Math 410 Homework 2

By: Hanting Zhang   Due Date: **Jan. 29, 2022**

Exercises 8, 9, 12, 26, 36, pp. 21-23.

8. (a) Since G is a subset of $\mathbb{C}$, it suffices to prove that G is a subgroup of $\mathbb{C}$. For any $g, h \in G$, we need to show that $gh^{-1} \in G$. By definiton there exist some $n, m \in \mathbb{Z}^+$ such that $g^n = h^m = 1$.

   We want to find N such that $(gh^{-1})^N = 1$. Let $N = nm$ and notice that $(gh^{-1})^{nm} = g^{nm} * h^{-nm} = (g^n)^m * (h^m)^{-n} = 1^m * 1^{-n} = 1$. Hence $gh^{-1} \in G$, and G is a subgroup of $\mathbb{C}$, which makes it a group in general.

   (b) Clearly $1 \in G$, but $1 + 1 = 2 \notin G$. So G is not closed under addition.

9. (a) Again we prove that G is a group by proving it is a subgroup of $\mathbb{R}$.

   For any $g, h \in G$, there are some $a, b, c, d \in \mathbb{Q}$ with $g = a + b\sqrt{2}$ and $h = c\sqrt{d}$. then $g - h = (a - c) + (b - d)\sqrt{2}$. Clearly $a - c$ and $b - d$ are rational, so $g - h \in G$, as desired.

   (b) Let g be a non-zero element of G such that $a + b\sqrt{2} = g$ for some $a, b \in \mathbb{Q}$ (where a and B are not both 0). Then note that $1/g = 1/(a + b\sqrt{2})$ is in G, since

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

   Letting $x = \frac{a}{a^2 - 2b^2}$ and $y = \frac{-b}{a^2 - 2b^2}$, we have $1/g = x + y\sqrt{2}$. Both x and y are rational, since they are made up of rational expressions. Hence $1/g$ (in $\mathbb{R}$) is the inverse of g in G.

   Note. This makes G a *field*. In fact it is the field $\mathbb{Q}[\sqrt{2}]$, the result of adjoining $\sqrt{2}$ to $\mathbb{Q}$.

12. We can just calculate the orders:

$$\begin{aligned}
|\overline{1}| &= 1 \\
\overline{-1}^2 = 1 \implies |\overline{-1}| &= 2 \\
\overline{5}^2 = \overline{25} = \overline{1} \implies |\overline{5}| &= 2 \\
\overline{7} = -\overline{5} \implies |\overline{7}| &= 2 \\
\overline{-7} = \overline{5} \implies |\overline{-7}| &= 2 \\
\overline{13} = \overline{1} \implies |\overline{13}| &= 1
\end{aligned}$$

26. We proceed by proving the goal axioms for H:

   Identity: Let $1_H = 1_G$. Then for all $h \in H$, $1_H *_H h = 1_G *_G h = h$ by definition.

   Associativity: For any $h_1, h_2, h_3 \in H$, $(h_1 *_H h_2) *_H h_3 = (h_1 *_G h_2) *_G h_3 = h_1 *_G (h_2 *_G h_3) = h_1 *_H (h_2 *_G h_3)$. Here we use the associativity of G.

   Closure: Given by assumption.

   Inverses: Given by assumption.

36. Write it out in a table!

	1	a	b	c
1	1	a	b	c
a	a			
b	b			
c	c			

With loss of generality we can swap between b and c by relabeling them $c = b'$ and $b = c'$. Hence for $aa =?$, we only need to consider cases $aa = 1$ and $aa = b$.

Case $aa = b$: Then $ab = 1$ or $ab = c$. In the first case, we have $aab = a1 \Rightarrow bb = a \Rightarrow aaaa = a \Rightarrow aaa = 1$. But a cannot be of order 3, thus we must have $ab = c$. So the final entry ac is 1 because that's the only choice left:

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b			
c	c			

Now ba is either c or 1. By the same logic it must be c and $ac = 1$. This makes it easy to fill out the rest of the table $bb = 1$, $bc = a$, $cb = a$, $cc = b$.

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

But here, we see that $aa = b$ and so $aaaa = bb = 1$. Thus a has order 4, so the table is **not** the one we're looking for.

Case $aa = 1$: Then we must have $ab = ba = c$ and $ac = ca = b$. More deductions show that, $bb = 1$, $cc = 1$, $bc = cb = a$. The tables is:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

So this is the unique table of G. Clearly G is abelian.

Exercises 3, 9, pp. 27-28.
We will have to use the fact that $D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$. This is not easy to prove formally because we don't have a formal definition of a presentation yet, so for now I will take it to be true.

3. Since x is not a rotation, it must be of the form sr^i for $0 \leq i < n$. Then $(sr^i)^2 = sr^i sr^i = ssr^{-i}r^i = 1 * 1 = 1$. Thus sr^i has order 2.

   We can combine s and sr to get $ssr = r$. Hence s and sr generate r, which together will generate D_{2n}.

9. Note that the orientation of the tetrahedron is determined the orientation of a single edge. Call the edge ab. Then there are 4 choices for a and 3 choices for b, giving a total of 12 orientations, or 12 possible rigid motions we can do.

Exercises 2, 4, 13, 16, 20, pp. 32-34.

2. Write everything in cycle notation. We have $\sigma = (1,13,5,10)(3,15,8)(4,14,11,7,12,9)$ and $\tau = (1,14)(2,9,15,13,4)(3,10)(5,12,7)(8,11)$.

   Then quick calculations show that:

$$\begin{aligned}
\sigma^2 &= (1,5)(5,10)(3,15,8)(4,11,12)(14,7,9) \\
\sigma\tau &= (1,11,3)(2,4)(5,9,8,7,10,15)(13,14) \\
\tau\sigma &= (1,4)(2,9)(3,13,12,15,11,5)(8,10,14) \\
\tau^2\sigma = \tau(\tau\sigma) &= (1,2,15,8,3,4,14,11,12,13,7,5,10)
\end{aligned}$$

4. (a) S_3 has 6 elements: $\{(), (12), (23), (13), (123), (132)\}$. Direct calculation shows that these elements have orders $0, 2, 2, 2, 3, 3$.

   (b) S_4 has 24 elements:

      i. 1 identity: (); order $= 0$;
      ii. 6 transpositions: $(12), (23), (34), (14), (13), (24)$; order $= 2$;
      iii. 3 disjoint products of transpositions: $(12)(34), (23)(14), (13)(24)$; order $= 2$;
      iv. 8 3-cycles: $(123), (132), (124), (142), (134), (143), (234), (243)$; order $= 3$;
      v. 6 4-cycles: $(1234), (1243), (1324), (1342), (1423), (1432)$; order $= 4$.

13. ($\Rightarrow$): If σ is a product of commuting 2-cycles. Let $\sigma = (a_1b_1)(a_2b_2)\dots(a_kb_k)$. Then

$$\sigma^2 = (a_1b_1)(a_2b_2)\dots(a_kb_k)(a_1b_1)(a_2b_2)\dots(a_kb_k) = (a_1b_1)^2\dots(a_kb_k)^2,$$

   since all the factors commute. But squaring a 2-cycle makes the term vanish, so $\sigma^2 = 1$ and σ has order 2.

   ($\Leftarrow$): Suppose σ has order 2. Decompose σ as the product of disjoint cycles $c_1, \dots c_k$, with lengths $\ell_1, \dots, \ell_k$. Since $\sigma^2 = 1$ and disjoint cycles do not affect each other, we must have $c_1^2 = c_2^2 = \dots = c_k^2 = 1$. Then $\ell_1 = \dots = \ell_k = 2$ and everything is a 2-cycle, as desired.

16. We make a combinatorial argument. To form an m-cycle we must choose m objects out of n, where order matters. This gives $n(n-1)\dots(n-m+1)$ possible choices. However, for each cycle, we have m different representations created by shifting the cycle over m times. Hence we have overcounted by a factor of m. Thus the final answer is

$$\frac{n(n-1)\dots(n-m+1)}{m}.$$

20. We know that $S_3 = \{(), (12), (23), (13), (123), (132)\}$ and that $(12)(23) = (123)$. So (12) and (23) can generate $()$, (123), and (132). Then $(132)(12) = (23)$. Hence $a = (12)$ and $b = (23)$ generate S_3. The relations are at least $a^2 = b^2 = 1$. This isn't enough though, because it tells us nothing about how $ab = (123)$ behaves. Thus we need another relation $(ab)^3 = 1$ to constrain (123). This gives

$$S_3 = \langle a, b : a^2 = b^2 = 1, (ab)^3 = 1 \rangle.$$

Exercises 17, 18, pp. 40.

17. Let $i : G \to G$ be the map $g \mapsto g^{-1}$. Then $i(gh) = (gh)^{-1} = h^{-1}g^{-1}$. Clearly $i(gh) = i(g)i(h)$ if and only if h^{-1} commutes with g^{-1} for all $g, h \in G$, i.e. G is abelian.

18. Let $s : G \to G$ be the map $g \mapsto g^2$. Then $s(gh) = (gh)^2 = ghgh$. If G is abelian, then $ghgh = gghh = g^2h^2 = s(g)s(h)$. Thus s is a homomorphism. Conversely, if $s(gh) = s(g)s(h)$, then we can take $ghgh = gghh$ and multiply by g^{-1} on the left and h^{-1} on the right to cancel. The result is $gh = hg$. This holds for any $g, h \in G$, therefore G is abelian.

Exercises 18, 19, pp. 45.

18. Let H be a left action on A. The relation $a \sim b$ defined by $a = hb$ for some $h \in H$ defines a equivalence relation:

    Reflexive: Let $h = 1$. Then clearly $a = 1a$ for all $a \in A$. Hence $a \sim a$ for all $a \in A$.

    Symmetric: Let $a \sim b$ with $a = hb$. Then $h^{-1}a = b$. Thus $b \sim a$.

    Transitive: Let $a \sim b$ and $b \sim c$ with $a = h_1 b$ and $b = h_2 c$. Then substitute b to see that $a = (h_1 h_2)c$. Hence $a \sim c$.

19. Define $f : H \to \mathcal{O}$ to be the map $h \mapsto hx$. If $f(x) = f(y)$, then $hx = hy$. Cancelling implies $x = y$; thus f is injective. Furthermore, for any $y \in \mathcal{O}$, we know by definition that $y \sim x$. Hence there is some $h \in H$ such that $y = hx$. Thus $f(h) = y$, and f is surjective. The two combine show that f is bijective. We conclude that $|H| = |\mathcal{O}|$.

    But this is true for every orbit $\mathcal{O}$, so all the orbits $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$ have size $|H|$. Since the orbits partition G, we have

    $$|G = \sum_{i=1}^{k} |\mathcal{O}_i| = \sum_{i=1}^{k} |H| = k|H|.$$

    (We may do the sum since G is finite.) Therefore we have *Lagrange's Theorem*: $|H|$ divides $|G|$ for any subgroup H of a finite group G.