## 9th Lecture: 10/2

To begin with, some more words on Example 8.14+ from the last day. In the notation of Figure 8.1, every element of $S_3$ can be written in terms of the elements denoted $g$ and $h$. These elements are said to form a *(minimal) set of generators* for $S_3$. In order to determine the structure of the group precisely, we also need to specify the so-called *relations* between the generators. Once again, we seek a minimal set of relations, such that any other relation is a consequence of these and the general properties of any group operation. For a group generated by two elements, it suffices to give the so-called *order* of each generator and the *commutator* between them.

**Definition 9.1.** Let $G$ be a group and $g \in G$. The *order* of $g$ is the least positive integer $n \in \mathbb{Z}_+$ such that $g^n = 1$. If no such $n$ exists we say that $g$ has *infinite order*.

**Definition 9.2.** Let $G$ be a group and $x, y \in G$. The *commutator* of $x$ and $y$ is the group element $[x, y] := x^{-1}y^{-1}xy$.

NOTE: In many books you'll see the commutator of $x$ and $y$ defined as $xyx^{-1}y^{-1}$. It doesn't matter which definition you use as long as you're consistent.

**Observation 9.3.** If $G$ is a finite group then every element $g \in G$ has finite order. For, since $G$ is finite, the elements $g^n$, $n \in \mathbb{Z}_+$, can't all be distinct. Hence there must exist some $0 < i < j$ such that $g^i = g^j$. Since $g$ is a group, the element $(g^i)^{-1}$ exists and it is clear that $(g^i)^{-1} = g^{-i}$. Thus $g^{-i} \cdot g^i = g^{-i} \cdot g^j \Rightarrow 1 = g^{j-i}$ and so the order of $g$ is at most $j - i$.

For a more precise statement, see Corollary 9.15 below.

**Observation 9.4.**

$$\begin{aligned}
[x, y] = 1 &\Leftrightarrow x^{-1}y^{-1}xy = 1 \\
&\Leftrightarrow x(x^{-1}y^{-1}xy) = x \cdot 1 = x \\
&\overset{\text{assoc}}{\Leftrightarrow} (xx^{-1})y^{-1}xy = x \\
&\Leftrightarrow y^{-1}xy = x \\
&\Leftrightarrow y(y^{-1}xy) = yx \\
&\overset{\text{assoc}}{\Leftrightarrow} (yy^{-1})xy = yx \\
&\Leftrightarrow xy = yx.
\end{aligned}$$

In other words, the commutator of $x$ and $y$ equals 1 if and only if $x$ and $y$ commute (which explains the terminology). In particular, $G$ is abelian if and only if $[x, y] = 1 \; \forall \, x, y \in G$.

Returning to the example of $S_3$, we get the following relations:

(i) $g^3 = 1$ (120-degree rotation times three is the identity)
(ii) $h^2 = 1$ (reflection times two is the identity)

(iii)

$$[g,\, h] = g^{-1}h^{-1}gh = g^2hgh = g(ghgh) = g(gh)^2 = g \cdot 1 = g.$$

We can put the generators and relations together into a so-called *presentation* of $S_3$:

$$S_3 = <\, g,\, h : g^3 = h^2 = 1,\, [g,\, h] = g >\, .$$

The point is that a presentation of a group gives a complete, but *purely algebraic* description of it. All properties of the group can be derived purely algebraically from the presentation, using the group axioms (Definition 8.15).

**Definition 9.5.** Let $G$ be a group and $H$ a subset of $G$. $H$ is said to be a *subgroup* of $G$ if

(i) $H$ is closed under the group operation

(ii) $1 \in H$

(iii) $h \in H \Rightarrow h^{-1} \in H$.

**Remark 9.6.** In the case of a finite group $G$, conditions (ii) and (iii) are superfluous - see Homework 2.

**Remark 9.7.** In any group $G$ there are at least two possibilities for a subgroup, either $H = \{1\}$ or $H = G$. The former is called the *trivial* subgroup and the latter is said to be an *improper* subgroup. Every other subgroup is said to be *proper*.

**Example 9.8.** Let's list all the subgroups of $S_3$. First we have the trivial examples guaranteed by Remark 9.7:

$$H_1 = \{1\}, \quad H_2 = S_3.$$

Secondly, any reflection plus the identity will form a subgroup of size 2:

$$H_3 = \{1,\, h\}, \quad H_4 = \{1,\, gh\}, \quad H_5 = \{1,\, g^{-1}h\}.$$

Finally, the rotations form a subgroup of size 3:

$$H_6 = \{1,\, g,\, g^2 = g^{-1}\}.$$

Note that the size of every subgroup is a divisor of 6, the size of $S_3$ itself. This is not a coincidence - see Theorem 9.13 below.

**Definition 9.9.** Let $G$ be a group, $H$ a subgroup of $G$ and $x \in G$. The set

$$Hx = \{g \in G : g = hx \;\exists\, h \in H\}$$

is called a *(right) coset* of $H$ in $G$.

**Proposition 9.10.** *Let $G$ be a group, $H$ a subgroup of $G$ and $x,\, y \in G$. Then either $Hx \cap Hy = \phi$ or $Hx = Hy$.*

PROOF: Suppose $Hx \cap Hy$ is non-empty. Thus there exist $h_1,\, h_2 \in H$ such that $h_1x = h_2y$. Since $G$ is a group we deduce that

$$x = h_1^{-1}(h_1x) = h_1^{-1}(h_2y) = (h_1^{-1}h_2)y.$$

Since $H$ is a subgroup, the element $h_1^{-1}h_2$ also belongs to $H$. Thus $x = hy \; \exists \, h \in H$. Now let $g \in Hx$, so $g = h_3 x$ for some $h_3 \in H$. Then $g = h_3(hy) = (h_3 h)y = h_4 y$, since $H$ is closed. Thus $g \in Hy$ so we have shown that $Hx \subseteq Hy$. Clearly, a completely analogous argument shows the reverse inclusion and so $Hx = Hy$, v.s.v.

**Remark 9.11.** One can formulate Proposition 9.10 in terms of equivalence relations. Let $G$ be a group and $H$ a subgroup. Define a relation $\sim_H$ on $G$ by

$$x \sim_H y \Leftrightarrow xy^{-1} \in H.$$

I leave it as an exercise to show that $\sim_H$ is an equivalence relation on $G$ and that the equivalence classes are the right cosets of $H$.

**Remark 9.12.** One can just as well work with *left* cosets $xH = \{xh : h \in H\}$. As usual, the important thing is to be consistent. The left cosets of $H$ will also partition $G$ (analog of Prop. 9.10.) and the corresponding equivalence relation is $x \sim y \Leftrightarrow y^{-1}x \in H$. Note that if $G$ is abelian then $xH = Hx \; \forall \, x \in G$. This may even be true in some non-abelian settings, e.g.: $G = S_3$ and $H = H_6$ in Example 9.8.

**Theorem 9.13. (Lagrange's Theorem for Groups)** *Let $G$ be a finite group and $H$ a subgroup. Then $|H|$ divides $|G|$.*

PROOF: This will follow immediately from Proposition 9.10 if we can show that all the right cosets of $H$ have the same size. I claim that every right coset has size $|H|$. Let $Hx$ be a coset. We have the natural map $h \mapsto hx$ from $H$ to $Hx$, so it suffices to verify that this map is injective. But

$$h_1 x = h_2 x \Rightarrow (h_1 x)x^{-1} = (h_2 x)x^{-1} \Rightarrow h_1(xx^{-1}) = h_2(xx^{-1}) \Rightarrow h_1 = h_2, \text{ v.s.v.}$$

**Definition 9.14.** Let $G$ be a group and $g \in G$. Consider the set of all powers of $g$, i.e.: $H = \{g^n : n \in \mathbb{Z}\}$. This subset of $G$
(i) is closed under the group operation: $g^m g^n = g^{m+n}$
(ii) contains the identity: $1 = g^0$
(iii) contains inverses: $(g^n)^{-1} = g^{-n}$.
Hence, $H$ is a subgroup of $G$. It is called the *cyclic subgroup* generated by $g$ and denoted $H = < g >$.

**Corollary 9.15.** Let $G$ be a finite group and $g \in G$. Then the order of $g$ divides $|G|$ and $g^{|G|} = 1$.

PROOF: The first statement follows from Theorem 9.13, applied to $H = < g >$. This is because, if $n$ is the order of $g$, then the powers $1 = g^0$, $g = g^1$, $g^2$, $\ldots$, $g^{n-1}$ are all distinct elements of $G$ (otherwise $g^m = 1$ would hold for some $1 \leq m < n$, see Observation 9.3) and every power of $g$ coincides with one of these: $g^{qn+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r$. In other words, $| < g > |$ equals the order of $g$.

The second statement then follows immediately also: $g^{|G|} = (g^{|H|})^{|G|/|H|} = 1^{|G|/|H|} = 1$, since the quotient $|G|/|H|$ is an integer, by Theorem 9.13.

Corollary 9.15 will be used to prove the *Euler/Fermat Theorem* in modular arithmetic in the next lecture.

**Rings and Fields.** In the last two lectures I have given a brief introduction to Group Theory. In a course on abstract algebra you will go further and also get a "proper" introduction to rings and fields. Here I am just going to give the bare minimum (definitions and a couple of examples) which we will need when we turn to modular arithmetic.

**Definition 9.16. (I)** Let $R$ be a set equipped with two binary operations, the default notation and terminology for which are $+$ (addition) and $\times$ (multiplication). The triple $(R,\, +,\, \times)$ is said to be a *ring* if the following hold:
(i) $(R,\, +)$ is an abelian group (the identity element for $+$ is denoted $0$)
(ii) $\times$ is associative
(iii) $\times$ is *distributive over* $+$, meaning that the following two equations hold for all $a,\, b,\, c \in R$:

$$a \times (b + c) = (a \times b) + (a \times c),$$
$$(b + c) \times a = (b \times a) + (c \times a).$$

**(II)** If there exists an identity for $\times$ (usually denoted $1$) then the ring is said to be *a ring with unity*.
**(III)** If $\times$ is commutative then the ring is said to be a *commutative ring*.
**(IV)** If there exists an identity for $\times$ and every non-zero element of $R$ possesses a multiplicative inverse, then the ring is said to be a *division ring*.
**(V)** A commutative division ring is called a *field*.

**Examples 9.17. (I)** $(\mathbb{Z},\, +,\, \times)$ is a ring with unity, under ordinary addition and multiplication of numbers.

**(II)** $(\mathbb{Q},\, +, \times)$ is a field and is the smallest field containing the ring $\mathbb{Z}$. $\mathbb{R}$ and $\mathbb{C}$ are also fields under ordinary addition and multiplication.

**(III)** For $n \geq 2$, $\mathbb{M}_n(\mathbb{R})$ is a non-commutative ring with unity, under addition and multiplication of matrices. Note that it is not a division ring, since not all non-zero matrices are invertible. Nor could we get a division ring by replacing $\mathbb{M}_n(\mathbb{R})$ by $\mathbf{GL}_n(\mathbb{R})$, since the latter is not closed under matrix addition, i.e.: the sum of two invertible matrices need not be invertible.

Note also that one can replace $\mathbb{R}$ by either $\mathbb{Q}$ or $\mathbb{C}$, since the operations of matrix addition and multiplication preserve membership of these sets (even matrix inversion does so, by the adjoint formula for a matrix inverse). Hence, more abstractly, one can replace $\mathbb{R}$ by any field.

**(IV)** More generally, we can form rings of functions under pointwise addition and composition of functions. But in order for the former to make sense, it has to be possible to add elements in the underlying set on which the functions are defined. Hence: let $(G,\, +)$ be an abelian group. Then $(G^G,\, +,\, \circ)$ is a ring, where $G^G$ is the set of all functions from (the set) $G$ to itself, $+$ is pointwise addition of functions

$((f_1 + f_2)(g) = f_1(g) + f_2(g))$ and $\circ$ is function composition $((f_1 \circ f_2(g) = f_1(f_2(g)))$. Note that the distributive laws hold:

$$f_1 \circ (f_2 + f_3) = (f_1 \circ f_2) + (f_1 \circ f_3), \quad (f_1 + f_2) \circ f_3 = (f_1 \circ f_3) + (f_2 \circ f_3).$$

The ring $G^G$ always has a unity (the identity function) but is non-commutative whenever $|G| > 1$ (see Example 8.14). The invertible elements are the permutations of $G$, hence $G^G$ is in general not a division ring and we can't get a division ring by restricting to the subset $S_G$ of $G^G$ (the set of permutations of $G$) because the sum of two permutations won't in general be a permutation.

**Remark 9.18.** The ring containing a single element $0$ and where $0 + 0 = 0 \times 0 = 0$ is called the *trivial ring*. Regarding item **(IV)** in Definition 9.16, one can show that, in any non-trivial ring, the zero element can't have a multiplicative inverse - see Homework 2.