Math 120: Homework 2 Solutions

- Section 1.2 # 9,
- Section 1.3 # 2 ($\sigma, \tau, \sigma\tau, \tau\sigma$ only), 5,13,20,
- Section 1.4 # 7,
- Section 1.5 # 2,
- Section 1.6 # 1.

Problem 1.2 # 9. Let G be the group of rigid motions of the tetrahedron. Show that $|G| = 12$.

Solution. Let us label the vertices of the tetrahedron $1, 2, 3, 4$. We enumerate the elements γ of G as follows. Let $\gamma(1) = x$, where $x \in \{1, 2, 3, 4\}$. Now with x fixed, let us count the number of possibilities for γ. The element γ is not quite determined by x, since we may replace γ by $\delta\gamma$ where δ is a permutation that fixes x. It is geometrically clear that there are three possibilities for δ, namely it can be a rotation in an angle of $0, \frac{2\pi}{3}$ or $\frac{4\pi}{3}$. Thus there are 4 choices for x, and once x is fixed, there are 3 choices for γ. Hence there are 12 elements of G altogether.

Problem 1.3 # 2. Let σ be the permutation

$$\begin{array}{lllll} 1 \mapsto 13, & 2 \mapsto 2, & 3 \mapsto 15, & 4 \mapsto 14, & 5 \mapsto 10, \\ 6 \mapsto 6, & 7 \mapsto 12, & 8 \mapsto 3, & 9 \mapsto 4, & 10 \mapsto 1, \\ 11 \mapsto 7, & 12 \mapsto 9, & 13 \mapsto 5, & 14 \mapsto 11, & 15 \mapsto 8. \end{array}$$

and let τ be the permutation

$$\begin{array}{lllll} 1 \mapsto 14, & 2 \mapsto 9, & 3 \mapsto 10, & 4 \mapsto 2, & 5 \mapsto 12, \\ 6 \mapsto 6, & 7 \mapsto 5, & 8 \mapsto 11, & 9 \mapsto 15, & 10 \mapsto 3, \\ 11 \mapsto 8, & 12 \mapsto 7, & 13 \mapsto 4, & 14 \mapsto 1, & 15 \mapsto 13. \end{array}$$

Find the cycle decompositions of the following permutations:

$$\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \tau^2\sigma.$$

Note: I only asked you to do four of these, but the book mentions six. We'll do all of them in this solution.

Problem 1.3 # 2. Let σ be the permutation

$$\begin{array}{lllll} 1 \mapsto 13, & 2 \mapsto 2, & 3 \mapsto 15, & 4 \mapsto 14, & 5 \mapsto 10, \\ 6 \mapsto 6, & 7 \mapsto 12, & 8 \mapsto 3, & 9 \mapsto 4, & 10 \mapsto 1, \\ 11 \mapsto 7, & 12 \mapsto 9, & 13 \mapsto 5, & 14 \mapsto 11, & 15 \mapsto 8. \end{array}$$

and let τ be the permutation

$$\begin{array}{lllll} 1 \mapsto 14, & 2 \mapsto 9, & 3 \mapsto 10, & 4 \mapsto 2, & 5 \mapsto 12, \\ 6 \mapsto 6, & 7 \mapsto 5, & 8 \mapsto 11, & 9 \mapsto 15, & 10 \mapsto 3, \\ 11 \mapsto 8, & 12 \mapsto 7, & 13 \mapsto 4, & 14 \mapsto 1, & 15 \mapsto 13. \end{array}$$

Find the cycle decompositions of the following permutations:

$$\sigma, t, \sigma^2, \sigma\tau, \tau\sigma, \tau^2\sigma.$$

Solution. Let us use the notation for a permutation in which $a \in \{1, 2, \cdots, 15\}$ is written above $\sigma(a)$. Thus

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix},$$

We can read off the disjoint cycles whose product is σ. Since $1 \to 13 \to 5 \to 10 \to 1$ one of those cycles will be

$$(1, 13, 5, 10) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 3 & 4 & 10 & 6 & 7 & 8 & 9 & 1 & 11 & 12 & 5 & 14 & 15 \end{pmatrix}.$$

Similarly, we will also need the cycles $(3, 15, 8)$ and $(4, 14, 11, 7, 12, 9)$. The cycles $(1, 13, 5, 10, 1)$, $(3, 15, 8)$ and $(4, 14, 11, 7, 12, 9)$ commute pairwise, so we can multiply them together in any order, and we get

$$\sigma = (1, 13, 5, 10)(3, 15, 8)(4, 14, 11, 7, 12, 9).$$

Optionally we could include (2) and (6) for notational comp

$$\sigma = (1, 13, 5, 10)(3, 15, 8)(4, 14, 11, 7, 12, 9).$$

leteness. It would not be wrong to write

$$\sigma = (1, 13, 5, 10)(2)(3, 15, 8)(4, 14, 11, 7, 12, 9)(6),$$

and then every element appears once. But (2) and (6) are just notations for the identity element, so including them is not necessary.

Similarly, with

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{pmatrix}$$

we have

$$\tau = (1, 14)(2, 9, 15, 13, 4)(3, 10)(5, 12, 7)(6)(8, 11).$$

Again, the inclusion of (6) here is optional: including it only serves the purpose of making it easier to see that $\tau(6) = 6$. The cycles commute, so we could permute them in any way and the answer would still be correct.

For the remaining elements I get:

$$\sigma^2 = (1,5)(3,8,15)(4,11,12)(14,7,9)(2)(6)(13,10),$$

$$\sigma\tau = (1,11,3)(2,4)(5,9,8,7,10,15)(6)(12)(13,14),$$

$$\tau\sigma = (1,4)(2,9)(3,13,12,15,11,5)(6)(7)(8,10,14),$$

$$\tau^2\sigma = (1,2,15,8,3,4,14,11,12,13,7,5,10)(6)(9).$$

Problem 1.3 # 5. Find the order of $(1,12,8,10,4)(2,13)(5,11,7)(6,9)$.

Solution. Define the *support* $\mathrm{supp}(\sigma)$ of a permutation σ of $X = \{1,2,3,\cdots,n\}$ to be the set of $x \in X$ such that $\sigma(x) \neq x$. If σ and τ have disjoint supports, then it is clear that σ and τ commute. The four cycles $(1,12,8,10,4)$, $(2,13)$, $(5,11,7)$ and $(6,9)$ have disjoint supports, so

$$((1,12,8,10,4)(2,13)(5,11,7)(6,9))^N = (1,12,8,10,4)^N(2,13)^N(5,11,7)^N(6,9)^N = 1$$

if and only if

$$(1,12,8,10,4)^N = (2,13)^N = (5,11,7)^N = (6,9)^N = 1.$$

Thus N must be a multiple of 5, 2, 3 and 2. Thus a necessary and sufficient condition is that N is divisible by the least common multiple of 5,2,3,2, that is, 30. Therefore the order of this permutation is 30.

Problem 1.3 # 13. Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Solution. Write the permutation σ as a product of disjoint cycles $\sigma_1 \cdots \sigma_r$. The cycles σ_i and σ_j permute since their supports are disjoint. So $\sigma^2 = \sigma_1^2 \cdots \sigma_r^2$. Now the supports of $\sigma_1^2, \cdots, \sigma_r^2$ are disjoint, so $\sigma^2 = 1$ if and only if $\sigma_1^2 = \cdots = \sigma_r^2 = 1$. Since σ_i is a cycle, $\sigma_i^2 = 1$ if and only if σ_i is a 2-cycle. Thus $\sigma_i^2 = 1$ if and only if each σ_i is a 2-cycle.

Problem 1.3 # 20. Find a set of generators and relations for S_3.

Solution 1. Since $S_3 \cong D_6$ we could take $r = (123)$ and $s = (12)$ and use the same generators and relations that we had for the dihedral group:

$$S_3 = \langle r, s | r^3 = s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Solution 2. The group S_3 is generated by $s = (12)$ and $t = (23)$. We have $st = (123)$, so we get the relations

$$s^2 = t^2 = 1, \qquad (st)^3 = 1.$$

We claim that these relations give a presentation of S_3. Indeed, let G be the group generated by s and t subject to these relations. We will show that G has order 6. First, let us show that it has order at most 6. We will need the relation

$$sts = tst. \tag{1}$$

To prove this note that $(st)^3 = 1$ can be written $ststst = 1$ and since s and t have order 2, this implies that $sts = sts(ststst) = tst$ after some cancellations, proving (1).

Now let us show that G has order at most 6. Let X be the subset consisting of

$$X = \{1, s, t, sts, st, ts\}.$$

We claim that $sX = X$ and $tX = X$. Indeed,

$$sX = \{s, 1, st, s^2ts, s^2t, sts\} = \{s, 1, st, ts, t, sts\} = X.$$

Similarly

$$tX = \{t, ts, 1, tsts, tst, s\} = \{t, ts, 1, st, sts, s\}$$

where we have used (1). The set X is closed under multiplication and contains s and t, so X is the group generated by s and t. This proves that G has order at most 6.

Now since (12) and (23) in S_3 satisfy the same relations as s and t in the abstract group G, the group G does not have order smaller than 6, and the group they generate is isomorphic to S_3.

Problem 1.4 # 7. Let p be a prime. Show that the order of $\mathrm{GL}_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$.

I'll give two solutions. There is a hint in the book for how to do this, but it seems to me there is a better way. (I did this in class.) So I'll present both solutions.

Solution 1. The hint in the book requests that we check this by computing the number of elements of $\mathrm{Mat}_2(\mathbb{F}_p)$ thta are not invertible. So let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{F}_p)$. A necessary and sufficient condition that M is not invertible is that $ad - bc = \det(M) = 0$. Let us count the number of solutions $ad = bc$ with $ad = k$ for $k \in \mathbb{F}_p$. First, if $k = 0$, there are $(2p - 1)$ possibilities for a and d, since

$$\{(a, d) | ad = 0\} = \{(a, 0) | a \in \mathbb{F}_p\} \cup \{(0, d) | d \in \mathbb{F}_p\},$$

and the two sets have one element $(0, 0)$ in common. Similarly there are $(2p-1)$ possibilities for b and c and therefore if $k = 0$ there are $(2p - 1)^2$ solutions to $ad = bc = 0$.

On the other hand if $k \neq 0$ there there are $p - 1$ solutions (a, d) to $ad = k$, namely

$$\left\{ \left(a, \frac{k}{a} \right) | a \in \mathbb{F}_p^\times \right\};$$

similarly there are $p - 1$ solutions (b, c) to $bc = 1$. There are thus $(p - 1)^2$ solutions to $ad = bc = k$ with $k \neq 0$. We must multiply this by $(p - 1)$ since there are $p - 1$ choices for k. Combining with our previous solutions we get

$$(2p - 1)^2 + (p - 1)^3 = 4p^2 - 4p + 1 + p^3 - 3p^2 + 3p - 1 = p^3 + p^2 - p$$

matrices that are *not* invertible. We subtract this number from the total number p^4 of all matrices to obtain $p^4 - p^3 - p^2 + p$.

Solution 2. A better way of counting invertible matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is to first note that the first column can be any nonzero vector $\begin{pmatrix} a \\ c \end{pmatrix}$. There are $p^2 - 1$ choices for this, namely any of the p^2 vectors in $\mathbb{F}_p^2$ except $(0,0)$. Then once a, c are chosen, the vector $\begin{pmatrix} b \\ d \end{pmatrix}$ can be any vector that is not one of the p multiples of $\begin{pmatrix} a \\ c \end{pmatrix}$; there are thus $p^2 - p$ choices for b, d. Now the total number is $(p^2-1)(p^2-p) = p^4 - p^3 - p^2 + p$.

(The second solution seems better, but does not follow the hint in the book.)

Problem 1.5 # 2. Write the group tables for S_3, D_8 and Q_8.

Solution. I'll only do the case of Q_8.

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Problem 1.6 # 1. Let $\varphi : G \longrightarrow H$ be a homomorphism.

(a) Prove that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}_+$.

(b) Show that $\phi(x^{-1}) = \phi(x)^{-1}$ and deduce that $\phi(x^n) = \phi(x)^n$ for all n.

Solution. (a) We have $\phi(x^n) = \phi(x \cdots x)$ where there are n copies of x. Since ϕ is a homomorphism, this equals $\phi(x) \cdots \phi(x) = \phi(x)^n$.

(b) First note that $\phi(1) = 1$. To prove this, note that $\phi(1) \cdot \phi(1) = \phi(1^2) = \phi(1)$ and multiplying both sides of this equation by $\phi(1)^{-1}$ gives $\phi(1) = 1$. This gives us $\phi(x^n) = \phi(x)^n$ when $n = 0$.

Now $\phi(x) \cdot \phi(x^{-1}) = \phi(x \cdot x^{-1}) = \phi(1) = 1$, proving that $\phi(x^{-1}) = \phi(x)^{-1}$.

To deduce that $\phi(x^n) = \phi(x)^n$ for all n, we have already settled the cases $n > 0$ and $n = 0$, so assume that $n < 0$. Then $\phi(x^n) = \phi((x^{-1})^{|n|})$ since $n = -|n|$. Now $|n| > 0$ so we can use (a) and obtain $\phi(x^n) = \phi(x^{-1})^{|n|} = (\phi(x)^{-1})^{|n|} = \phi(x)^n$.

Alternative Solution for (a): If you want to give more detail, this proof can be organized as an induction.

We show that $\phi(x^n) = \phi(x)^n$ if n is a positive integer. If $n = 1$ this is trivial so assume $n > 1$ and that the statement is true for $n - 1$. Then

$$\phi(x^n) = \phi(x \cdot x^{n-1}) = \phi(x)\,\phi(x^{n-1}).$$

By induction $\phi(x^{n-1}) = \phi(x)^{n-1}$. So $\phi(x^n) = \phi(x)\,\phi(x)^{n-1} = \phi(x)^n$. This completes the proof by induction.