CONCRETE GROUPS

COLTON GRAINGER (MATH 6130 ALGEBRA)

1. Assignment due 2018-09-05

1.1. **A Q-vector space with a radical basis [1, No. 1.1.8].** Let $G = \left\{a + b\sqrt{2} \in \mathbf{R} : a, b \in \mathbf{Q}\right\}$.

(a) Consider G under the binary operation addition. We'll show G is a subgroup of $(\mathbf{R}, +, 0)$ (and therefore a group itself).

- To show G is closed under addition. Consider $a + b\sqrt{2}$ and $c + d\sqrt{2}$ in G. Their sum is $(a+c)+(b+d)\sqrt{2}$ by commutativity and associativity[1] of the operation $+$ in $\mathbf{R}$; it's an element of G because $\mathbf{Q}$ is closed under addition and therefore $a + c, b + d \in \mathbf{Q}$.
- To show inverses exist for all elements in G. For all $g \in G$, there are $a, b, -a, -b \in \mathbf{Q}$ such that $g = a+b\sqrt{2}$ and $-g = -a + (-b)\sqrt{2}$. We see $g + (-g) = 0 + 0\sqrt{2}$, the identity.

So G is a subgroup of $(\mathbf{R}, +, 0)$, and therefore a group itself.[2]

(b) Now consider $G \setminus \{0\} = G^*$ with the binary operation multiplication, i.e., $G^* \leq (\mathbf{R}, \cdot, 1)$.

- To show G^* is closed, let $a + b\sqrt{2}$, $c + d\sqrt{2} \in G^*$. Their product is $(ac + 2bd) + (bc + ad)\sqrt{2}$, meeting the form of membership (atleast one of ac, bd, bc, ad is nonzero) required of G^*.
- To show inverses exist. For any $a + b\sqrt{2} \in G^*$, it's inverse is

$$\frac{a - b\sqrt{2}}{a^2 - 2b^2},$$

an element of G^* because $\mathbf{Q}$ is closed under addition, multiplication, and inverses (noting[3] that $a^2 \neq 2b^2$).

1.2. **The dressing-undressing principle [1, No. 1.1.15].** Suppose G is a group. Then $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2 \dots a_n \in G$.

Proof by induction. As a base case, for all $a, b \in G$ we verify that $(ab)^{-1} = b^{-1}a^{-1}$ since $abb^{-1}a^{-1} = 1$. For induction on n, suppose that $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$. Now for any a_{n+1}, because $(a_1 a_2 \dots a_n)a_{n+1}a_{n+1}^{-1}(a_1 a_2 \dots a_n)^{-1} = 1$, we have that

$$(a_1 a_2 \dots a_n a_{n+1})^{-1} = a_{n+1}^{-1} a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1},$$

as desired. □

1.3. **Every element its own inverse [1, No. 1.1.25].** If $x^2 = 1$ for every element x in the group G then G is abelian.

Proof. For any two elements x and y in G, consider their product $a = xy$. Because $a \in G$,

$$1 = a^2 = xyxy.$$

Now $x^2 = y^2 = 1$ implies $x^{-1} = x$ and $y^{-1} = y$, so from $1 = a^2$ we have

$$x1y = xa^2y \iff xy = xxyxxy \iff xy = yx,$$

demonstrating that G is abelian. □

Date: 2018-09-01.
Compiled: 2018-09-05.

[1] In future problems the familiar field properties of $\mathbf{R}$ will go unstated and assumed, unless good exposition calls for the extra detail.

[2] Assuming "subgroups are groups" and "a subset of a group is a subgroup iff it's closed under the group operation and taking inverses".

[3] Suppose that a, b are not both zero and $a^2 = 2b^2$. Then either $(a/b)^2 = 2$ or $(2b/a)^2 = 2$, implying $\sqrt{2} \in \mathbf{Q}$.

1.4. **Direct products of groups [1, No. 1.1.28].** Suppose that $(A, \star)$ and $(B, \diamond)$ are groups. We verify that the direct product $A \times B$ satisfies the group axioms.

(a) The binary operation $\cdot : (A \times B) \times (A \times B) \to (A \times B)$ is well-defined into $A \times B$. It's associative—one may verify, elementwise, given that the functions $A \times A \to A$ and $B \times B \to B$, respectively, are associative.

(b) The identity $(1_A, 1_B) \in A \times B$ exists and is given by $1_A \in A$ and $1_B \in B$. We check for any $(a, b) \in A \times B$ that

$$(1_A, 1_B)(a, b) = (1_A \star a, 1_B \diamond b) = (a, b).$$

(c) Inverses exist for all $(a, b) \in A \times B$, given there's $(a, b)^{-1} = (a^{-1}, b^{-1}) \in A \times B$ such that $(a, b)(a^{-1}, b^{-1}) = (1_A, 1_B)$.

1.5. **Abelian groups and their direct products [1, No. 1.1.29].** The direct product $A \times B$ is an abelian group if and only if both A and B are abelian.

Proof. For any two elements $(a, b), (c, d) \in A \times B$

$$(a, b)(c, d) = (c, d)(a, b) \iff ac = ca \text{ and } bd = db$$

for all $a, c \in A$ and for all $b, d \in B$. □

1.6. **Dihedral groups of odd regular polygons [1, No. 1.2.5].** Suppose n is odd and $n \geq 3$. Then the identity is the only element in the dihedral group D_{2n} that commutes with all elements of D_{2n}. That is, for odd $n \geq 3$, the center $Z(D_{2n})$ is trivial. (My proof is attributable to the discussion of subgroups of D_{2n} in [2].)

Proof. No reflections are in the center $Z(D_{2n})$. Why? If r and s commute, then

$$(r^i s)r = r^i sr = r^i r^{-1} s = r^{i-1} s, \quad r(r^i s) = r^{i+1} s,$$

and knowing $r^i s$ commutes with s we see $r^{i-1} = r^{i+1}$. Whence $r^2 = 1$, which is false when $n \geq 3$.

Now we'll find the rotations r^j in the center. Without loss of generality let $0 \leq j \leq n - 1$. If r^j is in the center, it should commute with s. In this case, we have $r^j s = sr^j$, whence (by induction on the relation $rs = sr^{-1}$) it follows that $sr^{-j} = sr^j$. So $r^j = r^{-j}$ or $r^{2j} = 1$. Since the order of r in D_{2n} is n, we have must have $n|2j$. For odd n this implies $n|j$, i.e., j is a multiple of n. We conclude $r^j = 1$. So 1 is the only element in the center, that is, 1 is the only element in D_{2n} that commutes with all other elements.[4] □

1.7. **Computing permutations [1, No. 1.3.1].** Consider the permutations of S_5

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}.$$

We have the following cycle decompositions.

element	cycle decomposition
σ	(1 3 5)(2 4)
τ	(1 5)(3 2)
σ^2	(1 5 3)
$\sigma\tau$	(2 5 3 4)
$\tau\sigma$	(1 2 4 3)
$\tau^2\sigma$	σ

1.8. **Cycle decompositions in S_4 [1, No. 1.3.6].** To list the cycle decompositions for all elements in S_4 of order 4. Suppose that $|\sigma| = 4$. Then the least common multiple of the $|\sigma_i|$ in the cycle decomposition $\sigma = \prod \sigma_i$ is 4 (to be proven below). We proceed to determine the order of each σ_i. I claim because there's only one partition $4 = \sum k_i$ for

[4] Is showing that $r^j \in Z(D_{2n})$ iff $j = 0$ and $s \notin Z(D_{2n})$ sufficient to say that an arbitrary product $r^k s^j$ is not in the center?

positive integers k_i with $\operatorname{lcm}\{k_i\} = 4$, namely the partition $k = 4$, we know σ_i must be a 4-cycle (why?). It follows that the only elements of S_4 with order 4 are 4-cycles.

How many such 4-cycles are distinct? Well, there are 4! distinct strings of letters (with no letter repeated) from the alphabet of indices $\{i_1 i_2 i_3 i_4\}$. When such strings are considered as 4-cycles, we recognize that each 4-cycle has 4 representations as a string. That is,

$$(i_1 i_2 i_3 i_4) = (i_2 i_3 i_4 i_1) = (i_3 i_4 i_1 i_2) = (i_4 i_1 i_2 i_3)$$

so the total number of distinct 4-cycles in S_n is $4!/4 = 6$.

We exhaustive enumerate these 6 distinct 4-cycles by listing them in lexicographic order:

- (1 2 3 4)
- (1 2 4 3)
- (1 3 2 4)
- (1 3 4 2)
- (1 4 2 3)
- (1 4 3 2)

1.9. **The least common multiple of lengths of disjoint cycles [1, No. 1.3.15].** The order of an element in S_n is equal to the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof. We take it for granted that [3, Ch. 1.6]:

> Every nonidentity permutation in S_n is uniquely (up to the order of the factors) a product of disjoint cycles, each of which has length at least 2.

Now suppose that $\sigma \in S_n$, and write $\sigma = \sigma_1 \sigma_2 \dots \sigma_r$ with $\{\sigma_i\}$ disjoint cycles. Since disjoint cycles commute, $\sigma^m = \sigma_1^m \sigma_2^m \dots \sigma_r^m$ for all integers m. Now, the order $|\sigma|$ is defined as the least positive integer m for which $\sigma^m = 1$. We have $\sigma^m = 1$ if and only if $\sigma_i^m = 1$ for all i. So $\sigma^m = 1$ if and only if $|\sigma_i|$ divides n for all i. Because m is the least such integer, $m = \operatorname{lcm}\{|\sigma_i| \text{ where } \sigma_i \text{ is a disjoint cycle in the decomposition of } \sigma\}$. □

1.10. **Order of elements in S_5 [1, No. 1.3.18].** We find all numbers n such that S_5 contains an element of order n.

To do so, we will find all the numbers n such that $n = \operatorname{lcm}\{a_h \text{ for } a_h \text{ in a partition } 5 = \sum a_h\}$.

There's a bijective map φ from the set of partitions of 5 to the equivalence classes S_5/E given by the equivalence relation $\sigma E \tau$ if and only if, for the cycle decompositions

$$\sigma = \prod \sigma_i \text{ and } \tau = \prod \tau_j, \text{ we have } \left(\left|\sigma_{i_1}\right|, \dots, \left|\sigma_{i_m}\right|\right) = \left(\left|\tau_{j_1}\right|, \dots, \left|\tau_{j_m}\right|\right),$$

choosing indices $1 \le i_k \le m-1$ so that $\left|\sigma_{i_k}\right| \ge \left|\sigma_{i_{k+1}}\right|$ (and respectively for τ_{j_k}). Informally, $\sigma E \tau$ if they have cycle decompositions (for which we commute disjoint cycles to write the largest on the left) where order of the kth cycle in each is equal. The bijective map $\varphi\colon S_5/E \to \{\text{partitions of 5}\}$ associates each equivalence class of disjoint cycles with orders $(a_1, \dots, a_m)$ to the partition $5 = a_1 + \dots + a_m$ (verify this is a partition).

Now, the map of an element to its order in the group S_5, call it $|\cdot| : S_5 \to \mathbf{N}$, is compatible with the equivalence relation E in the sense that $\sigma E \tau$ implies $|\sigma| = |\tau|$. Because the order is compatible with the equivalence E, we can exhaustively describe the order of elements in S_5 by computing the order of a representative element in S_5/E. Fortunately, given our careful definition of φ, the order of a representative element a in the equivalence class $\overline{a}$ is given by the least common multiple of the image of $\overline{a}$ under φ. With ν the natural map (a surjection) from S_5 to S_5/E, the following diagram commutes.

We proceed to find the least common multiple of the a_h for all partitions $\sum a_h = 5$. There are 6 such partitions,

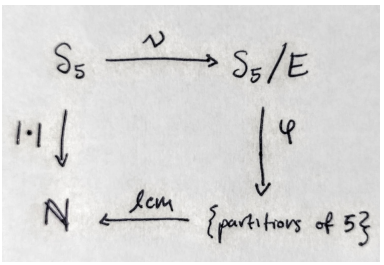

FIGURE 1. Symmetric group S_5 mapping to order of an element

$$\begin{aligned} 5 &= 5, & \operatorname{lcm}\{5\} &= 5 \\ &= 4+1, & \operatorname{lcm}\{4,1\} &= 4 \\ &= 3+2, & \operatorname{lcm}\{3,2\} &= 6 \\ &= 3+1+1, & \operatorname{lcm}\{3,1,1\} &= 3 \\ &= 2+1+1+1, & \operatorname{lcm}\{2,1,1,1\} &= 2 \\ &= 1+1+1+1+1, & \operatorname{lcm}\{1,1,1,1,1\} &= 1 \end{aligned}$$

So $\{1,2,3,4,5,6\}$ is the image of S_5 under the map $\operatorname{lcm} \circ \varphi \circ \nu$, or, by our argument, the image of S_5 under $|\cdot|$, so there is an element of order n in S_5 for $n = 1, 2, \ldots, 6$.

1.11. **Hamilton's quaternion group [1, No. 1.5.1].** To compute the order of each element in $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ we recall Hamilton's fundamental formula [4]

$$i^2 = j^2 = k^2 = ijk.$$

It's important to note $i^2 = -1$, and then we can proceed in tabulating

element	order in Q
1	1
-1	2
i	4
$-i$	4
j	4
$-j$	4
k	4
$-k$	4

REFERENCES

[1] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed. Hardcover; Prentice Hall, 2004 [Online]. Available: http://www.worldcat.org/isbn/0471433349

[2] K. Conrad, "Dihedral Groups" [Online]. Available: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral.pdf

[3] T. W. Hungerford, *Algebra*. Hardcover; Springer, 1974 [Online]. Available: http://www.worldcat.org/isbn/0387905189

[4] W. R. Hamilton and W. E. Hamilton, *Elements of quaternions*, vol. II. Longmans, Green, & Co., 1866 [Online]. Available: https://openlibrary.org/books/OL7211578M