REU APPRENTICE CLASS #6

INSTRUCTOR: LÁSZLÓ BABAI
SCRIBE: DANIEL SCHÄPPI

Tuesday, July 5, 2011

1. Groups. The Symmetric Group

Recall that a permutation of a set A is a bijection $\pi\colon A \to A$. For $A = \{1, 2, \dots, n\}$ we can denote permutations using the *cylcle notation*, e.g., we write

$$\pi = (156)(27)(34)$$

for the permutation of $[8] = \{1, 2, \dots, 8\}$ given by

x	1	2	3	4	5	6	7	8
$\pi(x)$	5	7	4	3	6	1	2	8

Note that we omit the cycle (8) of length 1. We say that π has *cycle structure* $(3, 2, 2)$. A cycle of length 2 is called a *transposition.*

Composition of functions defines an operation on the set S_n of permutations of $[n] = \{1, 2, \dots, n\}$. The resulting structure is called a group.

Definition 1.1. A *group* is a set G together with an operation $G \times G \to G$, $(a, b) \mapsto a * b$ satisfying the axioms:

(1) For all $a, b \in G$, there exists a unique $a * b$ in G (that is, the operation is a function with the correct domain and codomain).
(2) The operation is associative.
(3) (Identity) There exists an element $e \in G$ such that for all $a \in G$, $e * a = a = a * e$.
(4) (Inverses) For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

If, in addition, we have $a * b = b * a$ for all $a, b \in G$, then G is called an *abelian* group.

Convention 1.2. We compose permutations in the same order as functions, i.e., $(12)(23) = (123)$ and $(23)(12) = (132)$.

S_n is a group with $*$ given by composition of functions, called the *symmetric group of degree n*, and we just noticed that S_n is not abelian for $n \geq 3$. Examples of abelian groups are $(\mathbb{Z}, +)$, the nonzero elements $F^\times = F \setminus \{0\}$ of a number field F under multiplication, or the n-th roots of unity in $\mathbb{C}$ under multiplication.

While it is not true that *all* pairs of elements of the symmetric group commute, there are obviously some pairs of elements that do, for example, disjoint cycles.

Definition 1.3. The *support* of a permutation σ of $[n]$ is the set

$$\mathrm{supp}(\sigma) = \{x \in [n] | \pi(x) \neq x\},$$

that is, the support is the set of elements that are not fixed by σ.

Exercise 1.4. If $\mathrm{supp}(\pi) \cap \mathrm{supp}(\sigma) = \varnothing$, then $\pi\sigma = \sigma\pi$.

Problem 42. Find permutations π, σ such that $\mathrm{supp}(\pi) \cap \mathrm{supp}(\sigma) \neq \varnothing$ and $\pi\sigma = \sigma\pi$.

The *commutator* of π and σ is $[\pi, \sigma] = \pi\sigma\pi^{-1}\sigma^{-1}$.

Problem 43. If $|\mathrm{supp}(\pi) \cap \mathrm{supp}(\sigma)| = 1$, then the commutator $[\pi, \sigma]$ of π and σ is a 3-cycle.

Definition 1.5. A *subgroup* H of a group G is a subset $H \subseteq G$ such that

(1) $H \neq \varnothing$.

(2) H is closed under the multiplication.
(3) H is closed under inverses.

We use the shorthand $H \leq G$ for the statement "H is a subgroup of G."

Note that it follows immediately from the definition of a subgroup that the identity e lies in it, and that H is itself a group under the restricted multiplication.

Problem 44. A (possibly infinite) intersection of subgroups is a subgroup.

Corollary 1.6. *If $T \subseteq G$ is a subset, then there exists a unique* minimal *subgroup containing T, denoted by $\langle T \rangle$ and called the subgroup generated by T. Moreover, this subgroup is in fact the* smallest *subgroup containing T.*

Here H being minimal among subgroups containg T means that for all subgroups K, if $K \supseteq T$, then $K \subseteq H \Rightarrow K = H$, and H being the smallest subgroup containing T means that $K \supseteq T$ implies $K \supseteq H$.

Observation 1.7. The subgroup $\langle T \rangle$ consists of all finite products of elements of T and their inverses. Note that $\langle \varnothing \rangle = \{e\}$. This agrees with our convention that the product of nothing is the identity element.

Theorem 1.8. *The transpositions generate S_n. (The number of transpositions is $\binom{n}{2}$.)*

Proof. Write a generic k-cycle as a product of $k-1$ transpositions. □

Theorem 1.9. *The $n-1$ neighbour swaps $(i, i+1)$ generate S_n.*

Proof. Write the transposition $(i, i+k)$ as a product of $2k-1$ neighbour swaps. □

Can we generate S_n using $n-1$ transpositions in a different way? Fix a set T of transpositions. In order to study this question it is useful to consider the graph whose vertices are $\{1, 2, \ldots, n\}$, with an edge between i and j if and only if $(ij) \in T$.

Definition 1.10. Two graphs $X = (V, E)$ and $Y = (W, F)$ are *isomorphic* if there exists an isomorphism $X \to Y$, i.e., a bijection $\varphi \colon V \to W$ such that $(u, v) \in E \Leftrightarrow \big(\varphi(u), \varphi(v)\big) \in F$.

Problem 45. (a) Show that there are many non-isomorphic arrangements of $n-1$ transpositions that generate S_n. (That is, the graphs of the respective generating sets are not isomorphic.)
(b) Show that S_n cannot be generated by fewer than $n-1$ transpositions.

Problem 46. The identity cannot be written as a product of an odd number of transpositions.

Problem 47. Let $\sigma = (1, 2, \ldots, n)$ and let $\tau = (12)$. Then:
(a) $S_n = \langle \sigma, \tau \rangle$
(b) Every permutation is a product of $O(n^2)$ instances of $\{\sigma, \sigma^{-1}, \tau\}$.
(c) For some permutations we need $\Omega(n^2)$.

Recall that $O(n^2)$ means *at most* $C \cdot n^2$, $\Omega(n^2)$ means *at least* $C' \cdot n^2$ for some constants $C, C' > 0$.

2. Fields

Notation 2.1. For an abelian group G we usually write $a + b$ for $a * b$, 0 for the identity element, and $-a$ for the inverse of $a \in G$ (additive notation). For a nonabelian group we instead write $a \cdot b$ or ab for $a * b$, 1 for the identity element, and a^{-1} for the inverse of $a \in G$ (multiplicative notation). The multiplicative notation is also frequently used for abelian groups if we consider two group structures on the same set.

Definition 2.2. The *order* of a group is the number of elements, denoted by $|G|$. (Note that $|G| \geq 1$.)

Fix $n \geq 1$. The subgroup $\{z \in \mathbb{C} \mid z^n = 1\}$ of $(\mathbb{C}^\times, \cdot)$ is a group of order n.

Definition 2.3. A *field* $(F, +, \cdot)$ is a set two operations $+, \cdot \colon F \times F \to F$ such that
(1) $(F, +)$ is an abelian group whose identity element we denote by 0.
(2) $(F^\times, \cdot)$ is an abelian group, where $F^\times = F \setminus \{0\}$.

(3) The distibutive law holds, i.e., for all $a, b, c \in F$, the equation

$$(a + b)c = ac + bc$$

holds.

Exercise 2.4. Let $(F, +, \cdot)$ be a field. For all $a \in F$, $a0 = 0a = 0$. Thus $ab = ba$ for all $a, b \in F$.

Exercise 2.5. Let $(F, +, \cdot)$ be a field. For all $a, b \in F$, if $ab = 0$, then $a = 0$ or $b = 0$.

Note that the order $|F|$ of a field is at least two: every field contains the two elements $0 \neq 1$. In order to write down simple examples we can use multiplication tables for the respective group operations.

Problem 48. In the multiplication table of a group, every element appears exactly once in each row and each column.

The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ of integers modulo n has two operations given by addition modulo n and multiplication modulo n. Thus it is almost a field: $(\mathbb{Z}_n, +)$ is obviously an abelian group, and the distributive law already holds prior to reduction modulo p. Moreover, multiplication is clearly associative and has an identity element 1. Thus it is a field if and only if every non-zero element has an inverse modulo n.

Problem 49. Prove that $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Notation 2.6. Let p be a prime number. We write $\mathbb{F}_p$ for the field $(\mathbb{Z}_p, +, \cdot)$ of integers modulo p.

The set $\mathbb{F}_4 = \{0, 1, a, a^{-1}\}$ can be endowed with the structure of a field. The multiplication table for $(\mathbb{F}_4, +)$ is given by

$+$	0	1	a	a^{-1}
0	0	1	a	a^{-1}
1	1	0	a^{-1}	a
a	a	a^{-1}	0	1
a^{-1}	a^{-1}	a	1	0

and the multiplication table for $(\mathbb{F}_4^\times, \cdot)$ is given by

$\cdot$	1	a	a^{-1}
1	1	a	a^{-1}
a	a	a^{-1}	1
a^{-1}	a^{-1}	1	a

Note that $\mathbb{F}_4 \neq \mathbb{Z}_4$; indeed, $\mathbb{F}_4$ is a field, while $\mathbb{Z}_4$ is not.

Problem 50. If $\mathbb{F}$ is a finite field, then $|\mathbb{F}|$ is a prime power. (Note: the converse is also true: for every prime power q there is a field of order q, and this field is unique up to isomorphism.)

Problem 51. Let $\mathbb{C}_p = \{a + bi \mid a, b \in \mathbb{Z}_p\}$ be the "mod p complex numbers." For what values of p is $\mathbb{C}_p$ a field? (Experiment, conjecture, prove. Hint: use Problem 52.)

Definition 2.7. A *ring* $(R, +, \cdot)$ is a set with two operations $+, \cdot \colon R \times R \to R$ such that

(1) $(R, +)$ is an abelian group.
(2) $(R, \cdot)$ is associative.
(3) The two distributive laws hold.

A *commutative ring* is a ring such that $ab = ba$ for all $a, b \in R$.

Examples of commutative rings are $\mathbb{Z}$ and $\mathbb{Z}_n$.

Exercise 2.8. Let $(R, +, \cdot)$ be a ring. For all $a \in R$, $a0 = 0a = 0$.

Problem 52. A *finite* commutative ring R is a field if and only if $|R| \geq 2$ and for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

This concludes our discussion of finite fields. Note that every number field is a field, in fact, number fields are precisely the subfields of $\mathbb{C}$.

Problem 53. Give an example of an infinite field that is not isomorphic to a number field.

3. Asymptotics

Definition 3.1. Let G be a group, $a \in G$. The *order* $\mathrm{ord}(a)$ of a is the smallest integer $n > 0$ such that $a^n = 1$. If no such n exists we say that $\mathrm{ord}(a) = \infty$.

For example, the order of $\mathrm{ord}(123) = 3$, $\mathrm{ord}(1, 2, \ldots, n) = n$ and $\mathrm{ord}\big((123)(45)\big) = 6$. More generally, if σ has cycle structure $(n_1, n_2, \ldots, n_k)$, then $\mathrm{ord}(\sigma) = \mathrm{lcm}(n_1, n_2, \ldots, n_k)$. In order to get elements with big order, we could set n_i to be $2, 3, 5, 7, 11, \ldots$ What is the maximum order of a permutation of n elements? We study the asymptotic behavior of this function.

Definition 3.2. Two sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are *asymptotically equal*, $a_n \sim b_n$, if $\lim_{n\to\infty} a_n/b_n = 1$.

Theorem 3.3 (Prime number theorem)**.** *Let $\pi(x)$ be the number of primes $\leq x$. Then*

$$\pi(x) \sim \frac{x}{\ln(x)}$$

so the probability that a random number up to x is prime is asymptotically equal to $1/\ln(x)$.

For example, the probability that a random number with 200 digits is prime is roughly

$$\frac{1}{\ln(10^{200})} = \frac{1}{200\ln(10)} \approx \frac{1}{460}.$$

Problem 54. Prove that $\ln(x!) \sim x\ln(x)$.

Problem 55. Let

$$P(x) = \prod_{p\leq x \text{ prime}} p$$

be the product of all primes of size at most x. Prove that the statement

$$\ln\big(P(x)\big) \sim x$$

is equivalent to the Prime Number Theorem.

Problem 56. Find the log-asymptotics of the largest order of a permutation in S_n.