Notes on Cyclic Groups

09/13/06 Radford (revision of same dated 10/07/03)

$\boldsymbol{Z}$ denotes the group of integers under addition.

Let G be a group and $a \in G$. We define the power a^n for non-negative integers n inductively as follows: $a^0 = e$ and $a^n = aa^{n-1}$ for $n > 0$. If n is a negative integer then $-n$ is positive and we set $a^n = (a^{-1})^{-n}$ in this case. In this way a^n is defined for all integers n.

The familiar exponent laws

$$a^{m+n} = a^m a^n, \qquad (a^m)^n = a^{mn}$$

for all $m, n \in \boldsymbol{Z}$ and

$$(a^n)^{-1} = a^{-n}$$

for all $n \in \boldsymbol{Z}$ hold. If $b \in G$ and $ab = ba$ then $(ab)^n = a^n b^n$ for all $n \in \boldsymbol{Z}$. For the fourth exponent law to hold necessarily $ab = ba$. The proofs of the exponent laws are good exercises in induction. As a consequence of the first and third exponent laws

$$<a> = \{a^k \mid k \in \boldsymbol{Z}\}$$

is a (abelian) subgroup of G. From this point on we will use the exponent laws without particular reference.

The group G is *cyclic* if $G = <a>$ for some $a \in G$ in which case a is said to *generate* G. Since $<a> = <a^{-1}>$ for all $a \in G$, if G is cyclic and generated by a then G is also generated by a^{-1}.

Suppose that the binary operation of G is written *additively*. Then the notation $n{\cdot}a$, or na, is used instead of a^n and $n{\cdot}a$ is referred to as a multiple. The definitions of multiples read $0{\cdot}a = 0$ and $n{\cdot}a = a + (n-1){\cdot}a$ for all $n > 0$. If $n < 0$ we set $n{\cdot}a = (-n){\cdot}(-a)$. When $G = \mathbf{Z}$ observe that $n{\cdot}a = na$ is the product of the integers n and a.

The study of cyclic groups is based on one particular case.

Proposition 1 *Every subgroup of $\boldsymbol{Z}$ is cyclic. In particular, if H is a non-zero subgroup of $\boldsymbol{Z}$ then H contains a positive integer and is generated by the smallest positive integer in H.*

PROOF: The zero subgroup $(0) := <0> = \{0\}$ is cyclic. We may assume that $H \neq (0)$. In this case there is a non-zero integer k in H. Since H is a subgroup of $\boldsymbol{Z}$ the additive inverse $-k$ must be in H as well. One of k and $-k$ is positive. Therefore H contains a positive integer.

Let S be the set of all positive integers in H. We have shown $S \neq \emptyset$. By the Well-Ordering Principle there is a smallest positive integer n in S. Since $n \in H$ the cyclic subgroup $<n> = \{qn \,|\, q \in \boldsymbol{Z}\}$ of $\boldsymbol{Z}$ is a subset of H. We wish to show that $H = <n>$. Since $<n> \subseteq H$ we need only show that $H \subseteq <n>$.

Suppose that $a \in H$. By the Division Algorithm $a = qn + r$ for some $q, r \in \boldsymbol{Z}$, where $0 \leq r < n$. Since $r = a + (-q)n \in H$, and n is the smallest positive integer in H, necessarily $r = 0$. Therefore $a = qn \in <n>$ which establishes $H \subseteq <n>$. $\square$

The following technical lemma will be of great help to us in the proof of the theorem of this section.

Lemma 1 *Let $G = <a>$ be a cyclic group generated by a.*

a) *Suppose that $a^\ell = a^m$ for some integers $\ell < m$. Then $n = m - \ell > 0$ and $G = \{e, a, \ldots, a^{n-1}\}$.*

b) *Let H be a non-trivial subgroup of G. Then $a^k \in H$ for some positive integer k and furthermore $H = <a^n>$, where n is the smallest such integer.*

c) *Suppose that n is a positive integer and $a^n = e$. Let $k \in \boldsymbol{Z}$ and d be the greatest common divisor of k and n. Then $<a^k> = <a^d>$.*

PROOF: We first show part a). Since $a^\ell e = a^\ell = a^m = a^\ell a^{m-\ell}$, by cancellation $e = a^{m-\ell} = a^n$. Let $g \in G$. Then $g = a^k$ for some $k \in \boldsymbol{Z}$. By the Division Algorithm $k = nq + r$, where $q, r \in \boldsymbol{Z}$ and $0 \leq r < n$. Since $0 \leq r \leq n - 1$ we have

$$g = a^k = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r \in \{e, a, \ldots, a^{n-1}\}.$$

Thus $G \subseteq \{e, a, \ldots, a^{n-1}\}$. As $\{e, a, \ldots, a^{n-1}\} \subseteq G$ the proof of part a) is complete.

To show part b) let $\mathcal{H} = \{k \in \boldsymbol{Z} \,|\, a^k \in H\}$ be the set of exponents of powers of a which lie in H. Since H is a subgroup of G it is easy to see that $\mathcal{H}$ is a subgroup of $\boldsymbol{Z}$. Since $H \neq (e)$ it follows that $\mathcal{H} \neq (0)$. Thus $\mathcal{H} = <n>$, where n is the smallest positive integer in $\mathcal{H}$, by Proposition 1. Since every element of G is a power of a we have

$$H = \{a^k \,|\, k \in \mathcal{H}\} = \{a^{qn} \,|\, q \in \boldsymbol{Z}\} = \{(a^n)^q \,|\, q \in \boldsymbol{Z}\} = <a^n>$$

and part b) follows.

As for part c), we first note that $k = dm$ for some $m \in \boldsymbol{Z}$ since d divides k. Therefore

$$<a^k> = \{(a^k)^q \,|\, q \in \boldsymbol{Z}\} = \{(a^{dm})^q \,|\, q \in \boldsymbol{Z}\} = \{(a^d)^{mq} \,|\, q \in \boldsymbol{Z}\} \subseteq <a^d>.$$

Thus $<a^k> \subseteq <a^d>$. To show that $<a^k> = <a^d>$ we need only show that $<a^d> \subseteq <a^k>$.

Since d is the greatest common divisor of k and n we may write $d = ks + nt$ for some $s, t \in \boldsymbol{Z}$. Let $q \in \boldsymbol{Z}$. Since $dq = ksq + ntq$ we note that

$$(a^d)^q = a^{dq} = a^{ksq+ntq} = a^{kqs}a^{ntq} = (a^k)^{qs}(a^n)^{tq} = (a^k)^{qs}e^{tq} = (a^k)^{qs}$$

from which $<a^d> \subseteq <a^k>$ follows. $\Box$

Let $G = <a>$ be cyclic. The first calculation in part c) establishes:

$$\text{If } m, n \in \mathbf{Z} \text{ then } m|n \text{ implies } <a^m> \supseteq <a^n>. \qquad (1)$$

Suppose that $G = \mathbf{Z}$. Then it is easy to see

$$\text{If } m, n \in \mathbf{Z} \text{ then } m|n \text{ if and only if } <m> \supseteq <n>. \qquad (2)$$

By part b) of the preceding lemma subgroups of cyclic groups are themselves cyclic. There are two types of cyclic groups to consider – finite and infinite. Infinite cyclic groups are far simpler. There is basically one infinite cyclic group, namely $\mathbf{Z}$.

Corollary 1 *Suppose that $G = <a>$ in an infinite cyclic group.*

a) *Let $\ell, m \in \boldsymbol{Z}$. Then $a^\ell = a^m$ if and only if $\ell = m$.*

b) *The function* $f : \mathbf{Z} \longrightarrow G$ *defined by* $f(\ell) = a^\ell$ *for all* $\ell \in \mathbf{Z}$ *is an isomorphism.*

Proof: Suppose that $a^\ell = a^m$. If $\ell \neq m$ then G is finite by part a) of Lemma 1, a contradiction. Therefore $\ell = m$. Of course $\ell = m$ implies $a^\ell = a^m$. We have established part a). That f is a homomorphism follows from the calculation

$$f(\ell + m) = a^{\ell+m} = a^\ell a^m = f(\ell)f(m)$$

for all $\ell, m \in \mathbf{Z}$. Since all elements of G have the form a^ℓ for some $\ell \in \mathbf{Z}$ the function f is onto. Suppose that $\ell, m \in \mathbf{Z}$ and $f(\ell) = f(m)$. Then $a^\ell = a^m$ which means $\ell = m$ by part a). Therefore f is one-one. $\Box$

The finite case is much more complicated and interesting. The structure of a finite cyclic group is very closely related to the numerical properties of its order.

Theorem 1 *Suppose that* $G = <a>$ *be a finite cyclic group of order* n.

a) $G = \{e, a, \ldots, a^{n-1}\}$ *and* $n = |a|$. *In particular* $a^n = e$.

b) *Let* $\ell, m \in \boldsymbol{Z}$. *Then* $a^\ell = a^m$ *if and only if* n *divides* $\ell - m$. *In particular* n *is the smallest of the positive integers* m *such that* $a^m = e$.

c) *Let* H *be a subgroup of* G. *Then* $|H|$ *divides* n.

d) *Suppose that* m *is a positive integer which divides* n. *Then* G *has a unique subgroup* H *of order* m. *Furthermore* $H = <a^{n/m}>$ *and* n/m *is the least positive integer* ℓ *such that* $a^\ell \in H$.

e) *Let* $k \in \boldsymbol{Z}$ *and* d *be the greatest common divisor of* k *and* n. *Then* $<a^k> = <a^d>$ *and has order* n/d. *In particular* $d = n/|H|$.

f) *The generators of* G *are* a^k, *where* $1 \leq k \leq n$ *and* k, n *are relatively prime.*

Proof: Since G is finite there must be a repetition in the sequence

$$e = a^0, a = a^1, a^2, a^3, \ldots \; .$$

Therefore there is a positive integer k such that a^k is one of its predecessors $e, a, \ldots, a^{k-1}$. By the Well-Ordering Principle there is a smallest such positive integer which we call m. Thus

$$e, a, \ldots, a^{m-1}$$

are distinct and $a^m = a^\ell$ for some $0 \leq \ell < m$. In particular $m \leq |G| = n$. As $m - \ell \geq 1$, by part a) of Lemma 1 we conclude that $G = \{e, a, \ldots, a^{m-\ell-1}\}$. In particular $n \leq m - \ell$. Combining inequalities we have $m \leq n \leq m - \ell \leq m$ which means $m = n$ and $\ell = 0$. In particular $a^n = a^m = a^\ell = a^0 = e$. We have shown part a).

As for part b), observe that $a^{nq+m} = a^{nq}a^m = (a^n)^q a^m = e^q a^m = a^m$ for all $q, m \in \boldsymbol{Z}$ by part a). Consequently if n divides $\ell - m$ then $a^\ell = a^m$. To show the converse we need only observe that $\mathcal{H} = \{k \in \boldsymbol{Z} \,|\, a^k = e\}$ is a subgroup of $\boldsymbol{Z}$ which is generated by n; see Proposition 1 and part a) of Lemma 1. We have shown part b).

We prove parts c)–e) together. Let $k \in \boldsymbol{Z}$ and $H = <a^k>$. By part b) of Lemma 1 all subgroups of G have this form. Let $d = \gcd(k, n)$ be the greatest common divisor of k and n. Then $H = <a^k> = <a^d>$ by part c) of Lemma 1.

Since d is a positive divisor of n necessarily $0 < n - d < n$. Thus $e, a^d, \ldots, (a^d)^{((n/d)-1)} = a^{n-d}$ are distinct by part a). Since $(a^d)^{n/d} = a^n = e$ by the same, we use part a) of Lemma 1 to conclude that $<a^d> = \{e, a^d, \ldots, (a^d)^{(n/d)-1}\}$ and has order n/d. Thus: $|H| = n/d$ divides n,

$$d = \gcd(k, n) = n/|H|, \qquad \text{and} \qquad H = <a^k> = <a^{n/|H|}>. \tag{3}$$

Now suppose that ℓ is a positive integer and $a^\ell \in H$. Then $<a^\ell> \subseteq H$. This inclusion together with (3) implies

$$\ell \geq \gcd(\ell, n) = n/|<a^\ell>| \geq n/|H|.$$

Our proof of parts c)–e) is complete. Part f) follows by part a) and (3). $\Box$

Suppose that $G = <a>$ is a finite cyclic group of order n. Then the subgroups of G are cyclic. Observe that

$$\{\text{positive divisors of } n\} \longleftrightarrow \{\text{subgroups of } G\} \tag{4}$$

given by

$$d \mapsto <a^{n/d}>$$

is a bijective correspondence. Note that $<a^{n/d}>$ has order d.

The number of generators of G is $\phi(n)$, where $\phi(n)$ is the number of integers k in the range $1 \leq k \leq n$ which are relatively prime to n. The function $\phi : \mathbf{N} \longrightarrow \mathbf{N}$, where $\mathbf{N} = \{1, 2, 3, \ldots\}$, is called the *Euler ϕ-function.* As a consequence of the theorem:

Corollary 2 *Let n be a positive integer. Then* $\sum\limits_{d|n} \phi(d) = n.$

PROOF: Let $G = <a>$ be a cyclic group of order n. (There is such a group, namely $\boldsymbol{Z}_n$.) We define a relation on G by $x \sim y$ if and only if $<x> = <y>$. Since "equals" $=$ is an equivalence relation $\sim$ is also. For $x \in G$ note that the equivalence class $[x]$ is the set of all generators of the cyclic subgroup $<x>$ of G. The reader is left with the exercise of showing that the assignment $[x] \mapsto <x>$ determines a well-defined bijection between the set of equivalence classes of G and the set of cyclic subgroups of G. (Well-defined means that if $[x] = [y]$ then $<x> = <y>$.) Observe that this bijective correspondence holds for any group. Since the number of generators of $<x>$ is $\phi(|<x>|)$ by part f) of Theorem 1, using the bijective correspondence described by (4), we see that

$$\sum_{d|n} \phi(d) = \sum_{d|n} |[a^{n/d}]| = |G| = n.$$

□

Let us apply the theorem to a cyclic group $G = <a>$ of order 15. The divisors of 15 are $1, 3, 5, 15$. Therefore G has 4 subgroups. Since $1, 2, 4, 7, 8, 11, 13, 14$ lists the integers k such that $1 \leq k \leq 15$ which are relatively prime to 15 it follows that G has 8 generators:

$$a, a^2, a^4, a^7, a^8 = a^{-7}, a^{11} = a^{-4}, a^{13} = a^{-2}, \text{and } a^{14} = a^{-1}.$$

The subgroups of G are

$$<a^{15}> = <e> = \{e\},$$

$$<a^{15/3}> = <a^5> = \{e, a^5, a^{10}\},$$

$$<a^{15/5}> = <a^3> = \{e, a^3, a^6, a^9, a^{12}\},$$

and

$$<a^{15/15}> = <a^1> = G.$$

Now suppose that $G = <a>$ is cyclic of order 30 and let H be the subgroup of G of order 10. Then

$$H = <a^{30/10}> = <a^3> = \{e, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{25}, a^{27}\}.$$

Since the divisors of 10 are $1, 2, 5, 10$ it follows that H has 4 subgroups. These are

$$<(a^3)^{10/1}> = <a^{30}> = \{e\},$$

$$<(a^3)^{10/2}> = <a^{15}> = \{e, a^{15}\},$$

$$<(a^3)^{10/5}> = <a^6> = \{e, a^6, a^{12}, a^{18}, a^{24}\},$$

and

$$<(a^3)^{10/10}> = <a^3> = H.$$

What are the generators of H? Since the integers k which are relatively prime to 10 and satisfy $1 \leq k \leq 10$ are $1, 3, 7, 9$, it follows that

$$(a^3)^1 = a, (a^3)^3 = a^9, (a^3)^7 = a^{21}, (a^3)^9 = a^{27}$$

are the generators of H.

A good exercise would be to reformulate the preceding calculations for the (additive) cyclic groups $\boldsymbol{Z}_{15}$ and $\boldsymbol{Z}_{30}$ or orders 15 and 30 respectively.

We end by noting that just as there is essentially one infinite cyclic group, namely $\mathbf{Z}$, for each positive integer n there is essentially one cyclic group of order n, namely $\mathbf{Z}_n$. We denote its binary operation of $\mathbf{Z}_n$ by $\oplus$. As a set

$$\mathbf{Z}_n = \{0, 1, \ldots, n-1\}.$$

Let $\ell, m \in \mathbf{Z}_n$. By the Division Algorithm $\ell + m = nq + r$, where $q, r \in \mathbf{Z}$ and $0 \leq r < n$, and the integers q, r are uniquely determined by these conditions. By definition $\ell \oplus m = r$.

Suppose that $G = <a>$ ia a cyclic group of order n. Then $f : \mathbf{Z}_n \longrightarrow G$ defined by $f(\ell) = a^\ell$ for all $\ell \in \mathbf{Z}_n$ is a set bijection by part a) of Theorem 1. By the same $a^n = e$. Let $\ell, m \in \mathbf{Z}_n$ and write $\ell + m = nq + r$ as above. The calculation

$$f(\ell)f(m) = a^\ell a^m = a^{\ell+m} = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r = f(r) = f(\ell \oplus m)$$

shows that f is in fact an isomorphism.