MATH 6302 - Modern Algebra
Homework 3

Joel Sleeba

September 21, 2024

1. **Solution:**

$$
\begin{tikzcd}
 & Q_8 & \\
\langle i \rangle \arrow[ur] & \langle j \rangle \arrow[u] & \langle k \rangle \arrow[ul] \\
 & \langle -1 \rangle \arrow[ul] \arrow[u] \arrow[ur] & \\
 & \langle 1 \rangle \arrow[u] &
\end{tikzcd}
$$

2. **Solution:**

$$
\begin{tikzcd}
 & \langle 1 \rangle & \\
\langle 3 \rangle \arrow[ur] & & \langle 2 \rangle \arrow[ul] \\
\langle 9 \rangle \arrow[u] & & \langle 6 \rangle \arrow[u] \arrow[ull] \\
\langle 18 \rangle \arrow[u] & & \langle 12 \rangle \arrow[u] \\
 & \langle 0 \rangle \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

3. **Solution:** Consider the subset $\mathbb{N}$ of the group $\mathbb{Q}$ under addition. Since adding any two natural numbers give another natural number, we see that $\mathbb{N}$ is closed under addition. But there is no element in $\mathbb{N}$ which acts as an identity in $\mathbb{N}$. Hence it is an example of a subset of a group which closed under the group, yet not a subgroup.

4. **Solution:** Let S_i be a finite generating subset of G_i. Consider the set

   $$S = \{(e_1, \ldots, e_{i+1}, s_i, e_{i+1}, \ldots, e_n) \bigm| s_i \in S_i, e_i \text{ is the identity in } G_i, 1 \leq i \leq n\}$$

   Clearly $|S| = \sum_{i=1}^{n} |S_i| < \infty$. We claim that S generate $G = G_1 \times G_2 \times \cdots \times G_n$. For any element $(g_1, g_2, \ldots, g_n) \in G$, we see that

   $$(g_1, g_2, \ldots, g_n) = (g_1, e_2, \ldots, e_n)(e_1, g_2, \ldots, e_n) \ldots (e_1, e_2, \ldots g_n)$$

   Hence it is enough if we show S generate $(e_1, e_2, \ldots, g_i, \ldots, e_n)$ for an arbitrary $1 \leq i \leq n$. But since S_i is a generating set for G_i, there exists a collection $s_{ij} \in S_i$ such that $g_i = s_{i1}s_{i2} \ldots s_{ik}$. Then

   $$\begin{aligned}(e_1, e_2, \ldots, s_{i1}, \ldots, e_n) \ldots (e_1, e_2, \ldots, s_{ik}, \ldots, e_n) &= (e_1, e_2, \ldots, (s_{i1}s_{i2} \ldots s_{ik}), \ldots, e_n) \\ &= (e_1, e_2, \ldots, g_i, \ldots, e_n)\end{aligned}$$

   Hence we get that S generate G.

5. **Solution:** Assume $GL_2(\mathbb{Q})$ is finitely generated. We see that for every $r \in \mathbb{Q}$, the matrix

   $$\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}$$

   has determinant r. Now since we know $\det(AB) = \det(A)\det(B)$ for all $A, B \in GL_2(\mathbb{Q})$. Hence $\det : GL_2(\mathbb{Q}) \to \mathbb{Q} \setminus \{0\}$ is a surjective group homomorphism. Now if $GL_2(\mathbb{Q})$ is finitely generated by a set $S \subset GL_2(\mathbb{Q})$, we must have $\det(S)$ generate $\mathbb{Q} \setminus \{0\}$. But this gives a contradiction since we know $\mathbb{Q} \setminus \{0\}$ is not finitely generated.

6. **Solution:** Since G is Abelian and finitely generated by $g_1, g_2, \ldots, g_n$, every element of G can be written as $g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_n^{\alpha_n}$ where $0 \leq \alpha_i < |g_i|$. Now consider the map $\phi : Z_{|g_1|} \times Z_{|g_2|} \times \ldots Z_{|g_n|} \to G$ as $(\alpha_1, \alpha_2, \ldots, \alpha_n) \to g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_n^{\alpha_n}$. Clearly ϕ is a surjection. Therefore the cardinality of the domain is greater than the cardinality of the range, which gives our required inequality.

7. **Solution:**

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

   (b) $\sigma = (1\ 9)(1\ 3)(1\ 11)(2\ 4)(2\ 12)(5\ 8)(5\ 6)$
   $\tau = (1\ 5)(1\ 3)(2\ 10)(4\ 9)(4\ 11)(4\ 7)(4\ 8)(4\ 6)(4\ 12)$

   (c) $\sigma^2\tau = (1)(2\ 10\ 4)(3\ 8\ 7\ 9\ 12\ 5)(6)(11)$

   (d) We see that $\sigma\tau = (1\ 9\ 2\ 10\ 12\ 8\ 7\ 3\ 6\ 5\ 11)(4)$. Hence we'll get $(\sigma\tau)^{-1} = (11\ 5\ 6\ 3\ 7\ 8\ 12\ 10\ 2\ 9\ 1)(4)$

8. **Solution:** We'll use the combinatorial distinct balls in similar holes problem. Assume the places to put numbers in the 5 cycle representation (a, b, c, d, e) as holes and the numbers in Z_{10} as balls. There are $10P5 = 10 \times 9 \times 8 \times 7 \times 6$ ways to place balls in these holes. But we see that for every 5 cycle, there are 5 distinct ways to represent them like this. That is $(a, b, c, d, e), (b, c, d, e, a), (c, d, e, a, b), (d, e, a, b, c), (e, a, b, c, d)$ all correspond to the same cycle. Therefore the number of distinct cycles is $(10P5)/5 = \frac{10\times9\times8\times7\times6}{5} = 6048$

9. **Solution:**

   (a) Since it is given that σ is a 36 cycle, $|\sigma| = 36$. Moreover we know that for any group G with $g \in G$, $|g^k| = \frac{|g|}{(|g|,k)}$. Hence $|\sigma^k| = \frac{36}{(36,k)}$. And the possible values for $|\sigma^k|$ for $1 \leq k \leq 36$ are precisely the factors of 36. $36 = 2^2 3^2$. Hence the possible values are $\{36, 18, 12, 9, 6, 4, 3, 2, 1\}$.

   (b) Since $\langle\sigma\rangle$ is cyclic with order 36, it is isomorphic with Z_{36}. Therefore the question translates to finding the number of generators for Z_{36}, which is $\phi(36) = 12$.

10. **Solution:** From question 13, we see that $A_4 = \langle(1\ 2)(3\ 4), (1\ 2\ 3)\rangle$. We know $|A_4| = 4!/2 = 12$ while $|(1\ 2)(3\ 4)| = 2$ and $|(1\ 2\ 3)| = 3$. Since $12 > 2 \times 3 = 6$, this works as an example.

11. **Solution:** Since disjoint cycles commute in S_n, we get that $(\sigma_1\sigma_2\cdots\sigma_l)^m = \sigma_1^m\sigma_2^m\cdots\sigma_l^m$. Let $n = \text{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_l|)$. Then $|\sigma_i|\big|n$ for all $1 \leq i \leq l$

and therefore $\sigma_i^n = e$ for all $1 \leq i \leq l$. Hence we see that $(\sigma_1\sigma_2\cdots\sigma_l)^n = (\sigma_1^n\sigma_2^n\cdots\sigma_l^n) = e$. Therefore $|\sigma_1\sigma_2\cdots\sigma_l|\big|n$. Hence

$$|\sigma_1\sigma_2\cdots\sigma_l| \;\Big|\; \operatorname{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_l|)$$

Now if $m \in \mathbb{N}$ such that $(\sigma_1\sigma_2\cdots\sigma_l)^m = \sigma_1^m\sigma_2^m\cdots\sigma_l^m = e$, we must have $\sigma_i^m = e$ for each $1 \leq i \leq l$. This is because each of the cycle σ_i are pairwise disjoint, so must be their powers. This implies $|\sigma_i|\big|m$ for each $1 \leq i \leq l$. This gives that $\operatorname{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_l|)\big|m$. Now take $m = |\sigma_1\sigma_2\cdots\sigma_l|$ to get

$$\operatorname{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_l|) \;\Big|\; |\sigma_1\sigma_2\cdots\sigma_l|$$

Therefore $\operatorname{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_l|) = |\sigma_1\sigma_2\cdots\sigma_l|$

12. **Solution:**

    (a) We will use a counting procedure that will exhaust all possible orders of elements using disjoint cycle representation. Note from the previous problem that the order of $\sigma_1\sigma_2\cdots\sigma_n$ is $\operatorname{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_l|)\big||\sigma_1\sigma_2\cdots\sigma_l|$ if σ_i are disjoint cycles. Moreover in the disjoint cycle representation $\sigma_1\sigma_2\cdots\sigma_n$ we can demand that the cycles be ordered in the descending order of their orders. That is $\sigma_1\sigma_2\cdots\sigma_n \in S_m$ must have $|\sigma_1| \geq |\sigma_2| \geq \cdots \geq |\sigma_n|$

    Now we will iterate over the number of elements in Z_{10} fixed by elements in S_{10}. We will denote the number of elements being fixed using the variable r.

    - $r = 10$. If every elements of Z_{10} are fixed by an element in S_{10}, it must be the identity element. Hence the order of such elements is 1.
    - $r = 9$. If an element fixes 9 elements in Z_{10}, it must also fix the last element, since S_{10} is the collection of bijections of Z_{10}. Hence the only possibility is if the element in S_{10} is the identity which has order 1.
    - $r = 8$. If an element in S_{10} fixes 8 elements (avoiding the case where it fixed more than 8 elements) in Z_{10}, it must be of the form $(a\ b)$, which has order 2.
    - $r = 7$. Then the element must be of the form $(a\ b\ c)$, which has order 3

- $r = 6$. Then the element must be either of the two forms $(a\ b\ c\ d)$ or $(a\ b)(c\ d)$. Therefore the possible orders are 4 and 2.
- $r = 5$. Then the element must be of the following possible forms
  (i) $(a\ b\ c\ d\ e)$
  (ii) $(a\ b\ c)(d\ e)$

  Note that since we showed every element can be arranged with the disjoint cycles in the descending order of their orders, we omit $(a\ b)(c\ d\ e)$.

  Hence the possible orders are 5 and 6.
- $r = 4$. The possible forms are
  (i) $(a\ b\ c\ d\ e\ f)$
  (ii) $(a\ b\ c\ d)(e\ f)$
  (iii) $(a\ b\ c)(d\ e\ f)$

  Hence the possible orders are $6, 8$ and 9.
- $r = 3$. The possible forms are
  (i) $(a\ b\ c\ d\ e\ f\ g)$
  (ii) $(a\ b\ c\ d\ e)(f\ g)$
  (iii) $(a\ b\ c\ d)(e\ f\ g)$
  (iv) $(a\ b\ c)(d\ e)(g\ f)$

  Hence the possible orders are $7, 10, 12, 6$.
- $r = 2$. The possible forms are
  (i) $(a\ b\ c\ d\ e\ f\ g\ h)$
  (ii) $(a\ b\ c\ d\ e\ f)(g\ h)$
  (iii) $(a\ b\ c\ d\ e)(f\ g\ h)$
  (iv) $(a\ b\ c\ d)(e\ f\ g\ h)$
  (v) $(a\ b\ c\ d)(e\ f)(g\ h)$
  (vi) $(a\ b\ c)(d\ e\ g)(f\ h)$
  (vii) $(a\ b)(c\ d)(e\ f)(g\ h)$

  Hence the possible orders are $8, 12, 15, 4, 6, 2$.
- $r = 1$. The possible forms are
  (i) $(a\ b\ c\ d\ e\ f\ g\ h\ i)$
  (ii) $(a\ b\ c\ d\ e\ f\ g)(h\ i)$
  (iii) $(a\ b\ c\ d\ e\ f)(g\ h\ i)$

(iv) $(a\ b\ c\ d\ e)(f\ g\ h\ i)$

(v) $(a\ b\ c\ d\ e)(f\ g)(h\ i)$

(vi) $(a\ b\ c\ d)(e\ f\ g)(h\ i)$

(vii) $(a\ b\ c)(d\ e\ f)(g\ h\ i)$

(viii) $(a\ b\ c)(d\ e)(f\ g)(h\ i)$

Hence the possible orders are $9, 14, 18, 20, 10, 12, 3, 6$

- $r = 0$. Then the possible forms are

(i) $(a\ b\ c\ d\ e\ f\ g\ h\ i\ j)$

(ii) $(a\ b\ c\ d\ e\ f\ g\ h)(i\ j)$

(iii) $(a\ b\ c\ d\ e\ f\ g)(h\ i\ j)$

(iv) $(a\ b\ c\ d\ e\ f)(g\ h\ i\ j)$

(v) $(a\ b\ c\ d\ e\ f)(g\ h)(i\ j)$

(vi) $(a\ b\ c\ d\ e)(f\ g\ h\ i\ j)$

(vii) $(a\ b\ c\ d\ e)(f\ g\ h)(i\ j)$

(viii) $(a\ b\ c\ d)(e\ f\ g\ h)(i\ j)$

(ix) $(a\ b\ c\ d)(e\ f\ g)(h\ i\ j)$

(x) $(a\ b\ c\ d)(e\ f)(g\ h)(i\ j)$

(xi) $(a\ b\ c)(d\ e\ f)(g\ h)(i\ j)$

(xii) $(a\ b)(c\ d)(e\ f)(g\ h)(i\ j)$

Hence the possible orders are $10, 16, 21, 24, 12, 5, 30, 4, 12, 6, 2$

Therefore all the possible orders of elements in S_{10} are 30, 24, 21, 20, 18, 16, 15, 14, 12, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1.

(b) $30 = 2 \times 3 \times 5$. Hence the possible ways to write 30 as a product of co-primes are $1 \times 30, 2 \times 15, 3 \times 10, 6 \times 5, 2 \times 3 \times 5$, where the sum of the coprimes is the lowest at $2 \times 3 \times 5$. Hence S_{10} is the group we are looking for.

13. **Solution:** Clearly $(12)(34), (123) \in A_4$. Since we know that A_4 have 12 elements once we find 7 distinct elements in $\langle(12)(34), (123)\rangle$, using Lagrange's theorem we can be sure that $\langle(12)(34), (123)\rangle = A_4$.

- $(123)^{-1} = (132)$
- $(12)(34)(123) = (243)$

- $(123)(12)(34) = (134)$
- $(12)(34)(123) = (143)$
- $(12)(34)(132) = (143)$
- $(132)(12)(34) = (234)$

Since all the 7 elements above (including $(12)(34), (123)$) are in A_4 and generated by $(12)(34)$ and (123), we conclude that $A_4 = \langle (12)(34), (123) \rangle$

14. **Solution:**

 (a) Isomorphic. $\phi : \mathbb{Z} \to 8\mathbb{Z} := n \to 8n$ is an isomorphism. $\phi(a+b) = 8(a+b) = 8a + 8b = \phi(a) + \phi(b)$.

 (b) Not isomorphic. $\mathbb{Z}$ is cyclic but $\mathbb{Q}$ is not.

 (c) Not isomorphic. By Cantor's diagonalization argument we know that there does not exist a bijection between $\mathbb{Q}$ and $\mathbb{R}$.

 (d) Not isomorphic. The only element in $\mathbb{R}$ of finite order is 0. But the same does not hold for $\mathrm{SL}_2(\mathbb{R})$. For example I and $-I$.

 (e) Isomorphic. Since $49 = 7^2$, by primitive root theorem, we see that $\mathbb{Z}_{49}^*$ has $\phi(49) = 42$ elements and is cyclic. Since every cyclic group of same order is isomorphic we get $\mathbb{Z}_{49}^* \cong \mathbb{Z}_{42}$. We can verify that 3 is a primitve root modulo 49, hence the map $\phi : Z_{49}^* \to Z_{42} : 3^a \to a \mod 42$ is an isomorphism.

 (f) Isomorphic. We first notice that $C_2 \times C_3 \cong C_6$ by the map $\phi : (a, b) \to ab$ is an isomorphism. (Note that here we're identifying C_6, C_3 and C_2 with Z_6, Z_3 and Z_2 respectively). Then $\psi : C_2 \times C_2 \times C_3 \to C_2 \times C_6 := (a, b, c) \to (a, \phi(b, c))$ is an isomorphism which shows the groups are isomorphic.

 (g) Not isomorphic. In last assignment we proved that the group $(\mathcal{P}(\{1, 2\}), \Delta) \cong V_4$. Moreover we know that $V_4 \ncong C_4$.

 (h) Isomorphic. Consider the map $\phi : (\mathcal{P}(\{1, 2, 3\}), \Delta) \to C_2 \times C_2 \times C_2 := A \to (\chi_A(1), \chi_A(2), \chi_A(3))$. Since $A \Delta B = (A \setminus A \cap B) \cup (B \setminus A \cap B)$, we get

$$\begin{aligned}\chi_{A\Delta B} &= \chi_{A\setminus A\cap B} + \chi_{B\setminus A\cap B}\\ &= (\chi_A - \chi_A\chi_B) + (\chi_B - \chi_A\chi_B)\\ &= (\chi_A + \chi_B) \mod 2\end{aligned}$$

which proves that our map ϕ is a group homomorphism. Moreover it is bijective, hence a group isomorphism.

15. **Solution:** Since Z_n is cyclic, if $\phi : Z_n \to Z_n$ is a homomorphism, it is completely determined by where it sends its generator. Moreover ϕ should be an isomorphism, then it must send generators to generators.

    Let's fix $1 \in Z_n$ as the generator of the domain. We see that every integer less than n, which are relatively prime to n will again generate Z_n. Moreover by the definition of Euler-totient function, we know that there are exactly $\varphi(n)$ such numbers. Therefore ϕ to be isomorphism, $\phi(1)$ has $\varphi(n)$ many choices, and each of them give a different isomorphism. Hence there are $\varphi(n)$ automorphisms of Z_n.

16. **Solution:** Since we know that $C_2 \times C_2 \cong V_4$, there is a correspondence between homomorphims of $C_2 \times C_2$ and V_4, and specifically automorphisms. Now, we know that $V_4 = \langle a, b \;:\; a^2 = b^2 = 1, ab = ba\rangle = \{e, a, b, c\}$ where $c = ab$. If $\phi : V_4 \to V_4$ is an automorphism, then $\phi(e) = e$. Since the order of all the rest of the elements are 2, we have freedom over how ϕ permutes elements of the set $\{a, b, c\}$. Hence we see that there are $3! = 6$ automorphisms of V_4.

17. **Solution:** 23 is a prime. Therefore $|Z_{23}^*| = \phi(23) = 22$ elements and is cyclic by primitive root theorem. Therefore $Z_{23}^* \cong Z_{22}$. Since Z_{23}^* is cyclic and 5 is a generator, if $\phi : Z_{23}^* \to Z_{23}^*$ is any homomorphism, it is completely determined by the $\phi(5)$. Moreover if ϕ has to an automorphism, then $\phi(5)$ must also be a generator for Z_{23}^*. Since $Z_{23}^* \cong Z_{22}$, we see that there are $\varphi(22) = 10$ generators for Z_{23}^*. Hence there are 10 choices for $\phi(5)$ in Z_{23}^* which makes ϕ an automorphism.