MATH 436 Notes: Subgroups and Cosets.

Jonathan Pakianathan

September 15, 2003

1 Subgroups

Definition 1.1. *Given a group $(G, \star)$, a subset H is called a subgroup of G if it itself forms a group under $\star$. Explicitly this means:*

(1). The identity element e lies in H.(H has an identity)
(2). For $h_1, h_2 \in H$, $h_1 \star h_2 \in H$. (H is closed under $\star$.)
(3). If $h \in H$ then $h^{-1} \in H$. (H has inverses.)

We write $H \leq G$ whenever H is a subgroup of G.

Note a nonempty subset H of G satisfying (2) and (3) above will be a subgroup as we may take $h \in H$ and then (2) gives $h^{-1} \in H$ after which (3) gives $hh^{-1} = e \in H$. However in general, the 3 conditions are independent from each other and hence must all be checked as the next few "nonexamples" show:

Example 1.2 (Nonexamples). *Let G be the additive group of integers $\mathbb{Z}$.*

(a). If $S_1 = \emptyset$ then S_1 satisfies (2) *and* (3) *in the definition above but not* (1).
(b). If $S_2 = \mathbb{N}$ then S_2 satisfies (1) *and* (2) *but not* (3). *$\mathbb{N}$ is a submonoid of $\mathbb{Z}$ but not a subgroup.*
(c). If $S_3 = \{-1, 0, 1\}$ then S_3 satisfies (1) *and* (3) *but not* (2).
Thus S_1, S_2 and S_3 are not subgroups of $\mathbb{Z}$.

$\{e\}$ is always a subgroup of G which is called the trivial subgroup. G is also always a subgroup of G. A subgroup H of G with $H \neq G$ is called a proper subgroup of G.

The following definition is an important way of generating subgroups of a group G:

Definition 1.3. *Given a group G and a subset S, we define the subgroup generated by S, denoted $< S >$ as follows:*

$$< S >= \{s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n} | n \in \mathbb{N}, s_i \in S \text{ and } \epsilon_i = \pm 1 \text{ for all } 1 \leq i \leq n\}.$$

Thus $< S >$ consists of all finite products of elements of S and their inverses.

Since e can be either considered as an empty product or as ss^{-1} for some $s \in S$, it is a routine exercise to show that $< S >$ is a subgroup of G. Indeed it is easily seen to be the smallest subgroup of G containing S as any other subgroup H containing S must contain all such finite products of elements of S and their inverses and hence $< S > \leq H$.

We record some special cases next:

Definition 1.4. *If $G =< S >$ for a finite set S then we say that G is finitely generated. Thus if $S = \{x_1, \dots, x_k\}$ for example then*

$$< S >= \{x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \dots x_{i_n}^{\pm 1} | n \geq 0, 1 \leq i_j \leq k\}.$$

Definition 1.5. *If $G =< x >$ for a single element x then we call G a cyclic group. In this case $G = \{x^n | n \in \mathbb{Z}\}$. Cyclic groups are always Abelian since if $a, b \in G$ then $a = x^n, b = x^m$ and $ab = x^{n+m} = ba$. The canonical example of a cyclic group is the additive group of integers $(\mathbb{Z}, +)$ which is generated by 1 (or -1).*

Example 1.6. *Let $a = (1, 2)$ and $b = (1, 3)$ in Σ_3 then one may show that $\Sigma_3 = \{e, a, b, ab, ba, aba\}$ and so $< a, b >= \Sigma_3$ and we say that Σ_3 is generated by the 2 generators a and b. This is the smallest generating set that one can find for Σ_3 as Σ_3 cannot be generated by one element as it is non-Abelian and hence non-cyclic.*

We next record all the subgroups of $\mathbb{Z}$. This in an important example as we will see later!

Theorem 1.7 (Subgroups of $\mathbb{Z}$). *Let $\mathbb{Z}$ be the additive group of integers. Then any subgroup of G is of the form*

$$< d >= d\mathbb{Z} = \{\dots, -2d, -d, 0, d, 2d, 3d, \dots\}$$

for a unique integer $d \geq 0$. Thus all subgroups of $\mathbb{Z}$ are cyclic.

Proof. It is clear that the $< d >$ are subgroups and that they are distinct for different $d \geq 0$. Thus it remains only to show that any subgroup of $\mathbb{Z}$ is one of these. So let H be a subgroup of G. If H is the trivial subgroup then $H =< 0 >$ and we are done so assume H is nontrivial. Then H has a nonzero element and hence has a positive element (since H has inverses). By the inductive property of $\mathbb{N}$ we can find a least positive element $d \in H$. Then $< d > \subset H$.

On the other hand if $n \in H$ we may use the division algorithm to write $n = qd + r$ where q, r are integers and $0 \leq r < d$. Since n and qd are in H, we see that $n + (-qd) = r$ is in H. Since $r < d$ is nonnegative and d is the smallest positive integer in H, we conclude that $r = 0$ or that $n = qd \in < d >$. Thus $H \subset < d >$ and so we have shown that $H =< d >$. □

2 Cosets

To proceed any further in the study of subgroups, we have to introduce the fundamental notion of a coset. Roughly speaking, a coset of H in G is a translation of the subgroup H by an element $g \in G$.

Definition 2.1. *Given $H \leq G$, a left coset of H in G is a subset of G of the form $gH = \{gh | h \in H\}$ for some $g \in G$. Similarly a right coset of H in G is a subset of G of the form $Hg = \{hg | h \in H\}$ for some $g \in G$. Notice since $g = eg = ge$ that $g \in Hg$ and $g \in gH$.*

Example 2.2. *Suppose $G = \Sigma_3$, $H =< (1,2) >= \{e, (1,2)\}$ and $g = (1,3)$. Then a simple computation shows that $gH = \{(1,3), (1,2,3)\}$ while $Hg = \{(1,3), (1,3,2)\}$ and so $gH \neq Hg$. Thus we see that for a fixed element g, the left coset gH may be different from the right coset Hg in general.*

Definition 2.3. *A subgroup N of G is called normal if $gN = Ng$ for all $g \in G$. We write $N \trianglelefteq G$.*

Note in an Abelian group G, all subgroups will be normal. However if G is non-Abelian, there might be some subgroups which are not normal, as we saw in the last example.

We now proves some fundamental facts about left cosets. Similar facts hold for right cosets with analogous proof left to the reader.

Proposition 2.4. *If $H \leq G$ then:*
(1). $hH = H$ for all $h \in H$.
(2). $g_1H = g_2H$ if and only if $g_1 = g_2h$ for some $h \in H$.
(3). Any two left cosets g_1H and g_2H are either equal as sets or disjoint.
(4). There is a bijection between each left coset gH and H. Thus each left coset has the same cardinality as H.

Proof. **Part (1):** $hH = \{hh' | h' \in H\} \subseteq H$ as H is closed under the group multiplication. On the other hand given $h'' \in H$ we may write $h'' = h(h^{-1}h'')$ and so $h'' \in hH$ as $h^{-1}h'' \in H$. Thus $H = hH$.
Part (2): If $g_1H = g_2H$ then $g_1 = g_1e \in g_1H = g_2H$ so we may write $g_1 = g_2h$ for some $h \in H$.
On the other hand, if $g_1 = g_2h$ for some $h \in H$ then $g_1H = g_2hH = g_2H$ by part (1).
Part (3): Suppose $g_1H \cap g_2H \neq \emptyset$. Then there is $\alpha \in g_1H \cap g_2H$ and so $g_1h_1 = \alpha = g_2h_2$ for some $h_1, h_2 \in H$. We then have $g_1 = g_2h$ where $h = h_2h_1^{-1} \in H$. Thus by Part (2), we have $g_1H = g_2H$.
Part (4): Define $f : H \to gH$ by $f(h) = gh$. It is easy to check that $q : gH \to H$ defined by $q(gh) = h$ is a two-sided inverse function to f. Thus f is a bijection and hence gH and H have the same cardinality. □

Definition 2.5. *If $H \leq G$ we define G/H to be the set of left cosets of H in G. Similarly we define $H\backslash G$ to be the set of right cosets of H in G. In an exercise in Homework 1, you show that there is a bijection between G/H and $H\backslash G$ and so we may define $|G : H| = |G/H| = |H\backslash G|$, the index of H in G. Thus the index of H in G is the number of distinct left (right) cosets of H in G.*

Example 2.6. *Consider the group $\mathbb{Z}$ of integers under addition and let us look at the subgroup $d\mathbb{Z} =< d >$. Now if $n \in \mathbb{Z}$ then $n = qd+r$ for integers q, r with $0 \leq r < d$. Since $qd \in d\mathbb{Z}$ we have $n + d\mathbb{Z} = r + qd + d\mathbb{Z} = r + d\mathbb{Z}$. Thus any coset $n+d\mathbb{Z}$ is the same as the coset $r+d\mathbb{Z}$ where r is the remainder when we divide n by d. On the other hand if $0 \leq r_1 < r_2 < d$ then $0 < r_2 - r_1 < d$ and so $r_2 - r_1 \notin d\mathbb{Z}$. Thus $r_1 + d\mathbb{Z} \neq r_2 + d\mathbb{Z}$ by part (2) of Proposition 2.4. Hence we see that $\mathbb{Z}/d\mathbb{Z} = \{0 + d\mathbb{Z}, 1 + d\mathbb{Z}, \ldots, (d-1) + d\mathbb{Z}\}$ and that $|\mathbb{Z}/d\mathbb{Z}| = d$. Thus $d\mathbb{Z}$ has index d in $\mathbb{Z}$.*

Now let G be a finite group. From Proposition 2.4, we see that the distinct left cosets of H partition G into disjoint pieces of equal cardinality, i.e., the

cardinality of H. Thus we have $|G| = \sum |g_i H| = |G : H||H|$ where the sum is taken over the distinct cosets and we have used that $|g_i H| = |H|$ for all g_i. Thus we have proven a famous theorem of Lagrange:

Theorem 2.7 (Lagrange's Theorem). *If G is a finite group and $H \leq G$ then $|H||G : H| = |G|$. Thus both $|H|$ and $|G : H|$ must divide $|G|$.*

Example 2.8. *Since $|\Sigma_3| = 3! = 6$ we conclude from Lagrange's Theorem that the only possible orders for a subgroup are 1,2,3 and 6. These are also the only possible values for the index of a subgroup of Σ_3.*

3 Quotient groups

Given a group G and $H \leq G$ we wish to define a group structure on G/H under suitable conditions. The natural way to do this is to define

$$g_1 H \star g_2 H = g_1 g_2 H$$

for all $g_1, g_2 \in H$.

Unfortunately in order for $\star$ to induce a binary operation on G/H we must show that it is a well-defined operation on left cosets. The definition given above relies too heavily on the representatives g_1, g_2 to be well-defined in general. Thus if $g_1 H = g_1' H$ and $g_2 H = g_2' H$ we must find conditions so that $g_1 g_2 H = g_1' g_2' H$. It is only under these conditions that $\star$ defines a well defined binary operation on G/H.

Now since $g_i H = g_i' H$, by Proposition 2.4 we may write $g_i = g_i' h_i$ for $h_i \in H$, $i = 1, 2$.

Then $g_1 g_2 = (g_1' h_1)(g_2' h_2) = g_1' g_2' (g_2')^{-1} h_1 g_2' h_2$. Thus $g_1 g_2 H = g_1' g_2' H$ if and only if $(g_2')^{-1} h_1 g_2' h_2 \in H$ for all $g_2' \in G, h_1, h_2 \in H$. Right multiplying by h_2^{-1} and setting $g = g_2', h = h_1$ we find that this is equivalent to $g^{-1} h g \in H$ for all $g \in G, h \in H$, or in other words

$$g^{-1} H g \subseteq H \text{ for all } g \in G. \tag{1}$$

Since inclusion (1) holds for all $g \in G$ we may replace g with g^{-1} from which we get $g H g^{-1} \subseteq H$ which gives $H \subseteq g^{-1} H g$. Using this with inclusion (1) gives $g^{-1} H g = H$ for all $g \in G$ or in other words H is normal in G.

Thus the binary operation $\star$ above defines a well-defined binary operation on G/H if and only if H is a normal subgroup of G.

In this case, it is easy to see that $\star$ makes G/H into a group as the group properties are easily inherited from G. For example $eH = H$ is the identity element and $(gH)^{-1} = g^{-1}H$. We record this below:

Proposition 3.1 (Quotient groups). *If N is a normal subgroup of G, then G/N inherits a group structure from G via $g_1N \star g_2N = g_1g_2N$. We call G/N the quotient group of G by N.*

Example 3.2 (Additive Group of Integers modulo d). *From Example 2.6, we have that $\mathbb{Z}/d\mathbb{Z} = \{0 + dZ, 1 + dZ, \ldots, (d-1) + d\mathbb{Z}\}$. Since $\mathbb{Z}$ is Abelian, $d\mathbb{Z}$ is normal in $\mathbb{Z}$ and so the addition in $\mathbb{Z}$ induces an addition on $\mathbb{Z}/d\mathbb{Z}$ that makes it an Abelian group.*

For example in $\mathbb{Z}/5\mathbb{Z}$, we have $(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$. Thus the addition in $\mathbb{Z}/d\mathbb{Z}$ is like that of normal integers except that the answer is expressed modulo d, i.e., the remainder after dividing by d is used. The group $\mathbb{Z}/d\mathbb{Z}$ is called the additive group of integers modulo d. We often write $\bar{n}$ instead of $n + d\mathbb{Z}$ to simplify the notation, thus for example the above computation in $\mathbb{Z}/5\mathbb{Z}$ can be written: $\bar{3} + \bar{4} = \bar{2}$ modulo 5.

It is easy to see that the group $(\mathbb{Z}/d\mathbb{Z}, +)$ is cyclic of order d with generator $\bar{1}$ for example.

On occasion it is useful also to discuss quotient monoids. We will not do this systematically but just illustrate it with the following example which is probably the most important:

Example 3.3 (Multiplicative Monoid of Integers modulo d). *The integers $\mathbb{Z}$ are a monoid under multiplication of integers. $\mathbb{Z}/d\mathbb{Z}$ can also be given a multiplicative structure from this multiplication via $(n + d\mathbb{Z})(m + d\mathbb{Z}) = (nm + d\mathbb{Z})$. The main thing is to check that this is well-defined. Once it is, it is clear that it makes $\mathbb{Z}/d\mathbb{Z}$ into an Abelian monoid under multiplication with identity $1 + d\mathbb{Z} = \bar{1}$.*

To check well-definedness, suppose $n' + d\mathbb{Z} = n + d\mathbb{Z}$ and $m' + d\mathbb{Z} = m + d\mathbb{Z}$ and hence $n' = n + dk$, $m' = m + dt$ for $k, t \in \mathbb{Z}$. We then compute

$$n'm' = (n + dk)(m + dt) = nm + d(km + nt + dkt).$$

Since $km + nt + dkt \in \mathbb{Z}$, we have $n'm' + d\mathbb{Z} = nm + d\mathbb{Z}$ and so multiplication on $\mathbb{Z}/d\mathbb{Z}$ is well-defined.

Example 3.4 (Multiplicative Group of Units modulo d). *The group of units in the Abelian monoid $(\mathbb{Z}/d\mathbb{Z}, \cdot)$ is denoted $(\mathbb{Z}/d\mathbb{Z})^*$. Thus*

$$(\mathbb{Z}/d\mathbb{Z})^* = \{\bar{n}| \text{ There is a } \bar{s} \text{ such that } \bar{n}\bar{s} = \bar{1}\}.$$

In an exercise in Homework 2, you will show that for $d \geq 1$,

$$(\mathbb{Z}/d\mathbb{Z})^* = \{\bar{n}|1 \leq n \leq d, gcd(n, d) = 1\}.$$

Let $\mathbb{N}^+$ be the set of positive integers, then Euler's phi function $\phi : \mathbb{N}^+ \to \mathbb{N}^+$ is defined via $\phi(d) = |\{n|1 \leq n \leq d \text{ such that } gcd(n, d) = 1\}|$. Thus $|(\mathbb{Z}/d\mathbb{Z})^*| = \phi(d)$ for all $d \geq 1$.