PRESENTATIONS, REPRESENTATIONS AND GROUP ACTIONS

COLTON GRAINGER (MATH 6130 ALGEBRA)

1. Assignment due 2018-09-12

1.1. **Generating the dihedral groups [1, No. 1.2.7].** We have

$$\langle a, b : a^2 = b^2 = (ab)^n = 1 \rangle$$

as a presentation for D_{2n} in terms of the two generators[1] $a = s$ and $b = sr$ of order 2.

To verify, denote the above presentation as D_{ab} and define $\varphi\colon D_{2n} \to D_{ab}$ by $s \mapsto a$, $r \mapsto ab$, and $r^{-1} \mapsto ba$. We'll show that φ is an isomorphism of groups.

To show φ is a homomorphism, check that the images of the generators r and s satisfy the relations in the canonical presentation of D_{2n}:

- $\varphi(s)^2 = a^2 = 1$,
- $\varphi(r)^n = (ab)^n = 1$, and
- $\varphi(r)\varphi(s) = (ab)a = a(ba) = \varphi(s)\varphi(r^{-1})$.

So φ is a homomorphism. Consider now $\ker(\varphi)$. Exhaustively, we list elements in the preimage.

- $s^2 = \varphi^{-1}(a^2)$
- $srsr = \varphi^{-1}(b^2)$
- $r^n = \varphi^{-1}((ab)^n)$

Each element in the domain can be simplified to the identity. So the kernel of φ is trivial and φ is an isomorphism. That is, $D_{ab} \cong D_{2n}$. We've shown that D_{ab} gives a presentation of D_{2n} in terms of generating elements of order 2.

1.2. **General linear groups on finite fields [1, No. 1.4.5].** $GL_n(F)$ is a finite group if and only if F has a finite number of elements.

Proof. ($\Rightarrow$) Suppose F is finite, say of (prime) order p. If $A \in GL_n(F)$, then we'd better have that $\det(A) \neq 0$. We'll enumerate all such possible matrices A.

Consider all distinct n-tuples of elements in F, concretely, they are the functions $f\colon \{1, \dots, n\} \to F$. There are $|F|^n = p^n$ such distinct functions. Note only one such function maps each number j to $0 \in F$.

Now, minding that $\det(A) \neq 0$, we can populate the first row of A with $p^n - 1$ distinct nonzero n-tuples with entries from F. The second row cannot be a multiple of the first, so we can populate the second row with only $p^n - p$ distinct nonzero n-tuples. The jth row has in general $p^n - p^j$ possible arrangements. Hence there are

$$\prod_{j=0}^{n-1} (p^n - p^j)$$

distinct matrices in $GL_n(F)$. So $GL_n(F)$ is finite.

($\Leftarrow$) Suppose F is infinite. Then the set of (invertible) diagonal matrices in $GL_n(F)$ is infinite. So $GL_n(F)$ is infinite. □

Date: 2018-09-12.

Compiled: 2018-10-05.

[1] We assume that every element of D_{2n} which is not a power of r has order 2, whence one can deduce that D_{2n} is generated by the two elements s and sr both of which have order 2. See [1, No. 1.2.3].

1.3. **The Heisenberg group over a field [1, No. 1.4.11].** For a given field F (usually $F = \mathbf{R}$ for a meaningful interpretation in quantum mechanics), let $H(F)$ be the set of unit upper triangular 3×3 matrices with elements in the upper two diagonals from the field F, e.g.,

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ such that } a, b, c \in F \right\}.$$

We call this set the *Heisenberg group* over F.

(a) $H(F)$ is closed under matrix multiplication. The set of unit upper triangular matrices (of any finite dimension) is closed under multiplication; specifying, $H(F)$ is closed under matrix multiplication.
(b) $H(F)$ is non-abelian. For example

$$\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}.$$

(c) $H(F)$ is closed under inverses, with the explicit formula for the matrix inverse of

$$\begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \text{ given by } \begin{pmatrix} 1 & -a & ac-b \\ & 1 & -c \\ & & 1 \end{pmatrix}.$$

(d) The associative law holds for $H(F)$. That is, matrix multiplication is associative, and this is a specific case. (Thus $H(F)$ is a group).
(e) Every nonidentity element of the group $H(\mathbf{R})$ has infinite order. (Only $0 \in \mathbf{R}$ has finite additive order.) So if a or c is not 0, then

$$\begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & - \\ & 1 & nc \\ & & 1 \end{pmatrix} \neq I \text{ for all } n \in \mathbf{Z}.$$

1.4. **The order of images under isomorphism [1, No. 1.6.2].** If $\varphi \colon G \to H$ is an isomorphism, then $|\varphi(x)| = |x|$ for all $x \in G$.

Proof. Suppose $\varphi \colon G \to H$ is an isomorphism. Then for each element $g \in G$ of finite order there's a unique minimal element in the set $\{n \in \mathbf{N} : g^n = 1\}$. So $\varphi(g)^n = \varphi(g^n) = \varphi(1) = 1$. Hence $|\varphi(g)| \leq |g|$.

Since φ is an isomorphism, its inverse φ^{-1} exists and is an isomorphism. We recapitulate: For each $\varphi(g) \in H$ there's a unique minimal $m \in \mathbf{N}$ such that $\varphi(g)^m = 1$. So $g^m = \varphi^{-1}(\varphi(g))^m = \varphi^{-1}(\varphi(g)^m) = \varphi^{-1}(1) = 1$. Hence $|g| \leq |\varphi(g)|$.

We conclude that $|g| = |\varphi(g)|$, and continue with a corollary. □

Any two isomorphic groups have the same number of elements of order n for each $n \in \mathbf{N}$.

Proof sketch. $\varphi \colon G \to H$ is a bijection. Consider an equivalence relation such that gEh if and only if $|g| = |h|$. Since $|g| = |h|$ if and only if $|\varphi(g)| = |\varphi(h)|$ we have gEh if and only if $\varphi(g)E\varphi(h)$. We see that φ is a bijection that respects membership in the equivalence classes G/E and H/E of elements of order n. □

1.5. **Isomorphism preserves commutativity [1, No. 1.6.3].** If $\varphi \colon G \to H$ is an isomorphism, then G is abelian if and only if H is abelian.

Proof. ($\Rightarrow$) Suppose that G is abelian. Then each pair of elements $a, b \in G$ commutes. So $ab = ba$. Hence $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$. Since φ is surjective, each pair $c, d \in H$ is the image under φ of commutative elements. So H is abelian. ($\Leftarrow$) Suppose H is abelian. It's the same argument with the isomorphism φ^{-1}. □

We state as a corollary, if G is abelian and $\varphi \colon G \to H$ is a surjective homomorphism, then H is abelian.

1.6. **The automorphism group of G [1, No. 1.6.20].** Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G (these isomorphisms are called *automorphisms* of G). Then $\mathrm{Aut}(G)$ is a group (called the *automorphism group* of G) under function composition.

Proof. We'll show $\mathrm{Aut}(G)$ is a group. First note that $\circ\colon \mathrm{Aut}(G)\times\mathrm{Aut}(G) \to \mathrm{Aut}(G)$ is well defined as the composition of two isomorphisms is again an isomorphism.

(G3) Recall that function composition is associative, so the binary operation $\circ$ is associative. (G1) The identity set map id_G exists and is the identity automorphism. (G2) If $\varphi \in \mathrm{Aut}(G)$ then φ is a bijective homomorphism from G to G, so its functional inverse φ^{-1} is a bijective homomorphism with again from G to G, thus an automorphism. Hence $\varphi^{-1} \in \mathrm{Aut}(G)$. One verifies that φ^{-1} is the left and right inverse of φ in the group $\mathrm{Aut}(G)$ by composing φ^{-1} with φ on the left and right to obtain id_G. □

1.7. **An automorphism fixed point free [1, No. 1.6.23].** Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, then G is abelian.[2]

Proof sketch. Suppose G is finite and there's an automorphism σ of G such that σ fixes $g \in G$ if and only if $g = 1$. Further suppose that $\sigma^2 = \mathrm{id}_G$.

Knowing that G is finite, that σ is a bijection, and that each x^{-1} is corresponds uniquely with $x \in G$, apply the pigeon hole principle to write every element of $y \in G$ *uniquely* as $y = x^{-1}\sigma(x)$. Now take

$$\sigma(y) = \sigma(x^{-1}\sigma(x)) = \sigma(x^{-1})\sigma^2(x) = \sigma(x)^{-1}\mathrm{id}_G(x).$$

TODO. Show G is abelian.

1.8. **Faithful actions of multiplicative groups of fields [1, No. 1.7.8].** Consider a vector space V over a field F. We have then the multiplicative group $F^\times = (F \setminus \{0\}, \cdot)$ acting on the set V.

In the special case that $V = \mathbf{R}^n$ and $F = \mathbf{R}$, the action is specified by

$$\alpha(r_1, \ldots, r_n) = (\alpha r_1, \ldots, \alpha r_n)$$

for all scalars $\alpha \in \mathbf{R}$ and vectors $(r_1, \ldots, r_n) \in \mathbf{R}^n$.

This action is faithful. Why? Suppose that $\beta(\vec{v}) = \vec{v}$ for all $\vec{v} \in \mathbf{R}^n$, then component-wise $\beta v_i = v_i$ for all $v_i \in \mathbf{R}$. The field $\mathbf{R}$ has unique multiplicative identity, so $\beta = 1$ (note that β is synonymously the multiplicative identity for the group $\mathbf{R}^\times$). This is to say, distinct scalars $\alpha, \beta \in \mathbf{R}^\times$ induce distinct permutations on $\mathbf{R}^n$.

1.9. **Non-example of an action by a non-abelian group [1, No. 1.7.14].** Let G be a non-abelian group and let $A = G$. The maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

(GA1) Fails to hold generally in a non-abelian group; consider $(gh) \cdot a = agh \neq ahg = g \cdot (h \cdot a)$ whenever $gh \neq hg$.

1.10. **A group action by left multiplication [1, No. 1.7.15].** Let G be a group and let $A = G$. The maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ *do* satisfy axioms of a (left) group action of G on itself.

(GA1) We verify $(gh)\cdot a = a(gh)^{-1} = ah^{-1}g^{-1}$ and $g\cdot(h\cdot a) = g\cdot(ah^{-1}) = ah^{-1}g^{-1}$. (GA2) Note $1 \cdot a = a1^{-1} = a1 = a$.

1.11. **Orbits under an action [1, No. 1.7.18].** Let H be a group acting on a set A. The relation $\sim$ on A defined by

$$a \sim b \text{ if and only if } a = hb \text{ for some } h \in H$$

is an equivalence relation.[3]

Proof. We verify reflexivity, symmetry, and transitivity for the relation "$a \sim b$ if and only if a and b are in the same orbit under the action of H".

[2] *Hint*. Every element of G can be written in the form $x^{-1}\sigma(x)$. Apply σ to such an expression.

[3] For each $x \in A$ the equivalence class of x under $\sim$ is called the *orbit* of x under the action of H. The orbits under the action of H partition the set A.

- (Reflexivity) We have $a = 1 \cdot a$, so $a \sim a$.
- (Symmetry) We have $a \sim b$ if and only if there's an $h \in H$ such that $a = h \cdot b$. Suppose it is so. Then there's an $h^{-1} \in H$ such that $h^{-1} \cdot a = h^{-1} \cdot (h \cdot b) = (h^{-1}h) \cdot b = b$, implying $b \sim a$.
- (Transitivity) Suppose $a \sim b$ and $b \sim c$. So there are $g, h \in H$ such that $a = hb$ and $b = gc$. H is closed, so $a = hgc$, hence $a \sim c$.

We've shown that the relation "in the same orbit under the action of H" is an equivalence relation, and so gives rise to a partition of A into orbits under H. □

1.12. **Lagrange's theorem [1, No. 1.7.19].** Let H be a subgroup of the finite group G and let H act on G by left multiplication. Let $x \in G$ and let $\mathscr{O}$ be the orbit of x under the action of H. Then the map

$$H \to \mathscr{O} \text{ defined by } h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$).

Proof. The map $H \to \mathscr{O}$ is surjective (by definition of the equivalence classes) and injective as if $h \cdot x = g \cdot x$, then

$$(h^{-1}g) \cdot x = h^{-1} \cdot (g \cdot x) = h^{-1} \cdot (h \cdot x) = (h^{-1}h) \cdot x = 1 \cdot x = x,$$

so $h^{-1}g = 1$, hence $g = h$.

Now we state as a theorem, *if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.*

Proof. Having a bijection from a subgroup H to each orbit $\mathscr{O}$ under the action of H, we assert $|H| = |\mathscr{O}|$. Now since G (is finite) and is partitioned by finitely many orbits, we must have that $n\,|H| = n\,|\mathscr{O}| = |G|$. This implies that the order of a subgroup $|H|$ divides the order of the group $|G|$. □

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`