Math 120 Homework 3 Solutions

Xiaoyu He, with edits by Prof. Church

April 21, 2018

[Note from Prof. Church: solutions to starred problems may not include all details or all portions of the question.]

1.3.1*

Let σ be the permutation $1 \mapsto 3, 2 \mapsto 4, 3 \mapsto 5, 4 \mapsto 2, 5 \mapsto 1$ and let τ be the permutation $1 \mapsto 5, 2 \mapsto 3, 3 \mapsto 2, 4 \mapsto 4, 5 \mapsto 1$. Find the cycle decompositions of each of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \tau^2\sigma$.

The cycle decompositions are:

$$\begin{aligned} \sigma &= (135)(24) \\ \tau &= (15)(23)(4) \\ \sigma^2 &= (153)(2)(4) \\ \sigma\tau &= (1)(2534) \\ \tau\sigma &= (1243)(5) \\ \tau^2\sigma &= (135)(24). \end{aligned}$$

1.3.7*

Write out the cycle decomposition of each element of order 2 in S_4.

Elements of order 2 are also called involutions. There are six formed from a single transposition, $(12), (13), (14), (23), (24), (34)$, and three from pairs of transpositions: $(12)(34), (13)(24), (14)(23)$.

3.1.6*

Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

The fibers of φ are $\varphi^{-1}(1) = (0, \infty) = \{\text{all positive reals}\}$ and $\varphi^{-1}(-1) = (-\infty, 0) = \{\text{all negative reals}\}$.

3.1.7*

Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.

The map π is surjective because e.g. $\pi((x, 0)) = x$. The kernel of π is the line $y = -x$ through the origin. The fibers of π are all the lines $y = -x + c$ of slope -1.

3.1.8*

Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ.

The image of φ is the set of positive reals $(0, \infty)$. The kernel of φ is $\{\pm 1\}$. The fiber of φ over a point $x \in (0, \infty)$ is the two-element set $\{\pm x\}$. The fibers over the negative reals are empty.

3.1.9*

Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and fibers of φ geometrically (as subsets of the plane).

The image of φ is the set of positive reals $(0, \infty)$. The kernel is the unit circle $\{z \in \mathbb{C} | \ z| = 1\}$. The fibers are circles centered at the origin; if $x > 0$ then $\varphi^{-1}(x)$ is the circle $\{z \in \mathbb{C} || z| = x\}$ of radius x.

3.1.41

Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy | x, y \in G\rangle$ is a normal subgroup of G and G/N is abelian (N is called the *commutator subgroup of* G).

For a subgroup N to be normal means that $gNg^{-1} = N$ for all $g \in G$. We first prove a lemma: actually, it suffices to show that $gNg^{-1} \subseteq N$ for all $g \in G$. Why? Suppose we have proved this for all elements g. So for a given $x \in G$, we know both $xNx^{-1} \subseteq N$ *and* $x^{-1}Nx \subseteq N$. Multiplying the second equation by x on the left and by x^{-1} on the right, it becomes $N \subseteq xNx^{-1}$. Combining this with the first equation shows that $xNx^{-1} \subseteq N \subseteq xNx^{-1}$, so $xNx^{-1} = N$ as desired.

For readability, let's introduce the notation $[x, y] = x^{-1}y^{-1}xy$. This is called the *commutator* of x and y.

We need to check that $gNg^{-1} \subseteq N$ for all $g \in G$. Let $h \in N$. Then,

$$\begin{aligned} ghg^{-1} &= ghg^{-1} \cdot 1 \\ &= ghg^{-1}(h^{-1}h) \\ &= ghg^{-1}h^{-1}h \\ &= (ghg^{-1}h^{-1})h, \end{aligned}$$

which we recognize as the product $[g^{-1}, h^{-1}]h$ of a commutator $[g^{-1}, h^{-1}]$ and the element h. Since N is the subgroup generated by commutators of G, we know that $[g^{-1}, h^{-1}] \in N$ by definition; and $h \in N$ by assumption. Since N is a subgroup, their product ghg^{-1} must therefore lie in N as well. This concludes the proof that $gNg^{-1} \subseteq N$ for any $g \in G$, as desired. This shows N is a normal subgroup of G.

To see that G/N is abelian, we need to check that $(gN)(hN) = (hN)(gN)$ for any two cosets gN and hN of N. Since coset multiplication is given by multiplication of their representatives, we want $ghN = hgN$. But the commutator $[h, g] = h^{-1}g^{-1}hg$ lies in N, so $ghN = gh(h^{-1}g^{-1}hg)N = hgN$, as desired.

Question 1

Let $T \subset S_n$ be the *set* of transpositions. (A transposition is a permutation of the form $(i\ j)$, which swaps two elements and fixes all others. Note that $|T| = \binom{n}{2}$.)

Prove that the symmetric group S_n is generated by T.

As in class, write $(a_1a_2 \dots a_\ell)$ for the permutation with a single nontrivial cycle which sends $a_i \mapsto a_{i+1}$for $1 \leq i < \ell$, sends $a_\ell \mapsto a_1$, and fixes all the other elements of $[n]$. Since every permutation has a cycle decomposition, the set C of all such permutations $(a_1 \dots a_\ell)$ certainly generate S_n. So it suffices to show that every element of C is a product of transpositions. [Note: Think about why this suffices, if you don't understand why.]

In fact, we can explicitly check that $(a_1a_2 \dots a_\ell) = (a_1a_2)(a_2a_3) \cdots (a_{\ell-1}a_\ell)$. Thus, T generates S_n.

Question 2

Let G be a finite group of order $|G| = n$. Prove that there exists a subgroup H of S_n which is isomorphic to G.

Informally, each element $g \in G$ acts by left-multiplication on the set of all other elements of G, permuting them. Here's how to make this explicit.

Instead of constructing a subgroup H of S_n, it's more natural to construct a subgroup H' of $\mathrm{Perm}(G)$. Since $|G| = n$, we know that $\mathrm{Perm}(G)$ is isomorphic to S_n [there is an isomorphism for every bijection $G \to \{1, \ldots, n\}$], and under this isomorphism the subgroup $H' < \mathrm{Perm}(G)$ corresponds to an isomorphic subgroup $H < S_n$. [After constructing the subgroup H', we'll also show how you could directly construct H, if you wanted to.]

Construction of $H' < \mathrm{Perm}(G)$ We construct a function $\alpha \colon G \to \mathrm{Perm}(G)$ as follows. Given $g \in G$, the permutation $\alpha_g \in \mathrm{Perm}(G)$ is defined by $\alpha_g(k) = gk$ for $k \in G$. We must first show that α_g really is a permutation. We also want to show that α is a homomorphism and is injective.

It turns out to be easier to start with the second point, by noting that $\alpha_g \circ \alpha_h = \alpha_{gh}$. We can verify this simply by checking on elements:

$$\text{for any } k \in G, \quad \alpha_g \circ \alpha_h(k) = \alpha_g(\alpha_h(k)) = \alpha_g(hk) = g(hk) = (gh)k = \alpha_{gh}(k)$$

We can now also check that α_g is indeed a permutation. Note that α_1 is the identity permutation (since $\alpha_1(k) = 1 \cdot k = k$ for all k). Therefore taking $h = g^{-1}$ in $\alpha_g \circ \alpha_h = \alpha_{gh}$ tells us that $\alpha_g \circ \alpha_{g^{-1}} = \alpha_{gg^{-1}} = \alpha_1 = \mathrm{id}$. Therefore α_g is an invertible function on a finite set, and thus is a bijection $\alpha_g \in \mathrm{Perm}(G)$.

Finally, we must check that α is injective. Suppose that α_g and α_h are the same function. In particular, their values on the element $1 \in G$ are equal. But by definition $\alpha_g(1) = g \cdot 1 = g$ and $\alpha_h(1) = h \cdot 1 = h$, so this means $g = h$. This proves that α is injective.

Let $H' = \mathrm{im}\alpha < \mathrm{Perm}(G)$. Since α is an injective homomorphism, it is a bijection to its image H', so α is an isomorphism between G and H'.

Direct construction of $H < S_n$ (Alternate approach) Number the elements of G arbitrarily: $g_1, \ldots, g_n$. Define the function $f : [n]^2 \to [n]$ as $f(i, j) = k$ iff $g_i g_j = g_k$. Then, define the map $\varphi : G \to S_n$ by $\varphi(g_i)(j) = f(i, j)$. That is, $\varphi(g_i)$ is the permutation of $[n]$ which sends j to $f(i, j)$. [We must again check here that $\phi(g_i)$ is a permutation.] We claim that φ is an injective homomorphism.

To show that φ is a homomorphism, note that $g_i g_j g_k = g_i g_{f(j,k)} = g_{f(i,f(j,k))}$ by the definition of f. Thus, $\varphi(g_i g_j)$ is the permutation which sends $k \mapsto f(i, f(j, k))$. On the other hand, group multiplication in S_n is just composition, so $\varphi(g_i)\varphi(g_j)$ is also the permutation which sends $k \mapsto f(j, k) \mapsto f(i, f(j, k))$. This shows φ is a homomorphism.

To show that φ is injective, suppose without loss of generality that g_1 is the identity of G. Then, $g_i g_1 = g_i$, so $f(i, 1) = i$ for all i. Thus, $\varphi(g_i)$ is a permutation which sends $1 \mapsto i$, and so each g_i is sent to a different permutation.

Let $H = \mathrm{im}\varphi$. Since φ is an injective homomorphism, it is a bijection to its image H, so φ is an isomorphism between G and H.

Question 3

Recall that a group G is finitely generated if there exists a finite subset $T \subset G$ such that $G = \langle T \rangle$.

(a*) Prove that every finite group is finitely generated.

Take $T = G$.

(b*) Prove that $\mathbb{Z}$ is finitely generated.

Take $T = \{1\}$.

(c) Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.

Lemma 1. *Given two elements $a, b \in \mathbb{Z}$, the subgroup generated by a and b can be generated by a single element x*

Proof. In fact, that single element will be the gcd of a and b. Let $x = \gcd(a, b)$.

Since x is a divisor of a, we know that $a \in \langle x \rangle$; similarly, since x is a divisor of b, we know that $b \in \langle x \rangle$. Since $\langle a, b \rangle$ is defined as the smallest subgroup containing both a and b, this tells us that $\langle a, b \rangle \subseteq \langle x \rangle$. (So far we have only used that x is a *common* divisor of a and b, not that it is the *greatest* common divisor.)

Now let us use that x is actually the gcd of a and b. By the Euclidean algorithm, there exists $c, d \in \mathbb{Z}$ for which $ac + bd = \gcd(a, b) = x$. This implies that x is contained in the subgroup generated by a and b.[1] So $x \in \langle a, b \rangle$, and thus $\langle x \rangle \subseteq \langle a, b \rangle$. In light of the above, this shows that $\langle a, b \rangle = \langle x \rangle$, proving the lemma. □

Lemma 2. *Every finitely generated subgroup of $\mathbb{Z}$ is cyclic.*

Proof. Let H be a finitely generated subgroup of $\mathbb{Z}$, and let $n \geq 1$ be the minimum positive integer for which H has a generating set T of size n.

Suppose for the sake of contradiction that H is not cyclic, i.e. that $n \geq 2$. We may therefore choose two elements $a, b \in \mathbb{Z}$ of T. But Lemma 1 tells us that we can replace a and b in T by a single generator $x = \gcd(a, b)$ and still generate H. This gives a generating set for H of size $n-1$, contradicting the minimality of n. This contradiction implies that H must have been cyclic. □

Given $D \neq 0 \in \mathbb{N}$, let $\frac{1}{D}\mathbb{Z}$ denote the subgroup of $\mathbb{Q}$ consisting of elements that can be written as $\frac{n}{D}$ for some $n \in \mathbb{Z}$. Note that $\frac{1}{D}\mathbb{Z}$ is isomorphic to $\mathbb{Z}$ under the isomorphism $\frac{1}{D}\mathbb{Z} \ni \frac{n}{D} \leftrightarrow n \in \mathbb{Z}$.

Now, let H be a subgroup of $\mathbb{Q}$ generated by a finite set $T = \{\frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}\}$. Let $D = \operatorname{lcm}(q_1, \ldots, q_k)$ be the lcm of all the denominators of elements of T (or if we want to be lazier, we could just take $D = q_1 \cdots q_k$). In either case, we see that $\frac{p_i}{q_i} \in \frac{1}{D}\mathbb{Z}$ for all i.

Since $\frac{1}{D}\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ and every element of T lies in it, $H = \langle T \rangle$ is a subgroup of $\frac{1}{D}\mathbb{Z}$. But $\frac{1}{D}\mathbb{Z}$ is isomorphic to $\mathbb{Z}$ as a group, so by Lemma 2 every finitely generated subgroup thereof is cyclic. Thus, H is cyclic.

(d) Prove that $\mathbb{Q}$ is not finitely generated.

One way to see this is that any finite set T of rational numbers has a common denominator D, so that $\langle T \rangle \subseteq \frac{1}{D}\mathbb{Z}$. Thus no finite set of generators can generate the whole group of rational numbers additively.

Another way to see this is to use part (c). If $\mathbb{Q}$ is finitely generated, then it would be a finitely generated subgroup of itself, so by part (c) $\mathbb{Q}$ would have to be cyclic. Suppose for a contradiction that $x \in \mathbb{Q}$ is a purported generator of $\mathbb{Q}$. Then $y = \frac{1}{2}x$ cannot be obtained from x by addition/subtraction, so $y \notin \langle x \rangle$. This contradiction shows that $\mathbb{Q}$ is not cyclic.

Question 4

Let G be a finite group of order $|G| = n$, and suppose that p is a prime number dividing n. In this question you will prove that G has an element z of order $|z| = p$. Let

$$S = \{(g_1, \ldots, g_p) | g_1 \cdot g_2 \cdots g_p = 1\}$$

be the set of p-tuples of group elements whose product is equal to 1.

(a) Show that $|S| = |G|^{p-1}$. (Since $|G|$ is divisible by p by assumption, (a) implies that $|S|$ is divisible by p.)

Let

$$S' = G^{p-1}$$

be the set of all $(p-1)$-tuples of elements of G. We claim that the map $S \to S'$ which sends $(g_1, \ldots, g_p) \mapsto (g_1, \ldots, g_{p-1})$ by dropping the last coordinate is a bijection.

It is a surjection because for every $(g_1, \ldots, g_{p-1}) \in S'$, we can exhibit the tuple $(g_1, \ldots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}) \in G$ which maps to it. It is an injection because if two p-tuples in S have the first same $p-1$ coordinates $(g_1, \ldots, g_{p-1})$, then the last coordinate is uniquely determined by $g_1 \cdot g_2 \cdots g_p = 1$ to be $g_p = (g_1 \cdots g_{p-1})^{-1}$, so the two p-tuples must be identical.

Thus $|S| = |S'| = |G|^{p-1}$.

[1] If this confuses you, imagine we were writing the group operation multiplicatively: then the equation $ac + bd = x$ would instead be written in the form $\alpha^c \beta^d = \xi$.

Consider the equivalence relation on S defined by $\alpha \sim \beta$ if β is obtained by "rotating" α; in other words, for some k, $\alpha = (x_1, \ldots, x_p)$ and $\beta = (x_k, x_{k+1}, \ldots, x_p, x_1, \ldots, x_{k-1})$.

(b*) Convince yourself that this is an equivalence relation.

(c) Prove that every equivalence class has size 1 or p (using that p is a prime). Conclude that $|S| = a + pb$, where a is the number of classes of size 1 and b is the number of classes of size p.

First, note that if $\alpha \in S$ then any rotation of α is also in S. For example, suppose $x_1 x_2 \cdots x_p = 1$. Then, multiplying on the left by x_1^{-1} and on the right by x_1 (this is called conjugation by x_1^{-1}) gives

$$\begin{aligned} x_1^{-1} x_1 x_2 \cdots x_p x_1 &= x_1^{-1} x_1 \\ x_2 \cdots x_p x_1 &= 1. \end{aligned}$$

Repeating this conjugation process, we see that if a product of elements in a group is 1, then any rotation also has product 1.

So we may simply prove the same statement about equivalence classes of p-tuples in the larger set G^p containing S.

Suppose $\alpha = (x_1, \ldots, x_p)$. We will show that either all p rotations of α are different, in which case the equivalence class of α has size p, or they are all the same, in which case the equivalence class has size 1. If $x_1 = x_2 = \cdots = x_p$, then all rotations of α are the same, so the equivalence class containing α has size 1.

Otherwise, suppose α is not constant, i.e. there exist some $x_i \neq x_j$. We claim that all p rotations of α are different tuples.

If not, there are two rotations $(x_k, x_{k+1}, \ldots, x_p, x_1, \ldots, x_{k-1})$ and $(x_\ell, x_{\ell+1}, \ldots, x_p, x_1, \ldots, x_{\ell-1})$ which are the same p-tuple. This implies that $x_i = x_{i+\ell-k}$ for all i, where addition of indices is taken $\mod p$. But then,

$$\begin{aligned} x_1 &= x_{1+\ell-k} \\ &= x_{1+2(\ell-k)} \\ &= x_{1+m(\ell-k)} \end{aligned}$$

for all m. It is easy to check that if $\ell - k \not\equiv 0 \pmod p$, then the multiples of $\ell - k$ cycle through all residue classes mod p (this is a consequence of $\mathbb{Z}/p\mathbb{Z}^\times$ being a group, for example). Thus, for all $i \in [p]$, there exists m for which $1 + m(\ell - k) = i$, and so $x_1 = x_i$ for all i. This contradicts the fact that α is not constant. What we have shown is that any nonconstant α has a full set of p distinct rotations in its equivalence class.

To see that $|S| = a + pb$, divide S into the equivalence classes of size 1 and those of size p. This completely partitions S, so $|S| = a + pb$.

(d) Show that an equivalence class contains a single element if and only if that element is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

We showed in the last part that a singleton equivalence class in G^p must be constant $\alpha = (x, \ldots, x)$. If in addition this element is to lie in S, it must have product 1, i.e. $x^p = 1$. Conversely, any x with $x^p = 1$ gives a singleton equivalence class $(x, x, \ldots, x)$ which lies in S.

(e) Finish the proof (i.e. prove that G contains an element of order p) by showing that there must be at least one class of size 1 besides $(1, 1, \ldots, 1)$, Ã *la* HW1 Q3A.

Since $|S| = |G|^{p-1}$ by part (a), and p divides the order of G, p divides $|S|$. On the other hand, by part (c) $|S| = a + pb$ where a is the number of equivalence classes of size 1 and b is the number of equivalence classes of size p. Thus $p | a + pb$, which implies $p | a$. In particular, since all primes satisfy $p \geq 2$, there must be at least two classes of size 1, and therefore at least one such class $\alpha = (x, \ldots, x)$ with $x^p = 1$ and $x \neq 1$. This shows the existence of an element x of order exactly p, as desired.

Question 5

Notation: For any groups H and G, write $n(H, G)$ for the number of homomorphisms from H to G.

Say you are given two groups A and B. Your goal is to find a new group C with the new property (*) that for every group H,

$$n(H, C) = n(H, A) \cdot n(H, B).$$

Construct such a group C (it will depends on the groups A and B you are given!) and prove it has the property (*).

The group C we define is called the *direct product* (or simply product) of A and B, written $C = A \times B$. The underlying set of C is just the Cartesian product $\{(a, b) : a \in A, b \in B\}$ of A and B as sets, and the group operation of C is given by coordinate-wise multiplication. Explicitly, if $\cdot_A$, $\cdot_B$ are the group operations of A, B, then the group operation $\cdot_C$ on $C = A \times B$ is given by

$$(a_1, b_1) \cdot_C (a_2, b_2) = (a_1 \cdot_A a_2, b_1 \cdot_B b_2).$$

It is easy to check that C is also a group.

Write $\mathrm{Hom}(G, H)$ for the set of homomorphisms from G to H. Thus, $n(G, H) = |\mathrm{Hom}(G, H)|$.

To prove C has property (*), we construct a bijection φ between $\mathrm{Hom}(H, C)$ and the product set $\mathrm{Hom}(H, A) \times \mathrm{Hom}(H, B)$. To construct this bijection, define two projection homomorphisms $\pi_A : C \to A$ and $\pi_B : C \to B$ by $\pi_A((a, b)) = a$ and $\pi_B((a, b)) = b$. Thus π_A projects to the first coordinate and π_B to the second. Then, if $f \in \mathrm{Hom}(H, C)$, define $\varphi(f) = (\pi_A \circ f, \pi_B \circ f)$. Notice that compositions of homomorphisms are homomorphisms, so $\pi_A \circ f$ is a homomorphism $H \to A$ and $\pi_B \circ f$ is a homomorphism $H \to B$, as we wanted.

To prove that φ is a bijection, we can just construct a two-sided inverse for it.

In the other direction, if $(f_A, f_B) \in \mathrm{Hom}(H, A) \times \mathrm{Hom}(H, B)$, then define $\psi((f_A, f_B))$ to be the "product homomorphism" map $f : H \to C$ which sends $h \in H$ to $(f_A(h), f_B(h))$. It is easy to check that this map f is itself a homomorphism $H \to C$.

Finally, notice that φ and ψ are mutually inverse functions. Given $f \in \mathrm{Hom}(H, C)$, the map $\psi(\varphi(f))$ sends $h \in H$ to $(\pi_A(f(h)), \pi_B(f(h)))$, which is just $f(h)$, so $\psi(\varphi(f)) = f$ for all $f \in \mathrm{Hom}(H, C)$, and ψ is a left-inverse for φ.

Similarly, given $(f_A, f_B) \in \mathrm{Hom}(H, A) \times \mathrm{Hom}(H, B)$, the ordered pair $\varphi(\psi(f_A, f_B))$ is the pair of functions $(h \mapsto \pi_A(f(h)), h \mapsto \pi_B(f(h)))$, where $f(h) = (f_A(h), f_B(h))$. But then $\pi_A(f(h)) = f_A(h)$ and $\pi_B(f(h)) = f_B(h)$, and so $\varphi(\psi(f_A, f_B)) = (f_A, f_B)$. Thus ψ is a two-sided inverse for φ, showing that φ is a bijection. The existence of this bijection then proves that

$$\begin{aligned} |\mathrm{Hom}(H, C)| &= |\mathrm{Hom}(H, A) \times \mathrm{Hom}(H, B)| \\ n(H, C) &= n(H, A) \cdot n(H, B), \end{aligned}$$

where C is the product group $A \times B$.