NOTES ON GROUPS, MATH 369.101

Subgroups

Definition 1. A **subgroup** $H \subset G$ is a subset H of a group G which (using the same operation as in G) is itself a group.

Because of Corollary 3.2.3, we get the following.

Corollary 1. *Let G be a group and H a finite, non-empty subset of G. Then H is a subgroup if and only if $ab \in H$ for all a, b in H.*

Proof. If H is a subgroup then $a, b \in H \quad \Rightarrow \quad ab \in H$ is clear.

If, for any $a, b \in H$ we have $ab \in H$ then, in particular, $b^k \in H$ for $k > 0$. Since $|H| < \infty$, if $b \neq e$ (the identity of G), then there is some pair $i > j$ so that $b^i = b^j$, and so $b^{i-j} = e$, which means $b^{i-j-1} = b^{-1} \in H$. So we've shown $b \in H$ implies $b^{-1} \in H$, and so $a, b \in H$ implies $ab^{-1} \in H$, and so H is a subgroup by Corollary 3.2.3. □

Example:

(1) In the circle group $\mathbb{S}$, say you want a subgroup (as small as possible) containing $e^{i\frac{2\pi}{3}}$ and $e^{i\frac{\pi}{2}}$. From Corollary 1 we should make sure all possible products are in it.

For example, $e^{i\frac{3\pi}{2}} = (e^{i\frac{\pi}{2}})^3$ should be in there; and then we need $e^{i\frac{2\pi}{3}} e^{i\frac{3\pi}{2}} = e^{i\frac{13\pi}{6}} = e^{i\frac{\pi}{6}}$ to be in it also. Then that means we need all powers of $e^{i\frac{\pi}{6}}$:

$$H = \{1, e^{i\frac{\pi}{6}}, e^{i\frac{\pi}{3}}, e^{i\frac{\pi}{2}}, e^{i\frac{2\pi}{3}}, e^{i\frac{5\pi}{6}}, e^{i\pi} = -1, e^{i\frac{7\pi}{6}}, e^{i\frac{4\pi}{3}}, e^{i\frac{3\pi}{2}}, e^{i\frac{5\pi}{3}}, e^{i\frac{11\pi}{6}}\}.$$

Now note that H is a subgroup of $\mathbb{S}$ by Corollary 1.

Cyclic subgroups.

Definition 2. $\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbb{Z}\}$ is the **cyclic subgroup generated by** a.

G is **cyclic** if $\exists\, a \in G$ so that $G = \langle a \rangle$, and then a is a **generator** of G.

Examples:

(1) under normal addition, $\mathbb{Z} = \langle 1 \rangle$
(here $a = 1$ and a^n means $1 + 1 + \ldots + 1$ (n times)).

(2) $K = \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$ is a cyclic subgroup of $\mathrm{GL}_2(\mathbb{R})$. $|K| = 4$.

Date: Nov. 7 – Nov. 9.

(3) $(\mathbb{Z}_7)^\times = \langle 3 \rangle$ (recall, for a ring R, $R\times$ means the set of elements of R with a multiplicative inverse, with multiplication as the operation):

$$3^1 = 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1.$$

If a group is finite ($|G| < \infty$), then the order $o(a)$ is finite for each $a \in G$. And in this case, G will be cyclic exactly when there exists an a so that $o(a) = |G|$. If there is no such a, then G is not cyclic, but each $\langle a \rangle$ is a cyclic subgroup that has size $o(a)$.

While we have essentially proved this already, we point out:

Proposition 1. *If $o(a)$ is finite for $a \in G$ and $k \in \mathbb{Z}$ is such that $a^k = e$, then $o(a)|k$.*

Proof. We showed last class that $a^i = a^j$ if and only if $i \equiv j (\text{mod } o(a))$. Since $e = a^0$, this means $k \equiv 0 (\text{mod } o(a))$ which means $o(a)|k$. □

Sometimes $(\mathbb{Z}_n)^\times$ is cyclic, sometimes it isn't. We saw in example (3) above that $(\mathbb{Z}_7)^\times$ is cyclic. However, $(\mathbb{Z}_8)^\times$ consists of elements $\{1, 3, 5, 7\}$ and $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. So, except for the identity ($g = 1$), we have $o(g) = 2$ for every $g \in (\mathbb{Z}_8)^\times$. Since $|(\mathbb{Z}_8)^\times| = 4$ the group cannot be cyclic.

Lemma 1. *For a subgroup H of G, define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.*

Proof. To show it is an equivalence relation, we need to show it is reflexive ($a \sim a$ for all $a \in G$), symmetric ($a \sim b$ implies $b \sim a$ for all $a, b \in G$), and transitive ($a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in G$).

Reflexive: $a \sim a \iff aa^{-1} \in H$. Since H is a subgroup and $aa^{-1} = e$, this is true.

Symmetric: Suppose $a \sim b$. Then $ab^{-1} \in H$. Since H is a subgroup, $ba^{-1} = (ab^{-1})^{-1}$ is in H. This is the definition of $b \sim a$.

Transitive: Suppose $a \sim b$ and $b \sim c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$. Then since a product of elements in H is in H, $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$, and so $a \sim c$. □

Note: congruence mod n is a special case, $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

Theorem 1. *(Lagrange). If H is a subgroup of G and G is a finite group, then $|H|$ divides $|G|$.*

Proof. Let $[a]$ be the set of $b \in G$ such that $a \sim b$ (where $\sim$ is as in the previous lemma). For any $a \in G$, the function $\rho_a : H \to [a]$ defined by $\rho_a(x) = xa$ is well-defined (meaning $xa \in [a]$) since $xa(a^{-1}) = x \in H$ shows that $xa \sim a$ for any $x \in H$. It is also bijective:

If $\rho_a(x) = \rho_a(y)$ then $xa = ya$. By multiplying by a^{-1} on the right, $x = y$. This shows ρ_a is one-to-one.

If $b \in [a]$ then $a \sim b$ so $b \sim a$, and so $ba^{-1} \in H$. But then $\rho_a(ba^{-1}) = b$. Since b could be anything in $[a]$, ρ_a is onto.

Now that we know ρ_a is bijective for *any* $a \in G$, note that each element of G is in exactly one equivalence class (since by the above Lemma, $\sim$ is an equivalence relation). If $[a]$ is one of the equivalence classes, then ρ_a being bijective implies that $[a]$ has exactly $|H|$ elements in it. This is true for every a. So $|G| = t|H|$ where t is the number of distinct equiv. classes. □

Corollary 2. *Say $|G| = n$. Then $o(a)|n$ and $a^n = e$ for all $a \in G$.*

Proof. Since for any $a \in G$, $\langle a\rangle$ is a subgroup and it has size $o(a)$, Lagrange's theorem says that $o(a)$ must divide $n = |G|$. This implies that $n = k \cdot o(a)$ for some integer k. But then

$$a^n = (a^{o(n)})^k = e^k = e.$$

□

Corollary 3. *If $|G|$ is a prime, then G is cyclic.*

Proof. Choose some $a \in G$ and consider the subgroup $\langle a\rangle$. If $|\langle a\rangle| = 1$ then $o(a) = 1$ and a must be the identity. Otherwise, $|\langle a\rangle|$ is a divisor of $|G|$ that is bigger than 1. Since $|G|$ is a prime number, we must have $|\langle a\rangle| = |G|$, and so $G = \langle a\rangle$. □

Examples:

(1) The group of symmetries D of an equilateral triangle has 6 elements. So every subgroup of this group has size 1,2,3, or 6 by Lagrange's theorem. One element would simply mean the subgroup $\{e\} \subset D$, and 6 elements would mean the whole group. Every other subgroup has 2 or 3 elements, and any such subgroup would be cyclic by the last Corollary.

(2) Along the same lines as the last example, if a group G has n elements in it and the prime decomposition of n is p_1p_2, where p_1, p_2 are each primes, then every subgroup of G (other than $\{e\}$ and G itself) is a cyclic subgroup, either of size p_1 or of size p_2. Note that this does not mean that G is cyclic.

The above (and when n is prime) is basically the only time this works. If $|G|$ has 3 or more prime factors (like $30 = 2 \cdot 3 \cdot 5$), or has a prime being raised to a power more than 1 in its prime decomposition (like $4 = 2^2$, or $18 = 2 \cdot 3^2$), then you cannot guarantee that every proper (not equal to G or $\{e\}$) subgroup is cyclic – though it may well be true, such as for $(\mathbb{Z}_4, +)$.

In order to better understand the groups $(\mathbb{Z}_n)^\times$, we introduce Euler's totient function $\varphi : \mathbb{Z} \to \mathbb{Z}$. By definition, $\varphi(n)$ equals the number of $i \in \{1, 2, \ldots, n\}$ such that $\gcd(n, i) = 1$. Here are it's values for the first 10 values of n:

n	$\varphi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

Note that $\varphi(n)$ is the size of the group $(\mathbb{Z}_n)^\times$. A few comments:

(1) If n is a prime number then $\varphi(n) = n - 1$, since $\gcd(n, i)$ will be 1 for all $i \leq p - 1$.

(2) If $n = p^k$ for some $k > 0$ then the only numbers between 1 and n that are not relatively prime to n are multiples of p: $p, 2p, 3p, \ldots, (p^{k-1})p$. So in that case $\varphi(p^k) = p^{k-1}(p - 1)$.

There is a nice formula for computing $\varphi(n)$.

Proposition 2. $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, *where the product is being taken over all distinct primes p which divide n.*

Proof. The proof depends on a fact we won't prove: that φ is multiplicative. That is $\varphi(mn) = \varphi(m)\varphi(n)$.

Note that $1 - \frac{1}{p} = \frac{p-1}{p}$. Now suppose that the prime decomposition of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$. Then

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_m^{k_m}) \\ &= \prod_{i=1}^{m} p_i^{k_i - 1}(p_i - 1) \\ &= \left(\prod_{i=1}^{m} p_i^{k_i}\right)\left(\prod_{i=1}^{m} \frac{p_i - 1}{p_i}\right) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \end{aligned}$$

□

Exercise: Show that $\varphi(n)$ is even for any $n \geq 3$.
Exercise: Describe all proper subgroups of $(\mathbb{Z}_{23})^\times$.