KSOM ALGEBRA II 2021 MAY–AUG
NOTES AND TUTORIAL PROBLEMS: GROUP ACTIONS

(1) Let H be a subgroup of a group G. For g an element of G, let ${}^gH$ denote the conjugate gHg^{-1} of the subgroup H. Observe that $xH \mapsto xHg^{-1} = xg^{-1}\,{}^gH$ defines an isomorphism between the left G-sets G/H and $G/{}^gH$.

(2) The cardinality of any orbit under the action a finite group G divides the order of G. In particular, the cardinality of any conjugacy class of G divides the order of G.

(3) (Revision) Show from first principles that two permutations in the symmetric group $\mathfrak{S}_n$ are conjugate if and only if they have the same cycle type.

(4) Let $\lambda = 1^{r_1}2^{r_2}\ldots$ be the cycle type of a permutation σ in the symmetric group $\mathfrak{S}_n$ on n letters. Let $z_\lambda := 1^{r_1}2^{r_2}\cdots r_1!r_2!\cdots$. Show that the number of conjugates of σ in $\mathfrak{S}_n$ is $n!/z_\lambda$ and hence that the centraliser of σ has cardinality z_λ.

(5) Let $\mathbb{F}$ be a finite field with q elements. (Take, for example, $q = p$ to be a prime and $\mathbb{F}$ to be $\mathbb{Z}/p\mathbb{Z}$.) Let V be a vector space of finite dimension n over $\mathbb{F}$. Let k be an integer $0 \leqslant k \leqslant n$. What is the number of k-dimensional subspaces in V?

(6) (NBHM Master's Scholarship Test 2019) Let $\mathbb{F}$ be a field with exactly 7 elements. Let $\mathfrak{M}$ be the set of all 2×2 matrices with entries in $\mathbb{F}$. How many elements in $\mathfrak{M}$ are similar to the following matrix?:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

(7) (Cayley restated) For g an element of G, let ℓ_g denote the bijection $h \mapsto gh$ from G to itself. Then the map $g \mapsto \ell_g$ defines an injective group homomorphism from G to the group $\mathfrak{S}_G$ of bijections of G (where for p and q in $\mathfrak{S}_G$, the composition pq is defined to be the result obtained by first acting q first and then p). The resulting left action of G on G is the left regular action.

(8) (Semi-direct product) Let N be a group on which a group G acts by group automorphisms: $G \times N \to N$ denoted $(g, n) \mapsto {}^gn$ is a left action (that is, ${}^1n = n$ and ${}^{gh}n = {}^g({}^hn)$ for all n in N and all g, h in G) and ${}^g(n_1n_2) = {}^gn_1{}^gn_2$ for all g in G and all n_1, n_2 in N.
   (a) In this case we can form a new group called the semi-direct product of N and G, denoted $N \rtimes G$, as follows. As a set, it is the Cartesian product $N \times G$. Its multiplication is defined by $(n, g)(n', g') = (n\,{}^gn', gg')$. Verify that this definition satisfies the axioms for the multiplication in a group.
   (b) We may identity N and G respectively as the subgroups $N \times \{1\}$ and $\{1\} \times G$ of $N \rtimes G$. Note that N is normal in $N \rtimes G$ (which justifies the notation) and that the original action of G on N gets identified with the conjugation action of G on N (within $N \rtimes G$): $({}^gn, 1) = (1, g)^{-1}(1, n)(1, g)$.

(c) If the action of G on N is trivial, then the semi-direct product $N \rtimes G$ is just the direct product $N \times G$.

(9) (Semi-direct product continued) Let K be a group, N a normal subgroup of K, and G a subgroup of K. Restrict to G the conjugation action of K on N and form the semi-direct product $N \rtimes G$. We have a natural group homomorphism $N \rtimes G \to K$ given by $(n, g) \mapsto ng$. We say that K is the semi-direct product of N and G and write $K = N \rtimes G$ if the above homomorphism is an isomorphism.

(10) (Example of a semi-direct product) Given an abelian group A, there is a natural action of the group $\{\pm 1\} = \{1, t\}$ of two elements by group automorphisms on A given by $t(a) = -a$. We can form the semi-direct product $A \rtimes \{\pm 1\}$.

(11) (Cayley refined for semi-direct product) Let $K = N \rtimes G$ be a semi-direct product. Let $\ell : N \hookrightarrow \mathfrak{S}_N$ defined by $n \mapsto \ell_n$ be the Cayley homomorphism for N, where $\mathfrak{S}_N$ denotes the group of bijections of N. The image $\ell(N)$ is normalized by the subgroup $\operatorname{Aut} N$ of group automorphisms of N: for φ an automorphism of N and n an element of N, we have $\varphi \ell_n \varphi^{-1} = \ell_{\varphi n}$. Let $\rho : G \to \mathfrak{S}_N$ be the group homomorphism defining the action of G on N by group automorphisms. Let us now assume that ρ is an injection. Then, by identifying N and G with their images in $\mathfrak{S}_N$ under ℓ and ρ respectively, we may realize within $\mathfrak{S}_N$ the groups N, G, and the action of G on N. The subgroup of $\mathfrak{S}_N$ generated by $\ell(N)$ and $\rho(G)$ is the semi-direct product $\ell(N) \rtimes \rho(G)$, which is isomorphic to $N \rtimes G$.

(12) The solution to this problem is useful in analysing the dihedral group. Let R and S be respectively reflections of the Euclidean plane $\mathbb{R}^2$ in two lines k and l passing through the origin. Give a geometric description of $R \circ S$. When do R and S commute?

(13) (The dihedral group D_n) Let D_n denote the dihedral group, the group of symmetries of the regular n-gon. As is well known, it has the following presentation: $D_n = \langle r, s \,|\, r^n = 1,\ s^2 = 1,\ srs^{-1} = srs = r^{n-1} \rangle$. Here are some alternative descriptions of D_n:

(a) the group of automorphisms of the "cyclic graph" on n-vertices.

(b) the semi-direct product $\mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$ described in a previous item above.

(c) the group with the presentation $\langle s, t \,|\, s^2 = t^2 = 1,\ (st)^n = 1 \rangle$.

(14) (The dihedral group D_∞) This is the semi-direct product $\mathbb{Z} \rtimes \{\pm 1\}$ (obtained by taking $A = \mathbb{Z}$ in one of the previous items above). It has the presentation $\langle s, t \,|\, s^2 = t^2 = 1 \rangle$, and can be realized as the subgroup of isometries of the real line $\mathbb{R}$ generated by $s(x) = -x$ and $t(x) = 1 - x$.

(15) Discuss the conjugacy classes of the dihedral group D_n using geometry.

(16) (The group of isometries of $\mathbb{R}^2 \simeq \mathbb{C}$) Let G be the group of isometries of $\mathbb{R}^2 \simeq \mathbb{C}$. We identify three subgroups of G as follows:

- The subgroup C generated by the map $c : z \mapsto \bar{z}$ is isomorphic to $\{\pm 1\}$.

- The group $\{\lambda \in \mathbb{C} \mid |\lambda| = 1\}$ (of non-zero complex numbers under multiplication) embeds in G by $\lambda \mapsto e_\lambda$, where $e_\lambda(z) := z\lambda$ for z in $\mathbb{C}$. We denote its image by R.
- The group $(\mathbb{C}, +)$ embeds in G by $x \mapsto t_x$, where $t_x : z \mapsto z + x$. We denote its image by T.

Observe that C normalizes R ($ce_\lambda c^{-1} = ce_\lambda c = e_{\bar{\lambda}}$). The subgroup generated by C and R is the semi-direct product $R \rtimes C$. The subgroup T is normal in G ($gT_xg^{-1} = T_{g(x)}$) and G is the semi-direct product $T \rtimes (R \rtimes C)$.

(17) True of false?: Given an arbitrary subset S of G, there is a unique maximal subgroup K of G such that S is a union of right cosets of K.

(18) Let G denote the cyclic group of order m. For n a positive integer let $q(n)$ be the number of G-isomorphism classes of G-sets of cardinality n. Set $q(0) = 1$ (by definition). Show that the generating function $Q(t) := \sum_{n \geqslant 0} q(n)t^n$ equals

$$Q(t) = \frac{1}{\prod_{d|m}(1 - t^d)}$$

(19) For each of the following groups G, determine the number of orbits for the action of G on the power set of G induced from the left regular action of G on itself: the cyclic group of order 10, the Dihedral group D_p where p is an odd prime, and the symmetric group $\mathfrak{S}_4$. (Answers: 108, $2(2^{p-1} + p - 1)/p$, 701696.)

(20) Let H be a subgroup of a group G of finite index d. Then there exists a normal subgroup N of G that is contained in H and such that G/N imbeds in the symmetric group $\mathfrak{S}_d$. In particular, the index of N in G is at most $d!$. (Hint: Let $N = \cap_{g \in G} {}^gH$. Then the group homomorphism from G to $\mathfrak{S}_{G/H}$ defining the left action of G on G/H factors through G/N and the resulting map from G/N is injective.) In particular, an infinite simple group does not admit a finite index subgroup.

(21) (Jordan's lemma) Let X be a finite set consisting of at least 2 elements on which a group G acts transitively. Then there exists an element g of G that fixes no element of X. (Hint: We reduce to the case when G is finite using item (20) above. Invoke Burnside's lemma. The RHS of the lemma should work out to 1. Suppose that $|X^g| \geqslant 1$ for every g in G. Then the RHS is strictly bigger than 1, since $|X^{\text{id}}| = |X| \geqslant 2$, a contradiction.)

(22) (Some corollaries of Jordan's lemma) Given a finite but non-singleton conjugacy class in a group, there exists an element of the group that commutes with no element of the conjugacy class. Given a finite index proper subgroup H of a group, the conjugates of H cannot cover the group.

(23) Let G be a p-group and X a G-set. Then $|X| \equiv |X^G| \bmod p$. (Write X as a disjoint union of its orbits. The elements each of which forms a singleton orbit by itself are precisely those belonging to X^G. The cardinalities of the non-singleton orbits are divisible by p, since they divide $|G|$ and are bigger than 1.) Taking X to be G itself

with the conjugation action, we conclude that every p-group has non-trivial centre. (Because X^G in that case is the centre, and X^G is non-empty since the identity element belongs to it.)

(24) Let G be a group, and N a central subgroup such that G/N is cyclic. Then G is abelian. Conclude, using this fact, that a group of order p^2 (where p is a prime) is abelian.

(25) There exists a non-abelian group of order p^3 (for any prime p).

(26) (The class equation) Consider the conjugation action of a finite group G on itself. The orbits are the conjugacy classes. An element of the group forms a conjugacy class by itself if and only if it is central. We thus obtain

$$\boxed{|G| = |\text{centre of } G| + \sum |C|}$$

where the sum is over all non-singleton conjugacy classes C. This is called the class equation of G. Note that each summand $|C|$ occurring in the sum on the RHS is a factor of $|G|$ (see item (2) above).