HOMEWORK 5 (DUE: 11:15 AM, OCT 17 WED)

Feel free to use the statements in Exercise 13.E. without proof, but make sure that you know how to prove them.

1. Do Exercise 13.F.1–3. in [Pin10, p 132].

13.F.1. We have (note that $a = a^{-1}$ since $a^2 = e$)

$$b \neq a \Leftrightarrow b \neq a^{-1} \Leftrightarrow ba \neq e, \qquad b \neq a \Leftrightarrow b^2 \neq ba,$$
$$b \neq e \Leftrightarrow ba \neq a, \qquad a \neq e \Leftrightarrow ba \neq b.$$

Thus $ba \in \{ab, ab^2\}$.

13.F.2. We define the homomorphism $f : \mathbb{Z}_6 \to G$ to be $f(k) = (ab^2)^k = a^k b^{2k}$. This is clearly a homomorphism since $\mathbb{Z}_6$ is a cyclic group generated by 1, and f is well-defined since $f(1)^6 = (ab^2)^6 = a^6 b^{12} = e$. Also $f(3) = a^3 b^6 = a$ and $f(2) = a^2 b^4 = b$, thus $f(\mathbb{Z}_6) \ni a, b$. Since f is a homomorphism, $f(\mathbb{Z}_6)$ is a subgroup of G, and since it contains the generator a, b of G, f must be surjective. Since $|\mathbb{Z}_6| = |G| = 6$, it means that f is a bijection. In other words, f is an isomorphism.

13.F.3. We define the function $f : G \to S_3$ to be $f(a^i b^j) = (12)^i (123)^j$ for $0 \leq i \leq 1, 0 \leq j \leq 2$. We claim that it is a homomorphism; for any $0 \leq i, k \leq 1, 0 \leq j, l \leq 2$, we have

$$f(a^i b^j a^k b^l) = f(a^{i+k} b^{2^k j + l}) = (12)^{i+k \bmod 2} (123)^{2^k j + l \bmod 3} = (12)^{i+k} (123)^{2^k j + l},$$
$$f(a^i b^j) f(a^k b^l) = (12)^i (123)^j (12)^k (123)^l = (12)^{i+k} (123)^{2^k j + l}$$

Thus $f(a^i b^j a^k b^l) = f(a^i b^j) f(a^k b^l)$. Here we use the fact that $(12)^2 = (123)^3 = e$ and $(123)(12) = (12)(123)^2 = (13)$.

Note. If $k \geq 0$, we have $b^j a^k = a^k b^{2^k j}$. Indeed, by using $ba = ab^2$ repeatedly,

$$b^j a^k = a b^{2j} a^{k-1} = a^2 b^{4j} a^{k-2} = \cdots = a^k b^{2^k j}.$$

For a rigorous proof one can also use induction on the exponent.

Therefore, f is a homomorphism. Since $\{f(a), f(ab)\} = \{(12), (12)(123)\} = \{(12), (23)\} \in f(G)$ and $f(G)$ is a subgroup of S_3, it follows that f is surjective. (Recall that the set of adjacent transpositions generate the symmetric group.) Now since $|G| = |S_3| = 6$, it means that f is a bijection. In other words, f is an isomorphism.

2. Do Exercise 13.G.1–5. (*except 6*) in [Pin10, p. 132].

13.G.1. In the same manner, it follows from Exercise 10.E.3. since 2 and 5 are relatively prime.

13.G.2. We have

$$a \neq e, b, b^2, b^3, b^4 \Leftrightarrow ba \neq b, b^2, b^3, b^4, e, \qquad b \neq e \Leftrightarrow ba \neq a.$$

13.G.3. We define a homomorphism $f : \mathbb{Z}_{10} \to G$ to be $f(k) = (ab^2)^k = a^k b^{2k}$. This is well-defined since $f(1)^{10} = a^{10}b^{20} = e$. Also, $f(\mathbb{Z}_{10}) \supset \{f(5), f(8)\} = \{a^5b^{10}, a^8b^{16}\} = \{a, b\}$, which means that f is surjective since $\{a, b\}$ generates G. Then as $|\mathbb{Z}_{10}| = |G| = 10$, it follows that f is bijective and this it is an isomorphism.

13.G.4. If $ba = ab^2$ then $ba^2 = ab^2a = a^2b^4$. But $a^2 = e$, thus $b = b^4$ which means $b^3 = e$. This is impossible since $|b| = 5$.

13.G.5. Similarly, $ba = ab^3$ implies $ba^2 = ab^3a = a^2b^9$, which means $b = b^9$, i.e. $b^8 = e$. It is also impossible since $|b| = 5$ and 8 is not a multiple of 5.

3. Do Exercise 13.I.1–6. in [Pin10, pp. 133–134].

Here, the index of a subgroup is defined as follows.

Definition 0.1. For a subgroup H of G, *the index of H in G* is the number of left cosets of H in G, denoted $(G : H)$.

13.I.1. We need to check the following conditions.

- Reflexivity: $x = exe^{-1}$, thus $x \sim x$.
- Symmetry: If $x = gyg^{-1}$ for some $g \in G$, then $y = g^{-1}x(g^{-1})^{-1}$. Thus $x \sim y$ implies $y \sim x$.
- Transitivity: If $x = gyg^{-1}$ and $y = hzh^{-1}$ for some $g, h \in G$, then $x = (gh)z(gh)^{-1}$. Thus $x \sim y$ and $y \sim z$ implies $x \sim z$.

Thus $\sim$ is an equivalence relation.

13.I.2. Let us check the following conditions for C_a to be a subgroup of G.

- If $x, y \in C_a$, then $xa = ax$ and $ya = ay$, thus $xya = xay = axy$. It follows that $xy \in C_a$, which means that C_a is closed under the operation on G.
- $ex = xe$, thus $e \in C_a$.

- If $x \in C_a$, then $xa = ax$ which implies $ax^{-1} = x^{-1}a$. Thus $x^{-1} \in C_a$, which means that C_a is closed under taking inverses.

It follows that C_a is a subgroup of G.

13.I.3. $x^{-1}ax = y^{-1}ay \Leftrightarrow a = xy^{-1}a(xy^{-1})^{-1} \Leftrightarrow axy^{-1} = xy^{-1}a \Leftrightarrow xy^{-1} \in C_a$.

13.I.4. It follows from Exercise 13.E.1 and the statement above.

13.I.5. (Here we use the right cosets, but it is okay to use left cosets instead.) Let us define

$$f : \{\text{cosets of } C_a\} \to \{\text{conjugates of } a\} : C_a x \mapsto x^{-1}ax.$$

We claim that this is well-defined. Indeed, if $C_a x = C_a y$, then we should have $f(C_a x) = f(C_a y)$, i.e. $x^{-1}ax = y^{-1}ay$. But this is already proved above. Also, this map is injective since

$$f(C_a x) = f(C_a y) \Rightarrow x^{-1}ax = y^{-1}ay \Rightarrow C_a x = C_a y$$

again by the exercise above. Finally, it is surjective since any conjugate of a is of the form $x^{-1}ax$ for some $x \in G$, and $f(C_a x) = x^{-1}ax$. Therefore, f is a bijection between the cosets of C_a and the conjugates of a.

13.I.6. The number of cosets of C_a in G is by definition $(G : C_a)$, and it is the same as the number of conjugates of a by the exercise above. Now if $|G|$ is finite, then by Lagrange's theorem we have $(G : C_a) \cdot |C_a| = |G|$, i.e. $(G : C_a)$ is a factor of $|G|$. Thus the number of conjugates of any $a \in G$ is a factor of $|G|$. (If $|G|$ is infinite, then it is awkward to say that a number is a factor of ∞...)

References

[Pin10] Pinter, C. C., *A Book of Abstract Algebra*, 2nd ed., Dover Publications, 2010.