M7210 Lecture 15 Wednesday September 26, 2012

Groups

Definition. A *group* G is a set equipped with the following data:

a) a designated element e (called the *identity element*),

b) a function $g \mapsto g^{-1} : G \to G$ (called *inversion*),

c) a function $(g, h) \mapsto gh : G \times G \to G$ (called the *operation*),

with the requirement that the following axioms are satisfied:

1) The identity law: for all $g \in G$, $eg = g = ge$.
2) The law of inverses: for all $g \in G$, $gg^{-1} = e = g^{-1}g$.
3) The associative law: for all $f, g, h \in G$, $(fg)h = f(gh)$.

When speaking of a group G, if we want to refer to the underlying set only, without regard to the additional structural data (given by the identity, inversion and the operation), some people write $|G|$, some people write $F(G)$ (where "F" stands for "forget"), and some people withe G and just state their intent. The choice is optional. In practice, there is seldom confusion, but this is a difference that sometimes makes a big difference. So one must be alert to it.

Fact. *If $fg = e$ or $gf = e$, then $f = g^{-1}$.*

Proof.

$$fg = e \;\Rightarrow\; fgg^{-1} = eg^{-1} \;\Rightarrow\; fe = g^{-1} \;\Rightarrow\; f = g^{-1}.$$

Examples

1. The integers $\mathbb{Z}$ with identity 0, inversion $x \mapsto -x$ and operation $(x, y) \mapsto x + y$ is a group.
2. If $\mathbb{F}$ is a field, then the non-zero elements of $\mathbb{F}$ with identity 1_F, inversion $x \mapsto 1/x$ and operation $(x, y) \mapsto x\,y$ is a group.
3. The integers mod n consists of the set $\{0, 1, \ldots, n-1\}$. The identity is 0. The inversion map is $k \mapsto n - k$ if $k > 0$ and $0 \mapsto 0$, and the operation is:

   $$(k, \ell) \mapsto \begin{cases} k + \ell, & \text{if } k + \ell < n; \\ k + \ell - n, & \text{if } k + \ell \geq n. \end{cases}$$

   Later, we will identify this group with the "group of equivalence classes of $\mathbb{Z}$ mod n." The equivalence relation is

   $$x \equiv y \;\Leftrightarrow n|(y - x).$$

   A common notation for this group is $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$. The elements may be denoted $k + n\mathbb{Z}$ or $k + (n)$ or $[k]_n$ or $\overline{k}$, for $k \in \mathbb{Z}$.
4. If X is any set, the collection of bijections $f : X \to X$ is a group. The identity is the function $e = \mathrm{id}_X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$. Inversion is "functional inversion." In other words, $f^{-1} : X \to X$ is the function defined by

   $$\text{for all } w, z \in X,\ f^{-1}(z) = w \text{ if and only if } f(w) = z.$$

The operation is function composition:

$$\text{for all } x \in X,\ fg(x) = f(g(x)).$$

If X is a finite set with n elements, we call this group the group of permutations of n elements, or the *symmetric group* on n elements. It is denoted S_n (Knapp uses a gothic "S").

5. Let T be the set of complex numbers of modulus 1, i.e., the unit circle in the complex plane. Then T is a group under multiplication. Note that $\omega^{-1} = \overline{\omega}$ (complex conjugate).

Definition. Let G be a group. A *subgroup* of G is a subset of $|G|$ that contains the identitiy, that contains g^{-1} whenever it contains g and that contains fg whenever it contains f and g.

Facts that you should be able to prove in your sleep:

1. Any subgroup of a group is a group.
2. If H and K are subgroups of a group G, then $H \cap K$ is a subgroup of G. If $\{\, H_\alpha \mid \alpha \in A \,\}$ is any set of subgroups of G, then $\bigcap\{\, H_\alpha \mid \alpha \in A \,\}$ is a subgroup of G.
4. A union of subgroups need not be a subgroup. (Provide examples).
5. Given any subset $X \subseteq |G|$, there is a subgroup containing X that is smallest in the sense that it is contained in *every* subgroup of G that contains X. (Hint. Consider the intersection of all subgroups of G—including G itself, of course—that contain X.) (The smallest subgroup of G containing X is called the *subgroup of G generated by X.*)

Example. The dihedral groups. It $a \in T$, let $\rho_a : T \to T$ be defined by $\rho_a(z) = az$, and let $\sigma_a : T \to T$ be defined by $\sigma_a(z) = a\overline{z}$. Let D_∞ be the following set of bijections from T to T:

$$\{\, \rho_a z \mid a \in T\} \cup \{\, \sigma_a \mid a \in T\}.$$

Thus D_∞ consists of the rotations and the functions that can be obtained by a flip over the real axis followed by a rotation. We note that

$$a(bz) = (ab)z, \qquad a(b\overline{z}) = (ab)\overline{z}, \qquad a\overline{(bz)} = (a\overline{b})\overline{z} \qquad a\overline{(b\overline{z})} = (a\overline{b})z,$$

so

$$\rho_a\rho_b = \rho_{ab}, \qquad \rho_a\sigma_b = \sigma_{ab}, \qquad \sigma_a\rho_b = \sigma_{a\overline{b}} \qquad \sigma_a\sigma_b = \rho_{a\overline{b}}.$$

This shows that D_∞ is closed under composition. It clearly contains the identity ρ_1. As for, inverses: $\rho_b\rho_{\overline{b}} = \rho_1$, so

$$\rho_b^{-1} = \rho_{\overline{b}}.$$

Thus, D_∞ is a subgroup of the group of all bijections of T with itself. Also, note that $\sigma_a = \rho_a\sigma_1$. Thus if we write σ in place of σ_1, we see $D_\infty = \{\, \rho_a\sigma^j \mid a \in T,\ j \in \{0,1\} \,\}$. Finally, note that

$$\sigma\rho_b = \sigma_{\overline{b}} = \rho_b^{-1}\,\sigma.$$

This provides neat set of rules for simplifying any expressions involving the elements of D_∞. For example, fix some $a \in T$ and let $\rho := \rho_a$. Then:

$$\rho^i \sigma \rho^j \sigma \rho^k \sigma = \rho^i \rho^{-j} \sigma \sigma \rho^k \sigma = \rho^i \rho^{-j} \rho^k \sigma = \rho^{i-j+k} \sigma.$$

Finite dihedral groups. We call ω a *primitive n^{th} root of unity* if $\omega \in T$, $\omega^n = 1$ and $\omega^k \neq 1$ for $k = 1, 2, \ldots, n-1$. For example, i is a primitive 4^{th} root of unity, and in general $\cos(2\pi/n) + i\sin(2\pi/n)$ is a primitive n^{th} root of unity. Notice that if ω is a primitive n^{th} root of unity, then $\langle \omega \rangle = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$, with multiplication as a group operation, is essentially the same group as the group of integers mod n. Suppose ω is a primitive n^{th} root of unity. Let $\rho = \rho_\omega$. Then the *dihedral group with $2n$ elements* is the following subgroup of D_∞:

$$D_{2n} := \{\, \rho^i \sigma^j \mid i \in \{0, 1, \ldots, n-1\},\, j \in \{0, 1\} \,\}.$$

In D_{2n}, we multiply symbolically using the rules $\rho^i \rho^j = \rho^{i+j}$ and $\sigma \rho^k = \rho^{-k} \sigma$, as indicated above.

Definition. Let G and H be groups. A bijection $I : G \to H$ such that $I(fg) = I(f)I(g)$ for all $f, g \in G$ is called an *isomorphism.*

Example. Let ω be a primitive n^{th} root of unity. The map $[k]_n \mapsto \omega^n : \mathbb{Z}/(n) \to \langle \omega \rangle$ is a group isomorphism. This makes precise the observation made above when $\langle \omega \rangle$ was introduced.

Fact. *If I is an isomorphism, $I(g^{-1}) = (I(g))^{-1}$, and $I(e_G) = e_H$. The functional inverse of an isomorphism is an isomorphism.*

Theorem. *(Cayley). Suppose G is a group. Then G is isomorphic to a subgroup of the group of bijections of (the set) G.*

Proof. Let $\mathrm{Bij}(G, G)$ denote the group of bijections from G (viewed as a set) to G (viewed as a set). We are going to define a function from G to $\mathrm{Bij}(G, G)$. For each $g \in G$, define $\beta_g : |G| \to |G|$ by $\beta_g(h) = gh$. Each β_g is a bijection (WHY?), so $\beta_g \in \mathrm{Bij}(G, G)$, as desired. Now, the function $g \mapsto \beta_g : G \to \mathrm{Bij}(G, G)$ is injective, because if $g \neq h$, then $\beta_g(e) = g \neq h = \beta_h(e)$, so $\beta_g \neq \beta_h$. Let $\mathrm{Im}\beta := \{\, \alpha \in \mathrm{Bij}(G, G) \mid \alpha = \beta_g \text{ for some } g \in G \,\}$. Observe that $\beta_{gh} = \beta_g \circ \beta_h$, and consequently, $\mathrm{Im}\beta$ is closed under the group operation, contains e and contains inverses (this requires some light work to check explicitly), and thus is a group. Moreover $g \mapsto \beta_g : G \to \mathrm{Im}\beta$ is bijective and preserves the group operation, so it is an isomorphism. /////

Homework.

- Page 198: 1–8.
- Let $p \in \mathbb{N}$ be an odd prime. As you probably are aware, in $\mathbb{Z}/p\mathbb{Z}$ one may multiply as well as add—indeed, $\mathbb{Z}/p\mathbb{Z}$ is a field. Find a group of 3×3 matrices with entries in $\mathbb{Z}/p\mathbb{Z}$ such that every element has order p, but the group is not abelian. (Hint: Put 1s on the diagonal.)