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

8- Friday September 16, 2011.

Remark 8.1: For any set X, one denotes S_X the set of bijections of X into X, which is a group under the operation of composition of mappings (which is easily seen to be associative), with identity element $e = id_X$, the identity mapping id_X, defined by 'for all $x \in X$, $id_X(x) = x$' (which even makes sense if $X = \emptyset$), and the inverse of f is the inverse mapping f^{-1} defined by $f^{-1}\big(f(x)\big) = x$ for all $x \in X$.[1]

If $X = \{1, \ldots, n\}$, a bijection from X into X is called a *permutation* of the elements $1, \ldots, n$, and there are $n!$ of them, since there are n choices for the image of 1, then only $n-1$ choices for the image of 2 (because the image of 1 should only appear once), $n-2$ choices for the image of 3, and so on; instead of S_X, one writes S_n, and it is called the *symmetric group* S_n on n elements. Since $n!$ grows very fast, and $10! = 3$ 628 800, a result like Cayley's theorem that any subgroup of order n is isomorphic to a subgroup of S_n may not be of much practical use for large n: saying that all groups of size 10 appear (isomorphically) as some subgroups of a group of order 3 628 800 is not so relevant if one notices that any Abelian group of order 10 is isomorphic to $\mathbb{Z}_{10}$,[2] and any non-Abelian group of order 10 is isomorphic to the dihedral group D_5;[3] since D_5 is the symmetry group of a regular pentagon, it appears as a subgroup of S_n for $n \geq 5$, while S_n contains an isomorphic copy of $\mathbb{Z}_{10}$ for $n \geq 7$ (using as generator a permutation with a cycle of length 5 and a cycle of length 2).[4]

S_n is non-Abelian for $n \geq 3$, while S_2 is isomorphic to $\mathbb{Z}_2$ (and $S_1 = \{e\}$).

Remark 8.2: One may write a permutation $\sigma \in S_n$ as $\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$, by putting the elements in a first row and their images by σ in the second row, but it more useful to write σ as a product of disjoint *cycles*: one builds an oriented graph with vertices $1, \ldots, n$ by putting an oriented edge between i and $\sigma(i)$ for $i = 1, \ldots, n$, and the connected components of the graph are the cycles, so that they use different subsets of $\{1, \ldots, n\}$; one writes $(a_1 \ldots a_k)$ with distinct elements $a_1, \ldots, a_k$ for a cycle of length k (or period k), which means that a_1 is sent to a_2, a_2 is sent to a_3, and so on, until a_n is sent to a_1; for simplicity, one does not write the cycles (a) of length 1, and then every permutation is written as a product of cycles, using different elements of $\{1, \ldots, n\}$.

Since any cycle $(a_1 \ldots a_k)$ has order k, one deduces that the order of a permutation is the least common multiple of the lengths of its cycles. The maximum order of elements of S_n is then 3 for S_3, 4 for S_4, 6 for S_5 and S_6, 12 for S_7, 15 for S_8, 20 for S_9, 30 for S_{10}.

Lemma 8.3: Any permutation $\sigma \in S_n$ (for $n \geq 2$) can be written as a product of *transpositions*, which are the particular permutations having only one cycle of length 2, i.e. $(i\,j)$ for $i \neq j$.
Proof: By induction on n: it is true for $n = 2$ since $S_2 = \{e, \tau\}$ for $\tau = (1\,2)$ and $e = \tau^2$. If it is proved for n and $\sigma \in S_{n+1}$, one writes σ has a product of disjoint cycles; if σ is not a cyclic permutation $(a_1 \ldots a_{n+1})$, then each cycle is a product of transpositions by the induction hypothesis and σ then is such a product of transpositions. If $\sigma = (a_1 \ldots a_{n+1})$ is a cyclic permutation, then $(a_1 a_2)\,(a_1 \ldots a_{n+1}) = (a_2 \ldots a_{n+1})$, which is a product of transpositions $\tau_1 \cdots \tau_k$ by the induction hypothesis, so that $\sigma = (a_1 a_2)\,\tau_1 \cdots \tau_k$.

[1] Since one also uses f^{-1} for pre-images of subsets, let us use the notation $f^<$ instead, defined by $f^<(A) = \{x \in X \mid f(x) \in A\}$ for all $A \in \mathcal{P}(X)$ (i.e. for all $A \subset X$), and notice that for a bijection f one has $f^<\big(\{f(x)\}\big) = \{x\}$ for all $x \in X$. If instead of $f^<$ one writes f^{-1}, then for a bijection f one has two notations f^{-1}, one applying to elements and the other applying to subsets, and a subset with one element is written $\{x\}$, which belongs to $\mathcal{P}(X)$, and it should not be confused with the element x, which belongs to X.

[2] If n is square-free, every Abelian group of order n is isomorphic to $\mathbb{Z}_n$.

[3] If n is odd, every non-Abelian group of order $2n$ is isomorphic to the dihedral group D_n.

[4] For $n = 8$, the order of S_8 is 40 320, and S_8 then contains isomorphic copies of the three Abelian groups of order 8 ($\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$), and of the two non-Abelian groups of order 8 (D_4 and $\mathbb{Q}_8$), but for $n < 8$, S_n does not contain a copy of $\mathbb{Z}_8$.

Definition 8.4: The *signature* of a permutation $\sigma \in S_n$ is $\prod_i (-1)^{\ell_i - 1}$ where the ℓ_i are the lengths of the disjoint cycles (of length ≥ 2) forming σ.[5] It is an homomorphism from S_n into the multiplicative group $\{+1, -1\}$, whose kernel is called the *alternating group* A_n, which is the subgroup of *even permutations* in S_n, i.e. those which are the product of an even number of transpositions, so that $A_n \lhd S_n$, and $S_n/A_n \simeq \mathbb{Z}_2$ for all $n \geq 2$. For $n \geq 2$, $|A_n| = \frac{n!}{2}$, so that $A_2 \simeq \{e\}$, $A_3 \simeq \mathbb{Z}_3$.

Remark 8.5: For the definition to make sense, one has to check that multiplying σ by any transposition multiplies the signature by -1, so that if $\tau_1, \ldots, \tau_m$ are transpositions one has $signature(\tau_1 \cdots \tau_m) = (-1)^m$, and since every permutation is a product of transpositions one deduces that $signature(\sigma_1\sigma_2) = signature(\sigma_1)\, signature(\sigma_2)$ for any two permutations $\sigma_1, \sigma_2 \in S_n$.

One then wants to show that for $i \neq j$ one has $signature\big((i\,j)\,\sigma\big) = -signature(\sigma)$, and there are two cases to consider. In the first case, i and j belong to two different cycles of σ, so that σ contains a product $(i\,a_1 \ldots a_k)\,(j\,b_1 \ldots b_\ell)$ and one notices that $(i\,j)\,(i\,a_1 \ldots a_k)\,(j\,b_1 \ldots b_\ell) = (j\,b_1 \ldots b_\ell i\,a_1 \ldots a_k)$, and this form is valid even if there are no as or no bs, so that σ has one cycle of length $k+1$ and one cycle of length $\ell+1$, contributing to $(-1)^{k+\ell}$ in the definition of $signature(\sigma)$, while $(i\,j)\,\sigma$ has one cycle of length $k+\ell+2$ contributing to $(-1)^{k+\ell+1}$ in the definition of $signature\big((i\,j)\,\sigma\big)$. In the second case, i and j belong to the same cycle of σ, so that σ contains $(i\,a_1 \ldots a_k j\,b_1 \ldots b_\ell)$ and $(i\,j)\,(i\,a_1 \ldots a_k j\,b_1 \ldots b_\ell) = (i\,a_1 \ldots a_k)\,(j\,b_1 \ldots b_\ell)$, and this form is valid even if there are no as or no bs, so that σ has one cycle of length $k+\ell+2$ contributing to $(-1)^{k+\ell+1}$ in the definition of $signature(\sigma)$, and $(i\,j)\,\sigma$ has one cycle of length $k+1$ and one cycle of length $\ell+1$, contributing to $(-1)^{k+\ell}$ in the definition of $signature\big((i\,j)\,\sigma\big)$.

Remark 8.6: A_3 is simple, since it is isomorphic to $\mathbb{Z}_3$ (and $\mathbb{Z}_n$ is simple if and only if n is prime), and it will be shown in another lecture that A_n is simple for all $n \geq 5$, but Lemma 8.7 shows that A_4 is not simple.

Lemma 8.7: One has $N = \{e, (1 2)\,(3 4), (1 3)\,(2 4), (1 4)\,(2 3)\} \lhd S_4$, so that $N \lhd A_4$. One has $A_4/N \simeq \mathbb{Z}_3$, and $S_4/N \simeq S_3$ (and $S_4/A_4 \simeq \mathbb{Z}_2$).
Proof: Since an element like $(1 2)\,(3 4)$ is the product of the two transpositions $(1 2)$ and $(3 4)$, one has $N \subset A_4$, and N is a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, since $(1 2)\,(3 4)\,(1 3)\,(2 4) = (1 4)\,(2 3)$ and $\big((1 2)\,(3 4)\big)^2 = e$, for example. If $\sigma \in S_4$ and one considers $\sigma\,(1 2)\,(3 4)\,\sigma^{-1}$, for example, this permutation transposes $\sigma(1)$ and $\sigma(2)$ and it transposes $\sigma(3)$ and $\sigma(4)$, so that it belongs to N, showing that N is a normal subgroup of S_4, hence a normal subgroup of A_4. Because $|A_4| = 12$, A_4/N has order 3, and is isomorphic to $\mathbb{Z}_3$. S_4/N has order 6, and could be isomorphic to $\mathbb{Z}_6$ or to S_3, but if it was isomorphic to Z_6 there would exist $a \in S_4$ with $a, \ldots, a^6$ belonging to six different N-cosets, but in S_4 the only possible orders for an element are 1, 2, 3, or 4, so that S_4/N must be isomorphic to S_3.

Remark 8.8: Lemma 8.7 actually shows that S_4 is a *solvable* group, but it can be shown that S_n is not a solvable group for $n \geq 5$. This is related to the method of GALOIS for characterizing the polynomials P over a field E whose roots can be given by a formula using only radicals: one defines the *splitting field extension* F for P over E, and the *Galois group* $G = Aut_E(F)$ of automorphisms of F fixing E, and the condition is that G be solvable, and this means that there exists a *subnormal series* $G_0 = \{e\} \leq G_1 \leq \ldots \leq G_k = G$ (i.e. such that $G_i \lhd G_{i+1}$ for $i = 0, 1, \ldots, k-1$) for which G_{i+1}/G_i is Abelian for $i = 0, \ldots, k-1$. The case of S_4 corresponds to $\{e\} \lhd N \lhd A_4 \lhd S_4$.

Lemma 8.9: (Cauchy's theorem) Let p be a prime number, and let G be a finite group whose order is a multiple of p. Then, there exists an element $h \in G$ of order p, or equivalently there exists a subgroup $H \leq G$ of order p (so that there exist at least $p-1$ elements of order p). More precisely, the number of subgroups or order p is equal to 1 modulo p.
Proof: Let $\Gamma = G \times \cdots \times G$ (with p factors). One defines the mapping π from Γ into itself by $\pi\big((g_1, \ldots, g_p)\big) = (g_2, \ldots, g_p, g_1)$, and one writes $\pi\, x$ for $\pi(x)$; one notices that $\pi^p \gamma = \gamma$ for all $\gamma \in \Gamma$.

Let $X \subset \Gamma$ be the subset of $x = (g_1, \ldots, g_p)$ satisfying $g_1 \cdots g_p = e$, so that $|X| = |G|^{p-1}$ is a multiple of p, since $g_1, \ldots, g_{p-1}$ may be chosen arbitrarily, and then g_p is determined. For $x \in X$, one has $g_2 \cdots g_p g_1 = g_1^{-1}(g_1 \cdots g_p)\, g_1 = g_1^{-1} e\, g_1 = e$, so that π maps X into itself. If $\pi\, x \neq x$, then $x, \pi\, x, \ldots, \pi^{p-1} x$ are all distinct elements of X, and this is where the fact that p is a prime is used, because if $\pi^j x = \pi^k x$ for $0 \leq j < k \leq p-1$, then $\pi^\ell x = x$ for $\ell = k - j$, so that $\pi^{m\,\ell} x = x$ for all $m \geq 1$, and using for m the inverse of ℓ modulo p

[5] Another definition of $signature(\sigma)$ is $(-1)^m$, where m is the number of pairs $i < j$ such that $\sigma(i) > \sigma(j)$.

(so that $m\,\ell = 1 + n\,p$) one deduces that $\pi\,x = x$. A consequence is that X is made up of such subsets of p elements, together with the particular $x \in X$ satisfying $\pi\,x = x$, and the number of those must then be a multiple of p (and $\neq 0$ since $(e, \ldots, e)$ belongs to it).

Since $\pi\,x = x$ implies $g_1 = g_2 = \cdots = g_p$, one has $x = (h, \ldots, h)$ with $h \in G$ satisfying $h^p = e$, and the number of such h is a (non-zero) multiple of p, so that there are at least $p-1$ solutions of $h^p = e$ with $h \neq e$, which all have order p; a subgroup of order p is $H = \{e, h, \ldots, h^{p-1}\}$ for such a $h \neq e$.

Let the number of h be $k\,p$, and correspond to j distinct subgroups of order p; since two such subgroups are equal or intersect only at e (by Lagrange's theorem, because p is prime), one has $k\,p = j\,(p-1) + 1$, so that $j = 1 + p\,(j - k)$.

Remark 8.10: The preceding proof uses an action of the group $\mathbb{Z}_p$, and remarks about the size of orbits. The general question of action of a group on a set will be studied in the next lecture.