7210 HW 1

Duncan Wilkie

30 August 2022

1.1.25. *If $x^2 = 1$ for all $x \in G$, then G is Abelian.*

Proof. Let $a, b \in G$ be arbitrary. First note that by associativity and the $x^2 = 1$ property $abba = a(bb)a = aa = 1$. We may insert this form of the identity to obtain

$$ab = ab(abba) = (abab)ba = (ab)^2 ba = ba$$

The group is therefore Abelian. □

1.1.31. *Any finite group G of even order contains an element of order 2.*

Proof. Let $t(G) = \{g \in G | g \neq g^{-1}\}$. One may construct a pairing of $t(G)$ by binning g alongside its unique and distinct inverse g^{-1} until all elements are exhausted, so $t(G)$ has an even number of elements. There necessarily exists an element of G that's not in $t(G)$: the identity is its own inverse, so $|t(G)| < |G|$. Since $|G|$ and $|t(G)|$ are even, $|G - t(G)|$ is also even, and since it's nonzero must be at least 2, i.e. there is a non-identity element of G that is self-inverse. Any non-identity, self-inverse element a of a group has order 2, since $a \neq 1 \Rightarrow |a| > 1$ and $a = a^{-1} \Rightarrow a^2 = aa = aa^{-1} = 1 \Rightarrow |a| \leq 2$, implying $|a| = 2$. □

1.2.4. *If $n = 2k$ is even and $n \geq 4$, then $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Also, z is the only nonidentity element which commutes with all elements of D_{2n}.*

Proof. First, z is indeed of order 2: $(r^k)^2 = r^{2k} = r^n = 1$ by the presentation of r. It certainly commutes with other rotations, by induction. The base case follows from associativity,

$$r \cdot r^k = r \cdot (\underbrace{r \cdots r}_{\text{k times}}) = (\overbrace{r \cdots r}^{\text{k times}}) \cdot r = r^k \cdot r,$$

and the inductive step is identical: letting $0 \leq i \leq n - 1$,

$$r^i \cdot r^k = r^{i-1}(r \cdot r^k) \overset{\text{b.c.}}{=} r^{i-1} r^k r \overset{\text{i.h.}}{=} r^k r^{i-1} r = r^k r^i$$

It also commutes with reflection, morally because "it's half a full rotation." We have from the presentation that $sr = r^{-1}s$, which by induction implies $sr^k = r^{-k}s$:

$$sr^{k+1} = sr^k r \overset{\text{i.h.}}{=} r^{-k} sr \overset{\text{b.c.}}{=} r^{-k-1} s$$

Additionally, $r^k = r^{-k}$, since this is equivalent to $r^{2k} = r^n = 1$, which holds from the presentation. Therefore, $sr^k = r^k s$, i.e. r^k commutes with s. This implies r^k also commutes with sr^i, since $sr^i r^k = sr^k r^i = r^k sr^i$, so r^k commutes with all of D_{2n}.

We now demonstrate that every element other than z doesn't commute with at least one other element. If an element is a pure rotation, represented with no reflections, it usually doesn't commute with s: it is of the form r^i for $0 \leq i \leq n-1$, and $sr^i = r^{-i}s$ shows it doesn't commute *unless* $r^i = r^{-i}$. If an element *is* represented with a reflection, then it usually doesn't commute with r: letting $0 \leq i \leq n-1$,

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

shows it doesn't commute *unless* $r = r^{-1}$.

The first special condition multiplied on both sides by r^i yields $r^{2i} = 1$. This means $r^{2i} = r^{a \cdot n}$ for some a, implying $i = a \cdot n/2$. However, $0 \leq i \leq n-1$, so $a = 0$ or 1, as even $a = 2$ would mean $i = n$, which is too large. We're looking for non-identity elements, so $i = n/2$, and since exponents must be integral n is even, i.e. r^k for even $n = 2k$ is the only pure reflection that can possibly commute with s.

The second condition means the above argument doesn't work if $n = 2$, as in that case there is only one rotation, so $r = r^{-1}$, and $sr = r^{-1}s = rs$. However, for $n > 2$, $r \neq r^{-1}$ because two rotations of less than π radians don't add up to 2π, meaning $r^2 = 1 \Leftrightarrow r = r^{-1}$ doesn't hold, i.e. sr^i can only ever commute with r if $n \leq 2$, which we explicitly exclude. □

1.1.5. *If n is odd and $n > 3$, the identity is the only element of D_{2n} that commutes with all other elements.*

Proof. The second part of our proof above directly translates, as nothing depends on n's being even. We showed that all pure rotations r^i for $0 \leq i \leq n-1$ that don't satisfy $r^i = r^{-i}$ don't commute with at least s, and all non-pure-rotation elements of D_{2n} don't commute with at least r, so long as $r \neq r^{-1}$.

The former special condition never holds for odd $n \geq 3$, as that would require $r^{2i} = 1 \Rightarrow r^{2i} = r^{a \cdot n}$ for some natural a. Like above, $0 \leq i \leq n-1$ implies $a = 0$ or $a = 1$; the former would imply r^{2i} is the identity and the latter that n is even.

We also argued above $r = r^{-1}$ doesn't hold for $n > 2$. □

Lemma 1. *The k-fold composition of a cycle of order n with itself is the identity permutation iff $n \mid k$.*

Proof. Denote the general cycle by $\sigma = (a \ \cdots \ a_i \ \cdots \ a_n)$. Cycle notation has by definition that $\sigma(a_i) = a_{i+1 \pmod{n}}$. By induction on j from this base case, $\sigma^j(a_i) = a_{i+j \pmod{n}}$:

$$\sigma^{j+1}(a_i) = \sigma \circ \sigma^j(a_i) \overset{\text{i.h.}}{=} \sigma \circ a_{i+j \pmod{n}} \overset{\text{b.c.}}{=} a_{i+j+1 \pmod{n}}$$

Therefore, k for which $\sigma^k = 1$ (equiv. $k \mid \forall i, \sigma^k(a_i) = a_{i+k \pmod{n}} = a_i$) are precisely those k such that $k \equiv 0 \pmod{n}$, equiv. $n \mid k$.

Notice that this last argument depends on the injectivity of the function a_i implied by uniqueness of integers in a cycle in order to say that $a_l = a_m$ iff $l = m$. □

Lemma 2. *The composition of disjoint, nonidentity permutations is a nonidentity permutation.*

Proof. "Disjoint" is a property of two permutations (not necessarily cycles) $\sigma, \tau : S \to S$: letting $\operatorname{supp} \mu = \{x \in S \mid \mu(x) \neq x\}$ for any μ, σ and τ are *disjoint* if $\operatorname{supp} \sigma \cap \operatorname{supp} \tau = \emptyset$.

If $\sigma \neq 1$, then there exists a s.t. $\sigma(a) = b \neq a$. This implies $a \in \operatorname{supp} \sigma$. Since σ and τ are disjoint, $a \notin \operatorname{supp} \tau$, i.e. $\tau(b) = b$. If $\tau \circ \sigma = 1$, then $\tau(b) = a$ so that $\tau \circ \sigma(a) = a$. This is a contradiction, so $\tau \circ \sigma \neq 1$. □

Lemma 3. *Disjoint cycles of a cycle decomposition represent disjoint permutations.*

Proof. Disjoint cycles don't have any numbers in common, i.e. one cycle has the action of the identity on any element appearing the other, and is excluded from the other's permutation's disjointness set by definition. □

Lemma 4. *The support set and therefore disjointness are preserved under composition powers of permutations.*

Proof. Precisely, we intend to prove that $a \in \operatorname{supp} \sigma^n$ iff $a \in \operatorname{supp} \sigma$ and consequently that if two permutations σ, τ are disjoint, then arbitrary powers of each permutation are disjoint permutations. If $a \notin \operatorname{supp} \sigma$, then $\sigma(a) = a$, so $\sigma^n(a) = a$, implying $a \notin \operatorname{supp} \sigma^n$. Conversely, suppose for induction that $a \notin \operatorname{supp} \sigma^n$ implies $a \notin \operatorname{supp} \sigma$ (the case $n = 1$ is reflexive);

$$a \notin \operatorname{supp} \sigma^{n+1} \Leftrightarrow \sigma^{n+1}(a) = a \Leftrightarrow \sigma^n(a) = \sigma^{-1}(a) \overset{\text{i.h.}}{\Leftrightarrow} a = \sigma^{-1}(a) \Leftrightarrow \sigma(a) = a.$$

This proves $\operatorname{supp} \sigma = \operatorname{supp} \sigma^n$ for arbitrary n.

Since we have proven $\operatorname{supp} \sigma^n = \operatorname{supp} \sigma$ and $\operatorname{supp} \tau^k = \operatorname{supp} \tau$, and $\operatorname{supp} \sigma$ and $\operatorname{supp} \tau$ are disjoint by assumption, $\operatorname{supp} \sigma^n$ and $\operatorname{supp} \sigma^k$ are disjoint, so σ^n and σ^k are disjoint. □

Lemma 5. *Disjoint permutations commute.*

Proof. Take general disjoint $\sigma, \tau \in S_n$ and a general $1 \leq a \leq n$. If $a \in \operatorname{supp} \sigma$, then $\tau(a) = a$, so $\sigma(\tau(a)) = \sigma(a)$. By Lemma 4, $\operatorname{supp} \sigma$ is invariant under σ; in particular, $\sigma(a) \in \operatorname{supp} \sigma$. Since σ and τ are disjoint, $\sigma(a) \notin \operatorname{supp} \tau$, so $\tau(\sigma(a)) = \sigma(a)$. In particular, this shows $\sigma\tau(a) = \tau\sigma(a)$ in this case.

If $a \notin \operatorname{supp} \sigma$, then $\sigma(a) = a$, so $\tau(\sigma(a)) = \tau(a)$. Since $\operatorname{supp} \tau$ is invariant under τ, and $\operatorname{supp} \tau$ and $\operatorname{supp} \sigma$ are disjoint, $\tau(a) \in \operatorname{supp} \tau \Rightarrow \tau(a) \notin \operatorname{supp} \sigma$, so $\sigma(\tau(a)) = \tau(a)$. □

Lemma 6. *If any $a, b \in G$ commute, then $(ab)^n = a^n b^n$; in particular, this holds for cycles in a cycle decomposition.*

Proof. First, we show that $b^n a = ab^n$ inductively. $n = 1$ is immediate, so suppose the property holds for n. Then

$$b^{n+1}a = b^n ba = b^n ab \overset{\text{i.h.}}{=} ab^n b = ab^{n+1}$$

Doing another induction, the base case reduces to commutativity again. Suppose the main result holds for n. Then

$$(ab)^{n+1} = (ab)^n(ab) \overset{\text{i.h.}}{=} a^n b^n ab = a^n ab^n b = a^{n+1}b^{n+1}$$

This holds for cycles in a cycle decomposition because such cycles commute by Lemmas 3 and 5. □

1.3.14. *Let p be a prime. An element σ has order p in S_n iff its cycle decomposition is a product of commuting p-cycles. There exist composite numbers for which this doesn't hold.*

Proof. First, the forward implication. Since the p-cycles in the decomposition of σ are disjoint by Lemma 3, Lemma 6 implies σ^p is the composition of the pth power of p-cycles. By Lemma 1, each cycle is then the identity, since $p \mid p$, so $\sigma^p = 1$.

Conversely, if σ merely has order p, it still has a decomposition into disjoint (and therefore commuting) cycles, some of which may be p-cycles, and some of which may not be. Suppose there are some cycles in this decomposition that aren't p-cycles. Lemma 6 lets one distribute the exponent in σ^p. Those non-p-cycles when taken to the pth power aren't the identity by Lemma 1, as they're either of length less than p or greater than p; primality of p implies $n \nmid p$ in the first case and $n \nmid p$ if $n > p$ is an elementary arithmetic result resolving the second. Since the initial cycles are disjoint by Lemma 3, their pth powers are disjoint by Lemma 4. Since the pth power of the p-cycles is the identity, the composition of those disjoint nonidentity pth powers is σ^p, which by Lemma 2 can't be the identity permutation. This proves the contrapositive of the reverse implication.

Obviously, if p is composite the application of Lemma 1 in the proof of the reverse implication is unsound, and there exists no proof without this defect, as demonstrated by the following example:

$$\sigma = (1\ 2)(3\ 4\ 5) \in S_n,$$

$$\sigma^6 = (1\ 2)^6(3\ 4\ 5)^6 = (1)(2)(3)(4)(5) = 1 \Rightarrow |\sigma| \leq 6.$$

In fact $|\sigma| = 6$, since $\sigma \neq 1$, $\sigma^2 : 3 \mapsto 5$, $\sigma^3 : 1 \mapsto 2$, $\sigma^4 : 3 \mapsto 4$, and $\sigma^5 : 1 \mapsto 2$. Since the definition of σ is a cycle decomposition that is a product of a 2- and a 3-cycle, not 6-cycles, this is a counterexample to the composite case. □

1.1.15. *For all $\sigma \in S_n$, $|\sigma|$ is the least common multiple l of the lengths of the cycles in its cycle decomposition.*

Proof. First, we prove that $|\sigma| \leq l$. Write

$$\sigma = (a_1\ \cdots\ a_{m_1}) \cdots (a_{m_{k-1}+1}\ \cdots\ a_{m_k});$$

by Lemma 6,

$$\sigma^k = (a_1\ \cdots\ a_{m_1})^l \cdots (a_{m_{k-1}+1}\ \cdots\ a_{m_k})^l.$$

Since $m_i \mid l$ for all $1 \leq i \leq k$ by definition of l, by Lemma 1 each element of this product is the identity, so $\sigma^l = 1$.

Next, we prove that all $l' < l$ can't be $|\sigma|$. Since l is the *least* common multiple of the lengths of the cycles in the decomposition, no number less than l can be a multiple of every cycle length, and by Lemma 1 this implies there is at least one cycle that isn't the identity. Since the cycles are disjoint by Lemma 3, this implies by Lemma 2 that $\sigma^{l'} \neq 1$. □

1.1.7. *If p is prime, $|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p$.*

Proof. Elements of $GL_2(\mathbb{F}_p)$ look like

$$\begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}$$

Such matrices fail to be in $GL_2(\mathbb{F}_p)$ iff $cf_1 = f_3$ and $cf_2 = f_4$ for some $c \in \mathbb{F}_p$. If $f_1 = f_2 = 0$, then the matrix isn't invertible since its determinant $f_1 f_4 - f_2 f_3$ has a factor of 0 in each addend. So there are $p^2 - 1$ possible choices for f_1 and f_2 if the matrix is to be invertible: p for f_1 and p for f_2, except for the one where both are zero. There are then p^2 values one can put in the pair (f_3, f_4), but p and only p of those choices make the matrix singular. Once f_1 and f_2 are fixed, every c determines exactly one non-invertible matrix with $f_3 = cf_1$ and $f_4 = cf_2$, and every non-invertible matrix with one of $f_1, f_2 \neq 0$ is of this form, since the result is an equivalence. There are then $p^2 - p$ further choices that keep the matrix invertible after choosing f_1 and f_2.

This completely considers all possible choices of $f_1, f_2, f_3, f_4 \in \mathbb{F}_p$, so

$$|GL_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p) = p^4 - p^3 - p^2 + p$$

□