21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

9- Monday September 19, 2011.

Definition 9.1: An *action of a group G on a set X* is an homomorphism from G into S_X, the group of bijections of X. Equivalently, it is a mapping from $G \times X$ into X satisfying $e\,x = x$ for all $x \in X$, and $g_1(g_2 x) = (g_1 g_2)\,x$ for all $g_1, g_2 \in G$ and all $x \in X$, where $g\,x$ denotes the image of (g, x) by the mapping.[1]

For $x \in X$, the *orbit of x* is $\{g\,x \mid g \in G\} \subset X$, the *stabilizer of x* is $Stab(x) = \{g \in G \mid g\,x = x\} \subset G$.

Remark 9.2: For example, an action of $\mathbb{Z}_n$ on X is the same as having a bijection f from X onto itself satisfying $f \circ \cdots \circ f = id_X$, where there are n factors.

An action of $\mathbb{Z}_2 \times \mathbb{Z}_2$ on X is the same as having two bijections f and g from X onto itself satisfying $f \circ f = g \circ g = id_X$ and $f \circ g = g \circ f$.

Lemma 9.3: The relation $x \mathcal{R} y$ if and only if there exists $g \in G$ with $g\,x = y$ is an equivalence relation, and the equivalence classes are the orbits, which then form a partition of X.
Proof: For all $x \in X$ one has $x \mathcal{R} x$, because $e\,x = x$; $x \mathcal{R} y$ means $g\,x = y$ for some $g \in G$, which is equivalent to $x = g^{-1} y$, implying $y \mathcal{R} x$; $x \mathcal{R} y$ and $y \mathcal{R} z$ mean $g\,x = y$ and $h\,y = z$ for some $g, h \in G$, so that $h\,g\,x = z$, implying $x \mathcal{R} z$. The definition of the equivalence class of x coincides with the definition of the orbit of x.

Lemma 9.4: For $x \in X$, $Stab(x) \leq G$. The mapping $g\,x \mapsto g\,Stab(x)$ is a bijection between the orbit of x and the left cosets of $Stab(x)$, so that the size of the orbit of x is the index of $Stab(x)$, which both divide the order of G if it is finite. In particular, for a prime p, and for any action of $\mathbb{Z}_p$, the orbits have size 1 or size p.
Proof: Because $e\,x = x$, one has $e \in Stab(x)$; if $g_1, g_2 \in Stab(x)$, then $g_1 x = g_2 x = x$ implies $(g_1\,g_2)\,x = g_1 x = x$, so that $g_1 g_2 \in Stab(x)$, and $g_1^{-1} x = g_1^{-1}(g_1 x) = x$, so that $g_1^{-1} \in Stab(x)$.

The mapping is well defined if $g_1 x = g_2 x$ implies $g_1 Stab(x) = g_2 Stab(x)$: indeed, $g_1 x = g_2 x$ means $g_2^{-1} g_1 x = x$, i.e. $g_2^{-1} g_1 \in Stab(x)$, which implies $g_1 \in g_2 Stab(x)$ so that $g_1 Stab(x) \subset g_2 Stab(x)$, and exchanging the roles of g_1 and g_2 gives equality. Then, the size of the orbit of x is the number of left cosets of $Stab(x)$, i.e. the index of $Stab(x)$, which by Lagrange's theorem divides the order of G if G is a finite group.

Example 9.5: G acts on itself by left multiplication:[2] $X = G$ and (g, x) is mapped to the usual product $g\,x$ in G for all $g, x \in G$. G is isomorphic to a subgroup of S_G, and in particular every group of order n is isomorphic to a subgroup of the symmetric group S_n (Cayley's theorem).
Proof: For $x, g_1, g_2 \in G$, (e, x) is mapped to $e\,x = x$, and $(g_1, g_2 x)$ is mapped to $g_1(g_2 x) = (g_1 g_2)\,x$. Then, the homomorphism from G into S_G is injective, because if $g \in G$ is mapped to the identity of S_G, it means that $g\,x = x$ for all $x \in G$, and taking $x = e$ gives $g = e$; the first isomorphism theorem tells then that G is isomorphic to the image, which is a subgroup of S_G.

Example 9.6: G acts on itself by conjugation: $X = G$ and (g, x) is mapped to $x^g = g\,x\,g^{-1}$.[3] The orbit of $x \in G$ is called the *conjugacy class* of x, and the stabilizer of x is called the *centralizer of x*, i.e. $C_G(x) = \{g \in G \mid g\,x = x\,g\}$,[4] and the size of the conjugacy class is the index of the centralizer (so that its size divides the order of G if G is finite).
Proof: For $x, g, h \in G$, one has $e\,x = x^e = x$, and $(x^g)^h = h\,(g\,x\,g^{-1})\,h^{-1} = (h\,g)\,x\,(h\,g)^{-1} = x^{h\,g}$.

---

[1] In some concrete examples the notation $g\,x$ may lead to confusion, like for Example 9.6 and Example 9.7 below, and it is better to avoid it.

[2] Using right multiplication, i.e. $(g, x) \mapsto x\,g$, does not satisfy the axioms if G is not Abelian, because $(g_1\,g_2, x)$ is mapped to $x\,g_1 g_2$, while (g_2, x) is mapped to $x\,g_2$, and $(g_1, x\,g_2)$ is mapped to $x\,g_2 g_1$.

[3] Here the notation $g\,x$ for (g, x) would be a little misleading. Notice that the notation x^g may also be confused with a power of x in some cases.

[4] If G is Abelian, then the conjugacy class of each $x \in G$ is reduced to $\{x\}$, and $C_G(x) = G$ for all $x \in G$; conversely, if $C_G(x) = G$ for all $x \in G$, then G is Abelian.

Example 9.7: G acts on the set of its subgroups by conjugation:[5] (g, H) is mapped to $H^g = \{g\,h\,g^{-1} \mid h \in H\}$. The stabilizer of $H \leq G$ is called the *normalizer* $N_G(H) = \{g \in G \mid g\,H = H\,g\}$ of H in G, so that one has $H \lhd N_G(H) \leq G$.

Lemma 9.8: $N_G(H)$ is the largest subgroup of G in which H is normal.[6]
Proof: For $K \leq G$, the condition $H \lhd K$ is equivalent to $k\,H = H\,k$ for all $k \in K$, i.e. $K \leq N_G(H)$.

Remark 9.9: If G acts on X, then G acts on any subset of X which is a union of orbits. If $H \leq G$, then H acts on each G-orbit, which is then partitioned as a union of H-orbits.

Definition 9.10: If p is prime and divides the order of a finite group G, a *p-subgroup* H of G is any subgroup whose order is a power of p. If p^n is the highest power of p which divides $|G|$, any $H \leq G$ with $|H| = p^n$ is called a *Sylow-p subgroup* of G.

Remark 9.11: Sylow's theorem will be proved in another lecture, and its proof will use action by conjugation on subgroups, and it is stated here and then used on two examples: if p is a prime and G is a group of order $|G| = p^n a$ (with $n \geq 1$) and p does not divide a, then, every p-subgroup of G is included in a Sylow p-subgroup, all Sylow p-subgroups are conjugate, and their number n_p is congruent to 1 modulo p, and divides $|G|$, so that it divides a. In particular, if there is a unique Sylow p-subgroup, then it is a normal subgroup (and a normal Sylow p-subgroup is unique).

Example 9.12: For a group G of order 15, then $n_3 = 1 \pmod 3$ and n_3 divides 5, so that $n_3 = 1$ and there is only one Sylow 3-subgroup H_3, $n_5 = 1 \pmod 5$ and n_5 divides 3, so that $n_5 = 1$ and there is only one Sylow 5-subgroup H_5, and since both H_3 and H_5 are normal subgroups of G it will be shown that $G \simeq H_3 \times H_5$, and since $H_3 \simeq \mathbb{Z}_3$ and $H_5 \simeq \mathbb{Z}_5$, one has $G \simeq \mathbb{Z}_{15}$ by the Chinese remainder theorem.

Example 9.13: For a group G of order 21, then $n_3 = 1 \pmod 3$ and n_3 divides 7, so that n_3 is either 1 or 7, $n_7 = 1 \pmod 7$ and n_7 divides 3, so that $n_7 = 1$ and there is only one Sylow 7-subgroup H_7, which is a normal subgroup of G.

If $n_3 = 1$, there is only one Sylow 3-subgroup H_3, which is a normal subgroup of G, and in this case $G \simeq \mathbb{Z}_{21}$.

If $n_3 = 7$, there are 7 Sylow-3 subgroups $K_1, \ldots, K_7$, and since $K_i \cap K_j = \{e\}$ for $i \neq j$, there are 14 elements of order 2, which with the 6 elements of order 7 in H_7 and e make up the group. For each K_i, the action by conjugation generates an orbit of size 7 (since it gives all the K_j), so that the index of the stabilizer (called the normalizer of K_i) is 7, i.e. $N_G(K_i) = K_i$. That such a non-Abelian group of order 21 exists, will have to be shown, and it will be constructed as a semi-direct product.

[5] If $H \leq G$, and $g \in G$, then $g\,H$ is not a subgroup of G unless $g \in H$, but $H^g = g\,H\,g^{-1}$ is always a subgroup of G, hence the action of Example 9.6 leads to Example 9.7 for the set X of subgroups of G.

[6] If G is Abelian, then $N_G(H) = G$ for all $H \leq G$.