Math 375
Week 3

3.1 The Center and Centralizer

There are two subgroups of any group G that are easily defined and easily confused

Definition 1 *If G is a group then the* **center of** G *is the set*

$$C(G) = \{a \in G |\ ax = xa\ \forall x \in G\}.$$

Note that the center consists of the elements of G which commute with all elements of G.

Theorem 2 *Show that $C(G)$ is a subgroup of G.*

PROOF Let's use the two step method.

CLOSURE Let $a, b \in C(G)$. Show that $ab \in C(G)$. For all $x \in G$,

$$(ab)x = a(bx) = a(xb) = (ax)b = x(ab)$$

so $ab \in C(G)$.

INVERSES Let $a \in C(G)$. Show that $a^{-1} \in C(G)$. But

$$ax = xa \Rightarrow (ax)^{-1} = (xa)^{-1} \Rightarrow x^{-1}a^{-1} = a^{-1}x^{-1}.$$

So $a^{-1} \in C(G)$. ∎

Example 1 If G is abelian what is $C(G)$?

Example 2 Show that $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in C(GL(2, \mathbf{R}))$ where $a \neq 0$. In fact, it can be shown that

$$C(GL(2), \mathbf{R}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| \ a \neq 0 \right\}.$$

Example 3 $C(D_3) = \{e = r_0\}$ since non-zero rotations don't commute with flips.

Example 4 For an element to be in the center of G its row and column in the Cayley table for G must be identical. Clearly the identity must always be in the center.

Example 5 What is $C(V_4)$? What is $C(Q_8)$? Answers: V_4 and $\{I, -I\}$, respectively.

Definition 3 *Let G be a group and let $a \in G$. The* ***centralizer*** *of G is the set*

$$C(a) = \{g \in G \mid ga = ag\} = \{g \in G \mid gag^{-1} = a\}$$

Example 6 For an element g to be in the centralizer of a, the g entry of the a-row and a-column must be the same.

Theorem 4 *$C(a)$ is a subgroup of G.*

PROOF Use the one-step method. Note that $C(a)$ is never empty since it always contains e. So let $g, h \in C(a)$. Is $gh^{-1} \in C(a)$?

$$(gh^{-1})a(gh^{-1})^{-1} = g(h^{-1}ah)g^{-1}.$$

Now since $h \in C(a)$, then $hah^{-1} = a \Rightarrow a = h^{-1}ah$ using left and right multiplication by h^{-1} and h, respectively. So $h^{-1} \in C(a)$ (so maybe we should have done two-step method). So then from above,

$$(gh^{-1})a(gh^{-1})^{-1} = g(h^{-1}ah)g^{-1} = gag^{-1} = a$$

since $g \in C(a)$. So $gh^{-1} \in C(a)$, too. ∎

(ii) Inverses: use the method as in center proof. ∎

Example 7 In D_3, $C(a) = \{a,\ r_0\}$, $C(r_{120}) = \{r_0,\ r_{120},\ r_{240}\}$.

Example 8 In $GL(2, \mathbf{R})$ find $C\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$. By direct computation:

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbf{R} \right\}.$$

Example 9 In an abelian group G, $C(a) = G$.

Example 10 What is $C(J)$ in Q_8?

Note that we can think of both the centralizer and the center as a measure of the abelianness of the element or the group in question.

Example 11 It is clear that

$$C(G) = \bigcap_{a \in G} C(a)$$

since $C(G) \subseteq C(a)$ for any a and if $g \in C(a)$ for all a then it commutes with every element in G so it is in (G).

3.2 Cyclic Subgroups

Last time we were able to derive a finite subgroup test because if H were a finite closed subset of a group G, powers of the elements of H cycled around on themselves.

Example 12 In $(\mathbf{Z}_6, \oplus)$, let's examine the powers of 3, 4, and 5 explicitly.

a) $|3| = 2$ $\qquad \begin{cases} 1(3) = 3 \\ 2(3) = 0 \end{cases}$

b) $|4| = 3$ $\qquad \begin{cases} 1(4) = 4 \\ 2(4) = 2 \\ 3(4) = 0 \end{cases}$

c) $|5| = 6$ $\qquad \begin{cases} 1(5) = 5 \\ 2(5) = 4 \\ 3(5) = 3 \\ 4(5) = 2 \\ 5(5) = 1 \\ 6(5) = 0 \end{cases}$

In this last case all of the elements of $\mathbf{Z}_6$ are *multiples* (i.e., powers) of of 5. This is not the case with 3 or 4.

Our next goal is to make the notion of generation by powers precise.

Definition 5 *Let $x \in G$, a group. The set of powers (multiples) of x in G is denoted by $< x >$. In particular:*

$$< x > = \{x^n \mid n \in \mathbf{Z}\} \qquad \text{(for multiplicative groups)}$$
$$< x > = \{nx \mid n \in \mathbf{Z}\} \qquad \text{(for additive groups)}$$

Example **a)** in $\mathbf{Z}_6$

$$< 3 > = \{3,\ 0\}$$
$$< 5 > = \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$$

b) In D_3

$$< v > = \{v,\ r_0\}$$
$$< r_{120} > = \{r_{120},\ r_{240},\ r_0\}$$

c) Find $< 5 >$ in $U(12)$.

d) Find $< i >$ in $\mathbf{C}^*$. □

It is worth repeating, even though $< x >= \{\ldots, x^{-2}, x^{-1}, x^0 = e, x^1, x^2, \ldots\}$ would seem to have an infinite number of elements, it may only be finite if powers of the elements cycle around on themselves.

THEOREM 6 *Let G be a group. Then $< x >$ is a subgroup of G.*

Let's use the one step method. Pick two elements in $g, h \in < x >$. What do they look like? $g = x^n$ and $h = x^m$. Notice $gh^{-1} = x^n(x^m)^{-1} = x^n x^{-m} = x^{n-m} \in < x >$. ■

Note: It is obvious that $|x| = |< x >|$ since both numbers simply count the distinct powers(multiples) of x.

EXAMPLE **a)** In $U(12)$, $< 5 >= \{5, 1\}$.

b) In $\mathbf{Z}_{12}$, $< 3 >= \{3, 6, 9, 0\}$.

c) In Q_8, $< K >=< I, K, -I, -K >$.

d) In $\mathbf{Z}$, what is $< 1 >$? What about $< 2 >$?

DEFINITION 7 *If there is some element $x \in G$ such that $< x >= G$, then G is called a **cyclic** group. In other words, $G = \{x^n \mid n \in \mathbf{Z}\}$. We call x a **generator** of G.*

Note: Obviously if $< x >= G$, then $|x| = |G|$.

EXAMPLE 15 Which of the following are cyclic: D_3, V_4, Q_8, $\mathbf{Z}$, $\mathbf{Z}_n$, $\mathbf{Q}^*$, $U(12)$, $U(5)$, and $\mathbf{R}$.

LEMMA 8 *If x is a generator of G, then so is x^{-1}.*

PROOF Let $g \in G$. We must show that g can be written as some power of x^{-1}. Since G is generated by x, then for some $k \in \mathbf{Z}$, $g = x^k = (x^{-1})^{-k}$. ■

EXAMPLE 16 Find all the generators of $\mathbf{Z}_8$.

SOLUTION Certainly 1 is hence so is 7. 2 is not, so 6 is not. 3 is, so 5 is. 4 is not and 0 is not. □

THEOREM 9 *Let a be an element of a group G.*

a) *If $|a| = \infty$, then $a^j = a^k \iff k = j$.*

b) *If $|a| = n$, then $a^j = a^k \iff n \mid k - j \iff k = j \bmod n$.*

PROOF A Note that

$$\begin{aligned} a^j = a^k &\iff e = a^{k-j} \\ &\iff k - j = 0 \qquad \text{(since } |a| = \infty) \\ &\iff k = j \end{aligned}$$

PROOF B By the division algorithm, $k - j = qn + r$ where $0 \le r < n$.

$$\begin{aligned} a^j = a^k &\iff e = a^{k-j} \\ &\iff e = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r \\ &\iff e = a^r && a^n = e \text{ above} \\ &\iff r = 0 && |a| = n \text{ and } r < n \\ &\iff k - j = qn \\ &\iff n \mid k - j. \end{aligned}$$

COROLLARY 10 *Let $|a| = n$. If $a^k = e$, then $n \mid k$.*

PROOF Notice $a^k = e = a^0$, so by the theorem $n \mid k - 0$. ∎

Gallian's comments in the text about the theorem in the finite case are crucial. In the case where $|a| = n$, then the group operation in the cyclic group $< a >$ amounts to addition mod n. That is, if $k + j = r \bmod n$, then $a^k a^j = a^r$, no matter what the particular element represents. (Example: $i \in C^*$, $K \in Q_8$, and $r_{90} \in D_4$ all have order four. And the little cyclic subgroups that each generates are essentially the same.) This leads to the notion of an *isomorphism* which we will discuss in great detail later. A similar remark is true when $|a| = \infty$. Then the group operation in $< a >$ boils down to regular addition in $\mathbf{Z}$ since $a^j a^k = a^{j+k}$. The whole point is that both $\mathbf{Z}$ and $\mathbf{Z}_n$ are well understood, even by you. We want to find out when other groups are "just like them."

The first part of the next result is **not in the text.** But it is crucial.

THEOREM 11 ***(Generators of Finite Cyclic Groups: Sam Park's Thm)*** *Let $G =< a >$ be a cyclic group of order n.*

a) $|a^k| = \dfrac{\operatorname{lcm}(k,n)}{k} = \dfrac{n}{\gcd(k,n)}$.

b) *a^k is also a generator of G if and only if* $\gcd(k, n) = 1$.

PROOF A By the corollary

$$(a^k)^j = e \iff a^{kj} = e \iff n \mid kj.$$

Therefore $|a^k| = j \iff kj$ is the smallest multiple of k divisible n $\iff kj$ is the smallest common multiple of n and $k \iff kj = \text{lcm}(k, n)$. Therefore,

$$|a^k| = j = \frac{kj}{j} = \frac{\text{lcm}(k,n)}{k}$$
$$= \frac{\text{lcm}(k,n) \cdot \gcd(k,n)}{k \cdot \gcd(k,n)} = \frac{kn}{k \cdot \gcd(k,n)} = \frac{n}{\gcd(k,n)}$$

PROOF B Since $< a^k > \leq < a > = G$, to show that $< a^k > = < a >$, it suffices to show that $| < a^k > | = | < a > | = n$. But

$$| < a^k > | = |a^k| = \frac{n}{\gcd(k,n)} = n \iff \gcd(k,n) = 1.$$

Since $\mathbf{Z}_n$ is cyclic his theorem means that

Corollary 12 *An integer k is a generator of $\mathbf{Z}_n$ if and only if* $\gcd(k, n) = 1$.

Example 17 Find the order of each element of $\mathbf{Z}_{12}$. Which are generators? (Answer: 1, 5, 7, and 1 which are exactly the elelments of $U(12)$. More generally, the generators of $\mathbf{Z}_n$ are the elements of $U(n)$.

Example 18 Suppose that $G = < a >$ is cyclic of order 24. What are its generators?

Example **a)** What is the order of 756 in $\mathbf{Z}_{1155}$? Well, in the first week of class we saw $\gcd(1155, 756) = 21$. Therefore

$$|756| = \frac{1155}{\gcd(756, 1155)} = \frac{1155}{21} = 55.$$

e) What is the order of a^{756} in $G = < a >$ if $|a| = 1155$? Same as above: 21.

Theorem 13 ***(Fundamental Theorem of Cyclic Groups)*** *Let $G = < a >$ be a cyclic group, then:*

a) *every subgroup of G is cyclic;*

b) *if $| < a > | = n$, then the order of any subgroup of $< a >$ is a divisor of n;*

c) *if k is a divisor of $n = | < a > |$, then the group $< a >$ has exactly one subgroup of order k, namely $< a^{n/k} >$.*

Let's look at what this theorem means before we prove it.

EXAMPLE 20 $\mathbf{Z}$ is cyclic, so every subgroup of $\mathbf{Z}$ has the form $< n >$. But this is just the set of multiples of n. For example, $< 2 >$ is the set of even integers, $< 3 >$ is the set of integers divisible by 3. Now we also know that the intersection of two subgroups is again a subgroup.

b) What is $< 12 > \cap < 8 >$? Well, it must be $< n >$ since $\mathbf{Z}$ is cyclic. It is a set of multiples common to both $< 8 >$ and $< 12 >$. Therefore $< 12 > \cap < 8 > = < \operatorname{lcm}(8, 12) >$.

c) More generally, $< m > \cap < n > = < \operatorname{lcm}(m, n) \bmod n >$. ∎

EXAMPLE 21 Now consider $G = \mathbf{Z}_{24}$. It is cyclic and generated by 1. We can list all of its subgroups because we know all of its divisors: 1, 2, 3, 4, 6, 8, 12, and 24.

Order 24: $< 1 > = \{0, 1, \ldots, 23\} = < 23 > = ?$
Order 12: $< 2 > = \{0, 2, 4, \ldots, 22\} = < 22 > = ?$ Now we need $2 = \gcd(k, n)$ for k to generate this subgroup of order 12.
Order 8: $< 3 > = \{0, 3, 6, \ldots, 21\} = < 21 > = ?$
Order 6: $< 6 > = \{0, 6, 12, 18\} = < 18 > = ?$
Order 3: $< 8 > = \{0, 8, 16\} = < 16 >$
Order 2: $< 12 > = \{0, 12\}$
Order 1: $< 0 > = \{0\}$

Notice that in each case, the subgroup of order k had $24/k$ as one of its generators.

d) We can reinterpret this list for a multiplicative group $G = < a >$ of order 24.

Order 24: $< a > = \{e = a^0, a^1, \ldots, a^{23}\} = < a^{23} >$
Order 12: $< a^2 > = \{e, a^2, a^4, \ldots, a^{22}\} = < a^{22} >$
Order 8: $< a^3 > = \{e, a^3, a^6, \ldots, a^{21}\} = < a^{21} >$
Order 6: $< a^6 > = \{e, a^6, a^{12}, a^{18}\} = < a^{18} >$
Order 3: $< a^8 > = \{e, a^8, a^{16}\} = < a^{16} >$
Order 2: $< a^{12} > = \{e, a^{12}\}$
Order 1: $< e > = \{e\}$

EXAMPLE 22 Suppose that a finite cyclic group $G = < a >$ has exactly three distinct subgroups: G itself, a subgroup of order 7, and $\{e\}$. What is the order of G?

SOLUTION What do we know? Let $|G| = n$. We know that $7 \mid n$, and of course $1 \mid n$ and $n \mid n$? Can any other k divide n? Thus, n is a power of 7, i.e., $n = 7^m$. What must m be? Can't be 0 or 1, could be 2. Why can't it be higher than 2? ∎

PROOF To prove the theorem we proceed in steps.

(A) Let H be any subgroup of G. If $H = \{e\}$, then $H =< e >$ and so is cyclic. If H is not $\{e\}$, then H contains elements of the form a^k where $k \neq 0$. Of course if $a^k \in H$, then $a^{-k} \in H$ and either k or $-k$ is positive. By Well-Ordering, there is a smallest positive integer d such that $a^d \in H$. By closure, it is clear that $< a^d > \leq H$ We will now show that $< a^d >= H$.

Let $h \in H$. Then $h \in G$, $h = a^k$ for some k. By the division algorithm:

$$k = qd + r \qquad 0 \leq r < d.$$

Next since $a^d \in H$, then $(a^d)^{-q} = a^{-qd} \in H$. Therefore,

$$a^{-qd}h = a^{-qd}a^k = a^{-qd}a^{qd+r} = a^r \in H \qquad 0 \leq r < d.$$

If $r \neq 0$ this contradicts the choice of d as the minimal power of x in H. So we must have $r = 0$ and therefore $k = qd$. Thus

$$h = a^k = a^{qd} = (a^d)^q \in < a^d > .$$

(B) From (a) any subgroup H of $G =< a >$ is cyclic, so $H =< a^d >$. But then

$$|H| = | < a^d > | = |a^d| = \frac{n}{\gcd(n, d)}$$

so $n = |H| \cdot \gcd(n, d)$. But then $|H| \mid n$.

(C) Let k be any divisor of n, so $kd = n$ and $d = n/k$. We must show that there is only one subgroup of order k. First we find one such subgroup. Notice that $| < a^d > | = \frac{n}{\gcd(n,d)} = \frac{n}{d} = k$. So if $H =< a^d >$, then $|H| = | < a^d > | = k$.

Next, let H' be some other subgroup of order k. (To show $H = H'$.) From (a), $H' =< a^{d'} >$ for some d' and from (b)

$$\frac{n}{\gcd(n, d')} = |H'| = k = \frac{n}{d}.$$

Therefore,

$$\gcd(n, d') = d \Rightarrow d = kn + md' \Rightarrow a^d = a^{kn+md'} = a^{md'}$$

But then

$$a^{d'} = a^{md} = a^{d^m} \in < a^d > \Rightarrow < a^{d'} > \leq < a^d >$$

by closure. But

$$| < a^{d'} > | = |H'| = |H| = | < a^d > |$$

so we must have $H =< a^{d'} >=< a^d >= H$. ∎

Example **a)** List the subgroups of $\mathbf{Z}_{24}$. Illustrate their relation to each other with a schematic diagram called a **lattice**. Do the same for $\mathbf{Z}_{30}$ and $\mathbf{Z}_{20}$.

b) Show that in Z_n we have $< k > \cap < m > = < \text{lcm}(k, m) \bmod n >$, for example in $\mathbf{Z}_{24}$ we have: $< 6 > \cap < 8 > = < 0 >$, etc. (Show how this appears in the lattice. Also note that the smallest subgroup containing $< k >$ and $< m >$ is $< \gcd(k, m) \bmod n >$.)

Example 24 If $G = < x >$ and has order 225, find the order of the subgroup $< x^{90} >$. Solution $| < x^{90} > | = 225/\gcd(225, 90) = 225/45 = 5$. Notice that $< x^{45} > = < x^{90} >$ since there is only one subgroup of order 5 of G.

Example 25 Show that every group of order 3 must be cyclic. (Write out the Cayley table.)