

Geometry and Symmetry, Problem Set 9
Summer 2009

Exploration – Dictionary Groups

P1. We can write down every possible English word by listing the letters a, \dots, z of the alphabet and specifying word formation rules as follows: all letters are possible words, and given any two words w_1, w_2 , we can form a new word by the *concatenation product* $w_1 \star w_2$ which just puts w_1 next to w_2 . For example, $a \star b = ab, ab \star ab = abab, dog \star cat = dogcat$, etc. This product is clearly associative. We abbreviate words like $aaaaabbccdd$ by $a^5b^2cd^2$.

To make our dictionary into a group, we need an identity element, which can only be the “empty word”, denoted $_$, with the rule e.g. $dog \star _ = _ \star dog = dog$. We also need to add new letters $a^{-1}, b^{-1}, \dots, z^{-1}$ with the rules $a \star a^{-1} = a^{-1} \star a = \dots = z \star z^{-1} = z^{-1} \star z = _$. Now we have a group – for example, the inverse of cat is $t^{-1}a^{-1}c^{-1}$.

Let’s agree on a list of all possible swear words. We can impose the rule that if e.g. $abcde$ is a swear word, then we do not allow this word to be formed. In particular, we will expunge this word by declaring a new rule $abcde = a \star bcde = ab \star cde = abc \star de = abcd \star e = _$. Of course, if we eliminate $abcde$, we have to expunge its inverse as well. (Why?) Note that $hjkab \star cdem^3 = hjk \star abcde \star m^3 = hjkm^3$, so we delete swear words occurring in the middle of products. What group do we get if our alphabet consists only of the letter a (and it is understood that we also automatically have a^{-1}) and there are no swear words? What group do we get if our alphabet has only a , and a^{173} is a swear word? What group do we get if our alphabet has a, b and $aba^{-1}b^{-1}$ is a swear word? What group do we get if our alphabet has a, b and swear words a^2, b^3 ?

I claim that if you have a finite group $G = \{g_1, g_2, \dots, g_n\}$ and if you form a dictionary with the letters g_1, \dots, g_n and make every multiplication table entry a swear word, in the sense that $g_i g_j g_k^{-1}$ is a swear word if $g_i \cdot_G g_j = g_k$, then the group you get is isomorphic to G . Can you prove this? (Watch out for the “two” inverses for e.g. g_1 , namely its inverse g_j for some j and the new letter g^{-1} .)

Rotations in \mathbb{R}^3 and the Quaternions

Let S^3 be the unit quaternions. Recall that we have a two-to-one homomorphism $\rho : S^3 \rightarrow \text{SO}(3)$ given by $\rho(q) = C_q, C_q(v) = qvq^{-1}$. (Here we think of $v \in \mathbb{R}^3$ as an imaginary quaternion.)

P2. Show that the axis of $\rho(q)$ is given by the imaginary part of q (thought of as a point in \mathbb{R}^3). *Hint:* Write $q = a + \text{Im}(q)$, with $a \in \mathbb{R}$ and $\text{Im}(q)$ imaginary (quaternionic). Show that $qqq^{-1} = q$ implies $q(\text{Im}(q))q^{-1} = \text{Im}(q)$. Conclude that $\rho(q)$ fixes $\text{Im}(q)$, so $\text{Im}(q)$ must be the axis.

P3. In the notation of P2, write $a = \cos(\theta/2)$ for some angle $\theta \in [0, 2\pi)$. Show that $\rho(q)$ is rotation by angle θ . (The angle depends on your choice of a unit vector on the axis.) *Hint:* We know the axis of $\rho(q)$ by P2, and we know that $\rho(q)$ is a rotation in a plane $\text{Im}(q)^\perp$ perpendicular to the axis. Take your favorite vector in $\text{Im}(q)^\perp$; if $\text{Im}(q) = bi + cj + dk$, my favorite is $\vec{v} = (-c, b, 0)$. Compute $\rho(q)\vec{v} = \vec{w}$ — it’s not that bad. Then the angle of rotation of $\rho(q)$ is given by $\vec{v} \cdot \vec{w} = |\vec{v}| |\vec{w}| \cos(\theta)$.

P4. Take $A, B \in \text{SO}(3)$, and say $\rho(q_1) = A, \rho(q_2) = B$. We know how to find q_1, q_2 , and we know that $\rho(q_1 q_2) = AB$. Conclude that the axis of AB is the imaginary part of $q_1 q_2$ and the angle of rotation of AB is determined by the real part of $q_1 q_2$. (This is by far the easiest way I know to find the axis and angle of the composition of rotations.)

- *P5. Let A be rotation by an irrational angle around the z -axis, and let B be rotation by the same angle around the x -axis. Show that the group generated by A and B is isomorphic to F_2 . Here F_2 is the free group on two generators, the dictionary group with two letters a, b (and their inverses) and no swear words except the obvious ones ($aa^{-1} = a^{-1}a = bb^{-1} = b^{-1}b = \underline{\quad}$). You have to show that no word in $A^{\pm 1}, B^{\pm 1}$ is the identity except for the obvious swear words. Try an induction on the number of letters in a word.
- P6. Find the center of S^3 .
- P7. Is $\{\pm 1\}$ a subgroup of S^3 ? Is it a normal subgroup?
- P8. Is $C = \{a + bi \mid |a|^2 + |b|^2 = 1\}$ an abelian subgroup of S^3 ? Is it isomorphic to a group we've seen many times? Is C a normal subgroup of S^3 ?

Quotient Groups

- P9. Show that every group G of order p is cyclic (i.e. there exists $g \in G$ such that $\langle g \rangle = G$). *Hint:* pick $g \neq e$. What does Lagrange's theorem tell you about $\langle g \rangle$?
- P10. Let H be a subgroup of a group G . Show that each left coset $gH = \{gh \mid h \in H\}$ equals the right coset $Hg = \{hg \mid h \in H\}$ iff $H \triangleleft G$ (i.e. H is a normal subgroup of G).
- P11. Let H be a subgroup of an abelian group G . Define a multiplication on (left) cosets by $g_1H \cdot g_2H = (g_1g_2)H$. Then the set of cosets (denoted G/H) is a group. *Hint:* the coset $H = hH$ for any $h \in H$ is the identity.
- P12. Let $17\mathbb{Z} = \{17k \mid k \in \mathbb{Z}\}$. Use P10 to show that $\mathbb{Z}/17\mathbb{Z} \simeq Z_{17}$.
- P13. Show that $\{0, 3\} \subset \mathbb{Z}_6$ is isomorphic to \mathbb{Z}_2 . Show that $\mathbb{Z}_6/\mathbb{Z}_2 \simeq \mathbb{Z}_3$, where \mathbb{Z}_2 stands for $\{0, 3\}$.
- P14. PODSIP. If A and B are abelian groups, then $G = A \times B$ is abelian. The subset $A_1 = A \times \{e_b\}$ is a subgroup of G isomorphic to A , and similarly for $B_1 = \{e_a\} \times B$. We have $G/A_1 \simeq B$ and $G/B_1 \simeq A$. (Of course everyone just denotes A_1, B_1 by A, B , respectively, so e.g. $(A \times B)/A \simeq B$, as it should.)
- P15. PODASIP. If $H \triangleleft G$, then G/H has a group structure given by $g_1H \cdot g_2H = (g_1g_2)H$.
- P16. Let $f : \mathbb{Z} \rightarrow \mathbb{Z}_{17}$ be $f(a) = (a \bmod 17)$. What is the kernel $K = \text{Ker}(f)$ of f ? Show that f induces a well defined map $\bar{f} : \mathbb{Z}/(\text{Ker}(f)) \rightarrow \mathbb{Z}_{17}$ by $\bar{f}(nK) = f(n)$.
- P17. Let A, B be groups, and let $f : A \times B \rightarrow A$ be $f(a, b) = a$. Show that f is a homomorphism. Compute the kernel of f . Find a group isomorphic to $(A \times B)/(\text{Ker}(f))$.
- P18. Prove the *First Isomorphism Theorem* of group theory: if $f : G \rightarrow H$ is a homomorphism of groups, then $G/\text{Ker}(f) \simeq \text{Im}(f)$. *Hint:* show that f induces a well defined homomorphism $\bar{f} : G/\text{Ker}(f) \rightarrow \text{Im}(f)$ by $\bar{f}(gK) = f(g)$. Show that \bar{f} is the isomorphism we want.