Math 375
Week 7

7.1 Equivalence Relations Redux

Definition 1 *Let S be a set. $\sim$ is an* ***equivalence relation*** *on S if R satisfies the following three condidtions:*

i) for every $s \in S$, $s \sim s$ (s is related to itself; reflexive);

ii) for every $s, t \in S$, if $s \sim t$ then $t \sim s$ (symmetric);

iii) for every $s, t, u \in S$, if $s \sim t$ and $t \sim u$ then $s \sim u$ (transitive).

Definition 2 *For any $s \in S$, let $[s]$ denote the subset of S consistingt of all $t \in S$ such that $t \sim s$. That is,*

$$[s] = \{t \in S \mid t \sim s\}.$$

We call $[s]$ the ***equivalence class*** *of s under the relation $\sim$.*

Definition 3 *A* ***partition*** *of a set S is a collection of nonempty disjoint subsets of S whose union is all of S.*

Example 1 If $\sim$ is the equivalence relation $\equiv \pmod 5$ on $\mathbf{Z}$, then $[0], [1], [2], [3], [4]$ form a partition of $\mathbf{Z}$. This situation is the norm for any equivalence relation.

Example 2 We saw that isomorphisnm $\cong$ was an equivalence relation on the set of all groups.

Theorem 4 *Let $\sim$ be an equivalence relation on S. Then the equivalence classes of $\sim$ form a partition of S. That is, every element is in exactly one equivalence class. And conversely.*

PROOF Let $\sim$ be the equivalence relation. Since $s \sim s$ for any $s \in S$, it follows that $s \in [s]$. That is, no class is empty. Second, the union of all equivalence classes is clearly all of S since every element s of S lies in some equivalence class.

Finally we must show that any two classes are either disjoint or exactly the same. So suppose that two classes $[s]$ and $[t]$ are not disjoint, that is, that there is at least one element a in both $[s]$ and $[t]$. We must show that $[s] = [t]$. (To do this we must show $[s] \subset [t]$ and $[t] \subset [s]$.) To show $[s] \subset [t]$, let $b \in [s]$. Then: $b \sim s$. But $a \in [s]$, so $s \sim a$ and thus $b \sim a$. But $a \in [t]$ so $a \sim t$ and therefore $b \sim t$. That is, $b \in [t]$. So $[s] \subset [t]$ and similarly $[t] \subset [s]$.

The proof of the converse is an exercise. We'll never use it. ∎

Another way to say the same thing is :

$$[s] = [t] \iff [s] \cap [t] \neq \emptyset.$$

Notice that it is actually the equivalence classes mod n that we made into a group.

7.2 Cosets and the Equivalence Relation $\sim_H$

The most important use of an equivalence relation in elementary group theory has to do with the idea of cosets. Cosets are just the equivalence classes of a fancy equivalence relation on a group. Let's examine that relation.

Theorem 5 *Let H be a subgroup of a group G. Define $a \sim b \iff a^{-1}b \in H$. Then $\sim$ is an equivalence relation on G.*

PROOF We have seen this argument before. Reflexive: show $a \sim a$. Well

$$a \sim a \iff a^{-1}a \in H \iff e \in H.$$

Symmetric: If $a \sim b$, show $b \sim a$. But

$$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow b \sim a.$$

Transitive: Given $a \sim b,\ b \sim c$, show $a \sim c$.

$$\begin{aligned} a \sim b,\ b \sim c &\Rightarrow a^{-1}b,\ b^{-1}c \in H \\ &\Rightarrow (a^{-1}b)(b^{-1}c) \in H \\ &\Rightarrow a^{-1}c \in H \Rightarrow a \sim c. \end{aligned}$$ ∎

Remember that any equivalence relation partitions the original set (here G) into mutually disjoint subsets called **equivalence classes**. Recall that we used the notation $[a]$ to denote the set of all elements related to a. That is, $[a] = \{b \in G \mid a \sim b\}$. Here these equivalence classes are easy to describe.

Definition 6 *Let H be subgroup of a group G. For any element $a \in G$, the set aH is the **left coset of** H in G where $aH = \{ah |\ h \in H\}$.*

Lemma 7 *If $H \leq G$ and $\sim$ is the equivalence relation above, then $a \sim b \iff b \in aH$. (That is, $[a] = aH$.)*

PROOF Let $x \in G$. Then

$$\begin{aligned} a \sim b \iff a^{-1}b \in H &\iff a^{-1}b = h,\ h \in H \\ &\iff b = ah,\ h \in H \\ &\iff b \in aH. \ \blacksquare \end{aligned}$$

Example 3 Let $G = U(8) = \{1, 3, 5, 7\}$ and let $H = \{1, 5\}$. Then:

$$\begin{aligned} [1] &= 1H = \{1, 5\} \\ [3] &= 3H = \{3, 7\} \\ [5] &= 5H = \{5, 1\} = 1H \\ [7] &= 7H = \{7, 3\} = 3H \end{aligned}$$

Example 4 Let $G = \mathbf{Z}_{12}$ and $H =< 4 >= \{0, 4, 8\}$. Find the left cosets of H in G. Note that each coset has the same number of elements and that cosets are either disjoint or are identical, i.e., they partition G.

Example 5 Let $G = S_3$, $H = A_3 = \{(1),\ (123),\ (132)\}$. Notice that

$$(1) \sim g \iff (1)^{-1}g \in A_3 \iff g \in A_3.$$

So $[(1)] = (1)A_3 = A_3$. Notice that

$$(12) \sim g \iff (12)^{-1}g \in A_3 \iff (12)g \in A_3 \iff g \text{ is odd}.$$

Therefore $[(12)] = (12)A_3 = \{(12),\ (13),\ (23)\}$. Since the left cosets (equivalence classes) of A_3 partition S_3, we know we can stop looking for other left cosets. The two we found already yield all of S_3. They are A_3 and $(12)A_3 = \{(12), (23), (13)\}$ which are disjoint and partition S_3. Notice each class has the same number of elements. $\square$

Example 6 Let $G = \mathbf{Z}$ and let $H = 5\mathbf{Z} = \{\ldots, -10, 5, 0, 5, 10, \ldots\} = \{5n \mid n \in \mathbf{Z}\}$. H is clearly a subgroup. We saw that the equivalence classes of $\sim$ were $[a] = \{a + 5n \mid n \in \mathbf{Z}\} = a + H = a + 5\mathbf{Z}$. In particular:

$$\begin{aligned} 5\mathbf{Z} = 0 + 5\mathbf{Z} &= \{\ldots, -10, 5, 0, 5, 10, \ldots\} = \ldots = [-5] = [0] = [5] = \ldots \\ 1 + 5\mathbf{Z} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} = \ldots = [-4] = [1] = [6] = \ldots \end{aligned}$$

and so on.

Example 7 Let $G = GL(n, \mathbf{R})$ and let $H = SL(n, \mathbf{R}) = \{A \in GL(n, \mathbf{R}) \mid \det A = 1\}$. Notice that

$$\begin{aligned} A \sim B \iff A^{-1}B \in SL(n) &\iff \det A^{-1}B = 1 \\ &\iff \det B \det A^{-1} = 1 \\ &\iff \det B(\det A)^{-1} = 1 \\ &\iff \det A = \det B. \end{aligned}$$

Thus we get an equivalence class or left coset for $SL(n, \mathbf{R})$ for each different non-zero real number. ☐

Now we could have started out using a similar equivalaence relation: Let $H \leq G$ and define the equivalence relation $\approx$ defined by $a \approx b \iff ba^{-1} \in H$. (It is an easy check to see that this is an equivalence relation.) We would then find that $a \approx b \iff b \in Ha = \{ha \mid h \in H\}$. The set Ha is called the **right coset** of the subgroup H in G.

Example 8 It is not true that $aH = Ha$ for all $H \leq G$. Clearly, we ust look at nonabelian groups to find an example. Let $G = D_4$ and $H = \{r_0, v\}$. Then: $r_{90}H = \{r_{90}, d'\}$ while $Hr_{90} = \{r_{90}, d\}$. This is a very important example. However, do notice that both cosets do have the same number of elements in them. ☐

Example 9 Let $G = S_3$ and $H = S_2 = \{(1), (12)\}$. Compare the right and left cosets of H in G.

The right cosets:

$$\begin{aligned} H(1) &= H = H(12) \\ H(13) &= \{(13), (132)\} = H(132) \\ H(23) &= \{(23), (123)\} = H(123) \end{aligned}$$

The left cosets are:

$$\begin{aligned} (1)H &= H = (12)H \\ (13)H &= \{(13), (123)\} = (123)H \\ (23)H &= \{(23), (132)\} = (132)H \end{aligned}$$

Notice that the number of left cosets is the same as the number of right cosets. However, in general $aH \neq Ha$. Notice that all the cosets, left or right have the same number of elements. We will prove that this last observation is true in general.

Theorem 8 ***(Properties of Cosets)*** *Let H be a subgroup of G.*

- ***a)*** $a \in aH$;
- ***b)*** $aH = bH$ *or* $aH \cap bH = \emptyset$;
- ***c)*** $aH = bH \iff a^{-1}b \in H$;
- ***d)*** $aH = H \iff a \in H$;
- ***e)*** $|aH| = |bH| = |H|$;
- ***f)*** $aH = Ha \iff H = aHa^{-1}$;
- ***g)*** aH *is a subgroup of* $G \iff a \in H$ $(\iff aH = H)$.

PROOF A Since $e \in H$, then $a = ae \in aH$. Alternately, $a \sim a \Rightarrow a \in [a] = aH$.

B Cosets are just the equivalence classes of the relation $\sim_H$ and are, therefore, equal or disjoint.

C $aH = bH \iff b \in aH \iff a \sim b \iff a^{-1}b \in H$. (The first $\iff$ uses the previous fact that cosets are either disjoint or equal.)

D $H = a \iff eH = H \iff e^{-1}a \in H \iff a \in H$.

E Define the mapping $\phi : H \to aH$ by $\phi h = ah$. We have seen that this map is injective, and by definition of aH it is surjective. Therefore, $|H| = |aH|$. Similarly $|bH| = |H|$ so $|aH| = |bH|$.

F $aH = Ha \iff (aH)a^{-1} = (Ha)a^{-1} \iff aHa^{-1} = H$. Here $aHa^{-1} = \{aha^{-1} \mid h \in H\}$.

G $aH \leq G \Rightarrow e \in aH \Rightarrow eH = aH \Rightarrow H = aH$. Of couse this says that $a \in H$. Conversely, $a \in H \Rightarrow aH = H \Rightarrow aH$ is a subgroup. ∎

Part (e) of this theorem is very important. Let G be a finite group. Because the cosets of H partition G we can write

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH, \qquad a_iH \cap Ha_j = \emptyset.$$

Notice that finiteness of G is important because it means that the number of cosets is finite and the number of elements in each coset is finite. Therefore

$$|G| = |a_1H| + |a_2H| + \cdots + |a_kH| = |H| + |H| + \cdots |H| = k|H|.$$

Thus, $|H| \Big| |G|$. So we have shown:

7.3 Lagrange's Theorem

Theorem 9 ***(Lagrange's Theorem)*** *Let H be a subgroup of a finite group G. Then $|H|\Big||G|$.*

Definition 10 *The number of distinct right cosets of H in G is called the* **index** *of H in G and is denoted by $[G:H]$ or by $|G:H|$. (Note: if G is infinite, then the index of H in G may or may not be infinite.)*

Corollary 11 *For finite groups G, Lagrange's theorem says $|G| = [G:H]\cdot|H|$.*

Example

a) $[S_n : A_n] = 2$

b) $[S_n : S_{n-1}] = n$

c) $[S_n : D_n] = n!/2n = (n-1)!/2$

d) $[GL(n) : SL(n)] = \infty$

e) $[\mathbf{Z} : 2\mathbf{Z}] = 2$

f) If $GL(\mathbf{R}, n)^+ = \{A \in GL(\mathbf{R}, n) \mid \det A > 0\}$, then $[GL(\mathbf{R}, n) : GL(\mathbf{R}, n)^+] = 2$.

g) $[\mathbf{Z} : n\mathbf{Z}] = n$ (n a positive integer).

h) $[\mathbf{R}^* : \mathbf{R}^+] = 2$. $\square$

Note: The converse of Lagrange's theorem is false. That is, if $d \mid |G|$, then G need not have a subgroup of order d. The simplest example is with A_4. $|A_4| = 12$ and $6 \mid 12$. Now A_4 has $\frac{4\cdot 3\cdot 2}{3} = 8$ elements (3-cycles) of order 3. Suppose that $H < G$ and $|H| = 6$. Then let $a \in A_4$ be a 3-cycle such that $a \notin H$. Since $[A_4 : H] = 2$, the only two cosets of H are H and aH. So $a^2H = H$ or $a^2H = aH$. In the first case, $a^3H = aH \Rightarrow H = aH$, a contradiction. In the second case, $a^3H = a^2H \Rightarrow H = a^2H = aH$, again a contradiction.

There are some important yet easy to prove consequences of Lagrange's theorem. First recall that if $x \in G$, then $< x >$ is the cyclic subgroup of G consisting of all the powers of x, $\{x^n \mid n \in \mathbf{Z}\}$. Of course $| < x > | = |x|$.

So if G is finite and $H =< x >$, then Lagrange says: $|H|\Big||G|$, so $|x|\Big||G|$. That is,

Corollary 12 *If G is finite and $x \in G$, then $|x|\Big||G|$.*

Thus, if $|G| = n$ and $x \in G$, then $|x|\Big|n$ so $n = k|x|$ for some integer k. Thus

$$x^{|G|} = x^n = x^{k|x|} = (x^{|x|})^k = e^k = e.$$

We have proven

Corollary 13 *If G is a finite group of order $n = |G|$, then $x^n = e$ for all $x \in G$.*

Corollary 14 ***Fermat's Little Theorem*** *For all integers a and all primes p, $a^p = a \bmod p$.*

Example 11 $4^3 = 4 \bmod 3$, i.e., $64 = 1 \bmod 3$.

PROOF Use the division algorithm to write $a = qp + r$ with $0 \leq r \leq p - 1$. That is, $r \in U(p) = \{o, 1, \ldots, p-1\} = G$. From previous work, because "modding" is a group homomorphism, we can mod before or after multiplying. So $a = r \bmod p$, so $a^p = r^p \bmod p$. So ETS that $r^p = r \bmod p$. But $r \in G = U(p)$ and $|G| = p - 1$, so by the previous corollary, $r^{|G|} = r^{p-1} = 1$, i.e. $r^{p-1} = 1 \bmod p$. Therefore, $r^p = r \bmod p$.

At this point we can now classify certain types of groups.

Corollary 15 *If a group G is of prime order p, then G is cyclic.*

PROOF Let $|G| = p$, where p is prime. Let x be any element of G that is not the identity element. Then $|x|\Big||G|$ implies that either $|x| = 1$ and so $x = e$ (impossible) or $|x| = p$ which implies that $< x >= G$. Notice that we have shown that *any* non-identity element will be a generator in this case. (This is not true of all cyclic groups, $\mathbf{Z}_4$ is not generated by 2.) ∎

Thus there is only one group of order n where n is 2, 3, 5, and 7 and it is isomorphic to $\mathbf{Z}_n$ (i.e., its Cayley table looks like that of $\mathbf{Z}_n$) Compare with S_2 with $\mathbf{Z}_2$. There is only one group of order 3. We know there are at least two different groups of order 4, Z_4 and V_4. One of them is not cyclic. In fact V_4 is the smallest non-cyclic group. You might try to show that these are the only two possible groups of order 4. Which of these is $\mathbf{Z}_2 \oplus \mathbf{Z}_2$? We know of at least two groups of order 6, $\mathbf{Z}_6$ and D_3. We have seen that D_3 is tha same as S_3. D_3 is the smallest non-abelian group we have seen. Is there a smaller one? Are there other groups of order 6?

7.4 Consequences for Small Groups

Example 12 Suppose that G is a group of order p^2 where p is prime. Show that either G is cyclic or $g^p = e$ for all $g \in G$.

SOLUTION Suppose that G is not cyclic. Then we must show that $g^p = e$ for all $g \in G$. But $|g|\,\Big|\,|G| = p^2$, so $|g|$ is either 1, p, or p^2. The last case is impossible for we have assumed that G is not cylic. But then we are done, for now $|g|$ is either 1 or p and in either case $g^p = e$. ∎

Example 13 Suppose that G is a group of order p^2 where p is prime. Show that G must have a proper subgroup of order p. ∎

SOLUTION Break it into cases: G is either cyclic or not. What does our work above tell you about the latter case? In the former, if you have an element g of order p^2, can you find an element of order p? ∎

Example 14 Let G be a non-abelian group of order $2p$ where $p \neq 2$ is prime. Show G has a cyclic subgroup of order p and it also has p elements of order 2.

SOLUTION We know that if $a \in G$ with $a \neq e$, then $|a|\,\Big|\,2p$, so $|a| = 2$ or p or $2p$. If $|a| = 2p$, then G would be cyclic and hence abelian. If $a^2 = e$ for **all** elements in G, then we showed (about week 2 or 3) that G would be abelian. This is also a current homework problem. So G has some element a of order p and $H =< a >$ is a cyclic subgroup of order p. Le g be any one of the remaining p elements not in H. Note that $G = H \cup gH$. By cancellation $g^2 \notin aH$ (else $g^2H = gH \Rightarrow gH = H$), so $g^2 \in H$. Further, $|g|$ is either 2 or p. (Why?)

If $|g| = p$, then

$$|g^2| = \frac{p}{\gcd(p,2)} = p.$$

But $< g^2 >$ is a subgroup of $< g >$ and since both subgroups have order p, they must be equal. But $g^2 \in H$ implies that $< g^2 >$ is a subgroup of H and since $< g^2 > = < a >$ then $a \in H$. But this is a contradiction. So the order of g must have been 2. ∎

Let's apply this last result to a non-abelian group G of order $2 \times 3 = 6$. The example shows that we have an element x of order 3 and an element a of order 2. Then $< x > = \{e, x, x^2\} = H$. And G is composed of the two disjoint cosets: $G = H \cup aH$, where $aH = \{a, ax, ax^2\}$. Of course this means that $G = \{e, x, x^2, a, ax, ax^2\}$. We know that $a^2 = e$

since it has order 2. Let's see if we can fill in the Cayley Table for $G = \{e, x, x^2, a, ax, ax^2\}$. Here's what we know so far:

$\cdot$	e	x	x^2	a	ax	ax^2
e	e	x	x^2	a	ax	ax^2
x	x	x^2	e			
x^2	x^2	e	x			
a	a	ax	ax^2	e	x	x^2
ax	ax	ax^2	a		e	
ax^2	ax^2	a	ax			e

The rest is a homework problem. Can we fill in the spot in the x-row and a-column? Show that the only possibilities (since the table is a Latin Square) are that xa equals either ax or ax^2. Suppose that $xa = ax$; then show from the group table that the group ends up being abelian. (Can you give a better reason: if $xa = ax$, show that all the a's would commute with all the x's and since every element in G is written using a's and x's, G would be abelian.) Therefore, we must have $xa = ax^2$. And now the rest of the table can be filled in.

Example 15 Find all possible groups (up to isomorphism) of order 8 or less.

SOLUTION If $|G| = 1$, then the group consists of the identity element alone. If $|G|$ is $p = 2, 3, 5, 7$, these values of p are prime, so G is cyclic of order p and so $G \cong \mathbf{Z}_p$.

Now suppose that $|G| = 4$. Either G is cyclic (and isomorphic to $\mathbf{Z}_4$), or it is not. Suppose that $G = \{e, a, b, c\}$ is not cyclic. Then since the order of each element must divide the order of the group and since only e has order 1, then $|a| = |b| = |c| = 2$. So G is abelian, and from the Fundamental Theorem of Finite Abelian Groups, we must have $G \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2 \cong V_4$.

What about $|G| = 6$? If G is abelian, then the Fundamental Theorem again says that $G \cong \mathbf{Z}_2 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_6$, so in fact G is cyclic. If G is not abelian, then it must be the non-abelian group of order 6 whose table we filled in above. This table should be familiar: it is D_3 (which we have also seen is isomorphic to S_3 by interpretting the motions of the triangle as permutations of the vertices 1, 2, 3 of the the triangle).

What about groups of order 8? Which do we know? Suppose G is abelian. Then the maximum order of its elements could be 8, 4, or 2. If G is abelian, then by the Fundamental Theorem for Finite Abelian Groups, G is isomorphic to either $\mathbf{Z}_8$, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, or $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$. If G is not abelian, it has no element of order 8 (else it would be cyclic). If it has no elements of order 4, then all its non-identity elements would be order 2. But then G would be abelian. So G has an element of order 4, call it x and let $< x >= H$. As in the order $2p$-example, choose $a \notin H$. Then $G = H \cup aH$ again. so $G = \{e, x, x^2, x^3, a, ax, ax^2, ax^3\}$. Now it gets trickier. See if you can figure out what the possibilities are for xa this time!!! **I will give you a boat load of extra credit if you can figure out all the possibilities.**