# ACTIONS AND SUBGROUPS

COLTON GRAINGER (MATH 6130 ALGEBRA)

## 3. Assignment due 2018-09-19

3.1. **[1, No. 2.1.8].** Let $H$ and $K$ be subgroups of a group $G$. $H \cup K$ is a subgroup if and only if either $H \subset K$ or $K \subset H$.

*Proof.*[1] ($\Rightarrow$) If $H \subset H$ or $K \subset H$ then $H \cup K$ is $K$ or $H$, hence $H \cup K$ is a subgroup of $G$.

($\Leftarrow$) Suppose $H \cup K$ is a subgroup of $G$. For contradiction, let $H \not\subset K$ and $K \not\subset H$. Then choose $h \in H \setminus K$ and $k \in K \setminus H$. Because $H \cup K$ is closed as a subgroup, we have $hk \in H \cup K$. But in which set $H$ or $K$ is $hk$ an element? Either $hk \in H$, hence $h^{-1}hk \in H$, hence $k \in H$; or $hk \in K$, hence $hkk^{-1} \in K$, hence $h \in K$; which is the desired contradiction. □

3.2. **[1, No. 2.1.9].** Let $G = GL_n(\mathbf{F})$ where $\mathbf{F}$ is an field. We define the *special linear group*

$$SL_n(\mathbf{F}) = \{A \in GL_n(\mathbf{F}) : \det(A) = 1\}.$$

Then $SL_n(\mathbf{F}) \leq GL_n(\mathbf{F})$.

*Proof.* Knowing that $GL_n(\mathbf{F})$ is a group of which $SL_n(\mathbf{F})$ is a subset, it suffices to show that $SL_n(\mathbf{F})$ is nonempty and closed under products and taking inverses.

- (Nonempty) The identity $n \times n$ matrix $I \in SL_n(\mathbf{F})$ since $\det(I) = 1^n = 1$.
- (Products) Let $A, B \in SL_n(\mathbf{F})$. Then $\det(A) = \det(B) = 1$. So $\det(AB) = \det(A)\det(B) = 1$, thus $AB \in SL_n(\mathbf{F})$.
- (Inverses) Let $A \in SL_n(\mathbf{F})$. So $\det(A) = 1$, and since $\det(A^{-1}) = \frac{1}{\det(A)} = 1$, we have $A^{-1} \in SL(\mathbf{F})$.

So $SL_n(\mathbf{F}) \leq GL_n(\mathbf{F})$. □

3.3. **[1, No. 2.1.14].** The set $\{x \in D_{2n} : x^2 = 1\}$ is not a subgroup of $D_{2n}$ (where $n \geq 3$).

*Key idea.*[2] The elements of the dihedral group of order 1 or 2 are

- the identity,
- any of the $n$ reflections, and
- if $n$ is even, the rotation by $\pi$.

The set of such elements is not closed under composition.

*Proof.* Consider the presentation $D_{2n} = \langle r, s : r^n = s^2 = 1, sr^is = r^{-i}\rangle$. If $x \in D_{2n}$, then $x$ can be written as a product of generators $x = r^is^j$ where $i \in \{0, \ldots, n-1\}$ and $j \in \{0, 1\}$.

What is $\{x \in D_{2n} : x^2 = 1\}$? Or writing the elements of $D_{2n}$ as $r^is^j$, for which powers $i$ and $j$ is it true that $(r^is^j)^2 = 1$?

- When $j = 0$, we have $r^{2i} = 1$. Because $i < n$ and $n|2i$, either $i = 0$ or, if $n$ is even, $i \in \{0, \frac{n}{2}\}$.
- When $j = 1$, we have $(r^is)^2 = 1$ for all $i$, since $r^i(sr^is) = r^i(r^{-i}) = 1$.

*Date:* 2018-09-16.
*Compiled:* 2018-10-05.

[1] See `https://math.stackexchange.com/questions/334405/`, "Suppose both $H, K$ are distinct and proper. Then pick $h \in H \setminus K$ and $k \in K \setminus H$. In which of $K$ or $H$ or both does $hk$ lie?"

[2] See `https://math.stackexchange.com/questions/126639/`, "We can think of this geometrically, or use a presentation [. . . ]"; see also `https://groupprops.subwiki.org/wiki/Element_structure_of_dihedral_groups`.

So let $A = \{x \in D_{2n} : x^2 = 1\}$. We've shown

$$A = \left\{1, r^k, r^i s : k = 0 \text{ or, if } n \text{ is even, } k = \frac{n}{2}, i \in \{0, \dots, n-1\}\right\}.$$

To see $A$ is not closed, take $r^2 s, rs \in A$. But $(r^2 s)(rs) = r^2(srs) = r^2 r^{-1} = r \notin A$ (when $n \geq 3$). □

3.4. **[1, No. 2.2.6].** Let $H$ be a subgroup of the group $G$.

(a) $H \leq N_G(H)$. (This is not necessarily true if $H$ is not a subgroup.) Suppose that $H \leq G$, a group, and consider $N_G(H)$. Let $h \in H$. Now the normalizer of $H$ in $G$ is the set of all elements that fix $H$ under the conjugation action. Is it true that $hah^{-1} \in H$ for all $a \in H$? Yes, as $H$ is closed. So $h \in N_G(H)$, hence $H \leq N_G(H)$.

Consider $H \subset G$ but not $H \leq G$, for example,

$$H = \{(1\,2), (1\,2\,3)\} \text{ and } G = S_3.$$

Now the normalizer of $H$ in $S_3$ is the set

$$N_{S_3}(H) = \{g \in S_3 : \{g(1\,2)g^{-1}, g(1\,2\,3)g^{-1}\} = \{(1\,2), (1\,2\,3)\}\}$$

but $(1\,2) \notin N_{S_3}(H)$ as $\{(1\,2), (1\,3\,2)\} \neq \{(1\,2), (1\,2\,3)\}$.

(b) $H \leq C_G(H)$ if and only if $H$ is abelian. ($\Rightarrow$) Suppose $H$ is abelian, and consider $h \in H$. Since conjugation of $a \in H$ by $h$ fixes $a$ ($hah^{-1} = a$ whenever $ha = ah$), we have $h \in C_G(A)$. So $H$ is a subgroup of the centralizer $C_G(H)$. ($\Leftarrow$) Now suppose that $H \leq C_G(H)$. Then if $h \in H$, we have $h$ also in the centralizer of $H$ in $G$. So $hah^{-1} = a$ for all $a \in H$. Hence $ha = ah$ for all $a, h \in H$, and we conclude $H$ is abelian.

3.5. **[1, No. 2.2.10].** Let $H$ be a subgroup of order 2 in $G$. Then $N_G(H) = C_G(H)$.

*Proof by set inclusion.* ($\subset$) Suppose $g \in N_G(H)$. Because $H$ is a group of order 2, it is $\{1, x\}$ where $x^2 = 1$. If conjugation by $g$ fixes $H$, then $\{g1g^{-1}, gxg^{-1}\} = \{1, x\}$. Whence $\{1, gxg^{-1}\} = \{1, x\}$. For set equality, we must have $gxg^{-1} = x$. So $g \in C_G(H)$. ($\supset$) By definition, if $g \in C_G(H)$, then $g$ fixes each $h \in H$ by conjugation, so $g$ fixes $H$ by conjugation. □

Also, if $N_G(H) = G$, then $H \leq Z(G)$. TODO.

3.6. **[1, No. 2.2.12].** Let $R$ be the set of all polynomials with integer coefficients in the independent variables $\{x_j\}_1^4$. That is, members of $R$ are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$ where $a \in \mathbf{Z}$ and $r_j \in \mathbf{Z}_{\geq 0}$.

Each $\sigma \in S_4$ gives a permutation of $\{x_1, x_2, x_3, x_4\}$ by defining $\sigma \cdot x_j = x_{\sigma(j)}$. This extends naturally to a map from $R$ to $R$ by defining

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $p(x_1, x_2, x_3, x_4) \in R$ (that is, $\sigma$ simply permutes the indices of the variables).

(a) Let $p = p(x_1, x_2, x_3, x_4)$ be the polynomial

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23}$$

and consider the permutations $\sigma = (1\,2\,3\,4)$ and $\tau = (1\,2\,3)$. We compute:

- $\sigma \cdot p = 12x_2^5x_3^7x_1 - 18x_3^3x_4 + 11x_2^6x_3x_4^3x_1^{23}$
- $\tau \cdot (\sigma \cdot p) = 12x_3^5x_1^7x_2 - 18x_1^3x_4 + 11x_3^6x_1x_4^3x_2^{23}$
- $(\tau \circ \sigma) \cdot p = 12x_3^5x_1^7x_2 - 18x_1^3x_4 + 11x_3^6x_1x_4^3x_2^{23}$
- $(\sigma \circ \tau) \cdot p = 12x_3^5x_4^7x_1 - 18x_4^3x_2 + 11x_3^6x_4x_2^3x_1^{23}$

(b) This definition $(\sigma, p) \mapsto \sigma \cdot p$ gives a left subgroup action of $S_4$ on $R$. For clarity denoted $p(x_1, x_2, x_3, x_4)$ as $p(x_k)_1^4$. Then for all $\sigma, \tau \in S_4$ and $p \in R$ we have (GA1)

$$\begin{aligned}\sigma \cdot (\tau \cdot p) &= \sigma \cdot (\tau \cdot p(x_k)_1^4) \\ &= \sigma \cdot p(x_{\tau(k)})_1^4) \\ &= p(x_{\sigma(\tau(k))})_1^4) \\ &= p(x_{(\sigma\circ\tau)(k)})_1^4) \\ &= (\sigma \circ \tau)\cdot (x_k)_1^4.\end{aligned}$$

For (GA2) note that $\mathrm{id} \cdot p = p(x_{\mathrm{id}(k)})_1^4 = p$ for all $p \in R$.

(c) We exhaustively list all permutations in $S_4$ that stabilize $x_4$. They form a subgroup isomorphic to $S_3$.

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

(d) We list all permutations in $S_4$ that stabilize $x_1 + x_2$. They form an abelian subgroup of order 4.

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

(e) We list all permutations in $S_4$ that stabilize $x_1x_2 + x_3x_4$. They form a subgroup isomorphic to the dihedral group of order 8.

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

(f) The permutations in $S_4$ that stabilize the element $(x_1 + x_2)(x_3 + x_4)$ are the same as those in part (e). In our group action, there are $2^2$ permutations that stabilize the sums, and 2 permutations that stabilize the product. In part (e), we had 2 permutations to stabilize the sum, and $2^2$ to stabilize the product. Given the pairing of indices 1 with 2 and 3 with 4, however, the same permutations stabilize both elements in $R$, $x_1x_2 + x_3x_4$ and $(x_1 + x_2)(x_3 + x_4)$.

3.7. **[1, No. 2.3.25].** Let $G$ be a cyclic group of order $n$ and let $k$ be an integer relatively prime to $n$. The map $x \mapsto x^k$ is surjective.

*Proof.* Let $G = \langle x \rangle$ be a cyclic group of finite order $n$ generated by $x$, let $k$ be an integer relatively prime to $n$, and let $f : G \to G$ map $g \mapsto g^k$. We will show $f$ is surjective.

As a preliminary, note for all $g \in G$, there's a (unique!) modulo $n$ congruence class $\overline{c} \in \{\overline{0}, \ldots, \overline{n-1}\}$ for which $g = x^c$ where $c$ is the least residue of $\overline{c}$.

Now $f$ is surjective if for each $\overline{c} \in \{\overline{0}, \ldots, \overline{n-1}\}$ there's a $\overline{m} \in \{\overline{0}, \ldots, \overline{n-1}\}$ such that $km \in \overline{c}$, since then $f(x^m) = (x^m)^k = x^{km} = x^c$. So consider such a class $\overline{c}$. If $\overline{c} = \overline{0}$ we have $\overline{m} = \overline{0}$ satisfying $f(x^0) = f(1) = 1 = x^0$. Else we have

$\overline{c} \neq \overline{0}$. Now because $\gcd(k, n) = 1$, there's a $\mathbf{Z}$-linear combination of $k$ and $n$ such that $a, b \in \mathbf{Z}$ and

$$\begin{aligned} & ak + bn = 1, \\ \text{hence} \quad & cak + cbn = c, \\ \text{hence} \quad & (cb)n = c - (ca)k, \\ \text{hence} \quad & n \text{ divides } c - (ca)k \end{aligned}$$

Let $m$ be the least residue of $ca \pmod{n}$, and we have the desired class $\overline{m}$. Because for each $g \in G$, we have $x^m \in G$ such that $f(x^m) = (x^m)^k = x^{km} = x^{k(ca)} = x^c = g$, we conclude that $f$ is surjective. □

Moreover, for any group $G$ of finite order $n$, the same map $x \mapsto x^k$ is surjective when $k$ and $n$ are relatively prime.

*Proof.* If $G$ is of finite order $n$ and $x \in G$, then $|x|$ divides $|G|$ by Lagrange's theorem. So consider each cyclic group $\langle x_i \rangle$ in the domain for all $x_i \in G$. Restrict $f : G \to G$ to $\langle x_i \rangle$ and repeat the previous argument. Indeed, $\gcd(k, n) = 1$ and $|x_i|\,|n$ implies $\gcd(k, |x_i|) = 1$. Now each $\langle x_i \rangle$ is finite, so each restriction $f|_{\langle x_i \rangle}$ is surjective onto $\langle x_i \rangle$. The function $f$ is given piecewise as finitely many surjective functions on disjoint domains, whence we conclude that $f$ is surjective. □

3.8. **[1, No. 2.4.3].** If $H$ is an abelian subgroup of a group $G$ then $\langle H, Z(G) \rangle$ is abelian.

*Proof sketch.* Consider $x, y \in \langle H, Z(G) \rangle$. Now write these elements as products of generators $x = \prod_1^k h_i^{\alpha_i}$ (for $\alpha_i \in \mathbf{Z}$ and $h_i \in H \cup Z(G)$) and $y = \prod_1^\ell g_i^\beta$ (for $\beta \in \mathbf{Z}$ and $g_i \in H \cup Z(G)$). Each $h_i$ and $g_i$ with all elements of $H$ (by hypothesis) and $Z(G)$ (by definition of the center). Whence $xy = yx$. So $\langle H, Z(G) \rangle$ is abelian.

We exhibit an abelian subgroup of $H$ of $G$ such that $\langle H, C_G(H) \rangle$ is *not* abelian. That is, we want $xy \in C_G(H)$ such that $x$ and $y$ fix each $h \in H$ under the conjugation action, but where $xy \neq yx$. Consider $H = \{e\}$ and $G = S_3$. We have $H$ trivially abelian, so $C_G(H) = G = S_3$, and yet $\langle \{e\}, S_3 \rangle = S_3$ is not abelian, as desired.

3.9. **[1, No. 2.4.12].** The subgroup of upper triangular matrices in $GL_3(\mathbf{F}_2)$ is isomorphic to the dihedral group of order 8.

*Demonstration.* Let $H$ be the subgroup of upper triangular matrices in $GL_3(\mathbf{F}_2)$. Since elements of $H$ must be invertible, they must have full rank. Hence the diagonal of each matrix in $H$ must be filled with 1's. That gives $2^3$ distinct matrices in $H$. To show an isomorphism, we write out an epimorphism $\varphi : H \to D_8$ from the generators of $H$ to the generators of $D_8$ and argue that $\varphi(H)$ satisfies the relations on the given generators of $D_8$.

Let $\varphi$ be defined by

$$A = \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \mapsto r \quad \text{and} \quad B = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mapsto s.$$

One may verify that $A, B$ are generators of $H$. (Note that least integers $m, n$ such that $A^n = B^m = 1$ are $m = 2$ and $n = 4$.) One may verify that $AB^kA = B^{-k}$ for $k = 1, 2, 3$. Having a surjective map from the generators of $H$ to the generators of $D_8$, we see that $\varphi$ is an epimorphism. That $\varphi(H)$ satisfies the relations on the generators of $D_8$, we see that $\varphi$ is an isomorphism.

3.10. **[1, No. 2.4.15].** There's a proper subgroup of $\mathbf{Q}$ which is not cyclic.

*Demonstration.* Consider the family of cyclic subgroups of $\mathbf{Q}$

$$\left\{ \left\langle \frac{1}{2^n} \right\rangle : n \in \mathbf{N} \right\}.$$

If $n \leq m$, then $\left\langle \frac{1}{2^n} \right\rangle \leq \left\langle \frac{1}{2^m} \right\rangle$. Then certainly

$$\left\langle \frac{1}{2} \right\rangle \leq \bigcup_{n \in \mathbf{N}} \left\langle \frac{1}{2^n} \right\rangle = H.$$

Now $H$ is the intersection of a family of subgroups, and is therefore a subgroup of $\mathbf{Q}$. By construction, $H$ is not trivial. Further, $\frac{1}{3} \notin H$, so $H$ is not $\mathbf{Q}$.

3.11. **[1, No. 2.4.16].** A subgroup $M$ of a group $G$ is called a *maximal subgroup* if $M \neq G$ and the only subgroups of $G$ which contain $M$ are $M$ itself and $G$.

(a) If $H$ is a proper subgroup of the finite group $G$, then there is a maximal subgroup of $G$ containing $H$.

Consider the elements in $G \setminus H$. Let $|G \setminus H| = |G| - |H| = m$. There are then $2^m - 1$ proper subsets of $G$ containing $H$. Either $H$ is it's own maximal group in $G$, or one of the $2^m - 1$ proper subsets is a maximal group.

(b) The subgroup of all rotations in a dihedral group is a maximal subgroup.

The set of rotations in $D_8$ is a subgroup of order 4. Now every other subgroup of $D_8$ has an order which divides 8, of which 4 is the largest order strictly less than 8. So the set of rotations is maximal in $D_8$, for the only subgroups it is properly contained in are $D_8$ and itself.

(c) If $G = \langle x \rangle$ is a cyclic sugroup of order $n \geq 1$, then a subgroup $H$ is maximal if and only if $H = \langle x^p \rangle$ for some prime $p$ dividing $n$.

TODO.

3.12. **Maximal subgroups in a finite group.** A finite group with no more that two maximal subgroups is cyclic.

TODO.

## 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`