p) = p - 1$.*

Proof. If $p = 2$ then the result is trivial. So we can assume that $p > 2$. Let $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of $p - 1$ into powers of distinct primes. By the previous lemma there is, for each i, an element $\overline{a_i} \in U_p$ of order $q_i^{e_i}$. By Proposition 5 the element $\overline{a_1 \cdots a_r}$ has order $p - 1$. □

Definition 2. An element of U_m of order $\varphi(m)$ is called a *generator* or *primitive element*. The above theorem says that if $m = p$ is a prime then there are primitive elements. This theorem generalizes to other m including powers of primes $p > 2$. However, many U_m do not have primitive elements. For example, every element of U_8 has order 1 or 2, but $\varphi(8) = 4$. So U_8 has no primitive element.

The following theorem justifies the term *generator*.

Theorem 4. *If $\overline{a}$ is a primitive element of U_m then every element of U_m is a power of $\overline{a}$. In fact,*

$$U_m = \left\{ \overline{a}^0, \overline{a}^1, \overline{a}^2, \ldots \overline{a}^{\varphi(m)-1} \right\}.$$

Proof. Let $\overline{a}$ be a primitive element of U_m. In other words $\overline{a}$ has order $\varphi(m)$. Suppose that two elements on the list $\overline{a}^0, \overline{a}^1, \overline{a}^2, \ldots \overline{a}^{\varphi(m)-1}$ are equal: $\overline{a}^i = \overline{a}^j$. By Proposition 2, this implies that $i \equiv j \bmod \varphi(m)$ which cannot happen since i and j are between 0 and $\varphi(m) - 1$.

Thus $\overline{a}^0, \overline{a}^1, \overline{a}^2, \ldots \overline{a}^{\varphi(m)-1}$ gives us $\varphi(m)$ distinct elements of U_m. Recall that U_m only has $\varphi(m)$ elements, so this list gives us all elements of U_m. □

Definition 3. If U_m has a primitive element (or generator), then we say that U_m is a *cyclic group*.

Remark. By Theorem 3, U_p is cyclic if p is a prime. However, U_8 is not cyclic.

Remark. The term *cyclic* refers to the fact that powers of the generator $\overline{a}$ cycles through all the elements of the group.

Remark. The term *cyclic group* applies to any finite group such that powers of a designated element give all elements of the group.

To summarize,

Theorem 5. *If p is a prime, then U_p is a cyclic group. There is at least one element (usually several) $\overline{a} \in U_p$ that has order $p - 1$. For any such element*

$$U_p = \left\{ \overline{a}^0, \overline{a}^1, \overline{a}^2, \ldots \overline{a}^{p-2} \right\}$$

so every element of U_p is a power of $\overline{a}$.

Dr. Wayne Aitken, Cal. State, San Marcos, CA 92096, USA
E-mail address: waitken@csusm.edu