Abstract Algebra I Homework 2

Carson Connard

Section 2.1

1 In each of (a)-(e), prove that the specified subset is a subgroup of the given group:

(a) The set of complex numbers of the form $a + ai$ for $a \in \mathbb{R}$ (under addition).

Solution. We want to show that $A := \{a + ai : a \in \mathbb{R}\} \leq (\mathbb{C}, +)$. Certainly A is nonempty, as $0 + 0i \in A$. Take two elements $a + ai, b + bi \in A$. Then by the Subgroup Criterion (Prop 2.1.1), we have

$$(a + ai) - (b + bi) = (a - b) + (a - b)i,$$

which certainly is contained in A. Therefore $A \leq (\mathbb{C}, +)$.

(b) The set of complex numbers of absolute value 1, i.e. the unit circle in the complex plane (under multiplication).

Solution. We want to show that $B := \{a + bi : a, b \in \mathbb{R}, |a + bi| = 1\} \leq (\mathbb{C}, \cdot)$. Certainly B is nonempty, as $|1 + 0i| = 1$. Take two elements $a + bi, c + di \in B$. Then certainly by definition, $a^2 + b^2 = c^2 + d^2 = 1$. Then by the Subgroup Criterion, we have

$$(a + bi)(c + di)^{-1} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{c^2 + d^2} = (ac + bd) + (bc - ad)i.$$

Notice that we have

$$\begin{aligned}(ac + bd)^2 + (bc - ad)^2 &= a^2c^2 + 2abcd + b^2d^2 + b^2c^2 - 2abcd + a^2d^2 \\ &= (a^2 + b^2)(c^2 + d^2) = 1.\end{aligned}$$

Therefore, $(ac + bd) + (bc - ad)i \in B$. So, we have that $B \leq (\mathbb{C}, \cdot)$

(c) For fixed $n \in \mathbb{Z}_+$ the set of rational numbers whose denominators divide n (under addition).

Solution. We want to show that $C_n := \{a/q \in \mathbb{Q} : q \mid n\} \leq (\mathbb{Q}, +)$. Certainly C_n is nonempty, as $0/1 = 0 \in C_n$. Now take $a/q, b/p \in C_n$. By definition, we have that $q \mid n$ and $p \mid n$. Take $g = (q, p)$, and let $q = kg$ and $p = lg$. Then

$$\frac{a}{q} - \frac{b}{p} = \frac{ap - bq}{qp} = \frac{alg - bkg}{kglg} = \frac{al - bk}{klg} = \frac{al - bk}{(q, p)}.$$

Since $(q, p) \mid n$, we have by the Subgroup Criterion that $C_n \leq (\mathbb{Q}, +)$.

(d) For fixed $n \in \mathbb{Z}_+$ the set of rational numbers whose denominators are relatively prime to n (under addition).

Solution. We want to show that $D_n := \{p/q \in \mathbb{Q} : (q, n) = 1\} \leq (\mathbb{Q}, +)$. Certainly D_n is nonempty since $0/1 = 0 \in D_n$. Now take $a/q, b/p \in D_n$. By definition, we have that $(q, n) = (p, n) = 1$. Now since $(p, n) = (q, n) = 1 \implies (pq, n)$, we have that

$$\frac{a}{q} - \frac{b}{p} = \frac{ap - bq}{qp}.$$

Therefore, by the Subgroup Criterion, we have that $D_n \leq (\mathbb{Q}, +)$.

(e) The set of nonzero real numbers whose square is a rational number (under multiplication).

Solution. We want to show that $E := \{a \in \mathbb{R} : a \neq 0, a^2 \in \mathbb{Q}\} \leq (\mathbb{R}, \cdot)$. Certainly, E is nonempty, as $1^2 \in \mathbb{Q}$. Now take $m^2 = a$ and $n^2 = b$ for $a, b \in \mathbb{Q}$. Then

$$(m/n)^2 = m^2/n^2 = a/b.$$

Since $a, b \in \mathbb{Q}$, we have that a/b is as well. Moreover, since $\mathbb{Q} \subset \mathbb{R}$, we have that $E \leq (\mathbb{R}, \cdot)$.

16 Let $n \in \mathbb{Z}_+$ and let F be a field. Prove that the set $T := \{(a_{ij} \in GL_n(F) : a_{ij} = 0 \ \forall i < j\}$ is a subgroup of $GL_n(F)$ (called the group of upper triangular matrices).

Proof. First notice that T is not empty, as the identity matrix is in T. Now consider $A, B \in T$. Then from linear algebra, since inverting a matrix maintains the position of elements in the 'lower' triangle (it negates them, however $-0 = 0$), we know that (without loss of generality) $B^{-1} \in T$. We claim that $AB^{-1} \in T$; indeed, we see that if $A = (a_{i,j})$ and $B^{-1} = (b_{i,j})$, we have that $AB^{-1} = (\sum_k a_{i,k} b_{k,j})$. Now suppose $i > j$, then if $k > j$, we have $b_{k,j} = 0$. Else if $k \leq j$, we have $a_{i,k} = 0$. Certainly $0 + 0 = 0$ and we have that $AB^{-1} \in T$. Then by the subgroup criterion, we have shown that $T \leq GL_n(\mathbb{F})$. □

Section 2.2

7 Let $n \in \mathbb{Z}_+$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = 1$ if n is odd.

Proof. Recall that D_{2n} has the presentation $\langle r, s : r^n = s^2, rs = sr^{-1} \rangle$. So, since $rs = sr^{-1}$, we know that $\{s, r, r^2, ..., r^{n-1}\} \notin Z(D_{2n})$. Also we see that since $(r^k s)s = r^k$ for all k but $s(r^k s) = s^2 r^{-k} = r^{-k}$. So, $r^k s \notin Z(D_{2n})$ for all $1 \leq k \leq n-1$. This exhausts all elements except for the identity, so $Z(D_{2n}) = \{1\}$ for n odd. □

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Proof. We have a similar situation for n even, except that now we see that $r^{n/2} s = sr^{n/2}$ since $r^{-n/2} = r^{n/2}$. So, considering the centralizer for n odd, we have that $\{1, r^{n/2}\} = Z(D_{2n})$. □

Section 2.3

3 Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Solution. Consider $\mathbb{Z}/48\mathbb{Z}$. Generators for $\mathbb{Z}/48\mathbb{Z}$ are the equivalence classes $[k]$ where $\gcd(k, 48) = 1$ (where $1 \leq k \leq 48$). Notice that $48 = 2^4 \cdot 3$. As such, let us consider all factors of 48 as a set, and remove those which are multiples of either 2 or 3:

$$A := \{1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 35,\ 37,\ 41,\ 43,\ 47\}$$

So, the generators of $\mathbb{Z}/48\mathbb{Z}$ are the equivalence classes $[a]$ for $a \in A$.

26 Let Z_n be a cyclic group of order n and for each integer a, define $\sigma_a : Z_n \to Z_n$ by $\sigma_a(x) = x^a$ for all $x \in Z_n$.

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.

Proof. ($\Longleftarrow$) Assume that $(a, n) = 1$. We want to show that σ_a is a bijective homomorphism. First, let us note that according to the problem statement of problem 2.3.25, we see that the mapping $\sigma_a(x) = x^a$ is a surjection. Since Z_n is a finite group, we have that σ_a is also injective. Consider now some $z_1, z_2 \in Z_n$, where $z_1 = x^i$ and $z_2 = x^j$. Then considering $(a, n) = 1$, we have that

$$\sigma_a(z_1 z_2) = (z_1 z_2)^a = (x^i x^j)^a = x^{ia+ja} = (x^i)^a (x^j)^a = \sigma_a(z_1)\sigma_a(z_2).$$

Thus, σ_a is indeed a bijective homomorphism, and by the definition of the map, it is an automorphism.

($\Longrightarrow$) Assume that σ_a is an automorphism of Z_n. We want to show that $(a, n) = 1$. Consider some $z \in Z_n$ such that z generates Z_n, then we have that $|\sigma_a(z)| = |z|$ as σ_a is certainly an injection. This implies that $Z_n = \langle z^a \rangle$, which by Proposition 2.3.6 gives that $(a, n) = 1$. □

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \mod n$.

Proof. ($\Longrightarrow$) Assume that $\sigma_a = \sigma_b$. We want to show that $a \equiv b \mod n$. Certainly $\sigma_a(x) = \sigma_b(x)$, therefore $x^a = x^b$. Now since we showed that σ_a is an automorphism, we have that $|x| = n$. As such, this shows that $a \equiv b \mod n$.

($\Longleftarrow$) Assume that $a \equiv b \mod n$. We want to show that $\sigma_a = \sigma_b$. We can rewrite our assumption as $a = b + kn$ for some $k \in \mathbb{Z}$. Then for all $x \in Z_n$, we have

$$\sigma_a(x) = x^a = x^{b+kn} = x^b = \sigma_b(x).$$

So, we have that $\sigma_a = \sigma_b$. □

(c) Prove that every automorphism of Z_n is equal to σ_a for some integer a.

Proof. Consider $\phi \in \text{Aut}(Z_n)$. Then $\phi(x) = x^k$ for some $k \in \mathbb{N}$ since $Z_n = \langle x \rangle$ as a result of part (a). Then we have for all $i \in \mathbb{Z}$:

$$\psi(x^i) = \phi(x)^i = x^{ki} = (x^i)^k = \sigma_k(a^i).$$

Since all elements of Z_n are of the form x^i, we have that $\phi = \sigma_a$, which proves our claim as ϕ was taken arbitrarily. $\square$

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\text{Aut}(Z_n)$ is an abelian group of order $\phi(n)$).

Proof. Consider a map $\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \text{Aut}(Z_n)$ defined by $\psi(\overline{a}) = \sigma_a$. By part (b), we see that ψ is a well-defined map. If we take some arbitrary $x \in Z_n$, we have the following:

$$(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x),$$

which gives that $\psi(\overline{a}\overline{b}) = \psi(\overline{a})\psi(\overline{b})$, which by definition means that ψ is a homomorphism. By part (c), we see that ψ is surjective, and since both $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\text{Aut}(Z_n)$ are finite, we have that ψ is injective. So, ψ is a bijective homomorphism, which by definition is an isomorphism. $\square$

Section 2.4

13 Prove that the multiplicative group of positive rational numbers is generated by the set $\{1/p : p \text{ prime}\}$.

Proof. First let us consider that by the fundamental theorem of arithmetic, we have that any $m \in \mathbb{Z}$ can be expressed as a product of primes p. As such, we can take the reciprocal and state that any $1/m$ for $m \in \mathbb{Z}$ can be expressed as a product of a's in A. We will take three cases: first, take

$$\frac{1}{m} = \left(\frac{1}{p_1}\right)^{n_1} \left(\frac{1}{p_2}\right)^{n_2} \cdots \left(\frac{1}{p_k}\right)^{n_k}.$$

Since $1/m$ is a product of powers of A, we know that $1/m$ is in the set generated by A, which we denote $\langle A \rangle$. Second, take

$$n = \left(\frac{1}{p_1}\right)^{-n_1} \left(\frac{1}{p_2}\right)^{n_2} \cdots \left(\frac{1}{p_k}\right)^{n_k}.$$

Again, since n is a product of powers of A, we know that $n \in \langle A \rangle$. Third, consider some $n/m \in \mathbb{Q}_+$. Since $n, 1/m \in \langle A \rangle$, we have that their product is $n/m \in \langle A \rangle$. We have shown that elements of all forms in $\mathbb{Q}_+$ are generated by A, and therefore $\mathbb{Q}_+ \leq \langle A \rangle$. Trivially, we also have that $\langle A \rangle \leq \mathbb{Q}_+$, and therefore $\langle A \rangle = \mathbb{Q}_+$. $\square$

Section 3.1

3 Let A be an abelian group and let $B \leq A$. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Proof. Take arbitrary $a_1, a_2 \in A$, and hence take arbitrary $a_1B, a_2B \in A/B$. Then since A is abelian, we have the following:

$$(a_1B)(a_2B) = a_1a_2B = a_2a_1B = (a_2B)(a_1B).$$

Since a_1B, a_2B are arbitrary elements of A/B, we see that A/B is abelian. $\square$

Consider the subgroup $H = \{1, -1, i, -i\} \leq Q_8$. Let us now take the normalizer, $N_G(H) = \{g \in G : gH = Hg\}$. Clearly this is just equivalent to Q_8, and therefore $H \trianglelefteq G$. But, note that $|Q_8| = 8$, $|H| = 4$, and therefore $|G/H| = 2$, and thus $G/H \cong \mathbb{Z}_2$, an abelian group.

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).

Proof. We know that some subgroup $H \leq G$ is normal if H is invariant under conjugation by members of G, that is $H \trianglelefteq G$ if and only if $ghg^{-1} \in H$ for all $g \in G, h \in H$. Let us consider some $a \in N$. Then we can express a as a product of commutators, that is $a = (x_1^{-1}y_1^{-1}x_1y_1)(x_2^{-1}y_2^{-1}x_2y_2)...(x_k^{-1}y_k^{-1}x_ky_k)$ for some k. Then if we take some arbitrary $g \in G$, we have:

$$\begin{aligned} g(x_i^{-1}y_i^{-1}x_iy_i)g^{-1} &= gx_i^{-1}y_i^{-1}x_iy_ig^{-1} \\ &= gx_i^{-1}g^{-1}gy_i^{-1}g^{-1}gx_ig^{-1}gy_ig^{-1} \\ &= (gx_i^{-1}g^{-1})(gy_i^{-1}g^{-1})(gx_ig^{-1})(gy_ig^{-1}) \\ &= (gx_ig^{-1})^{-1}(gy_ig^{-1})^{-1}(gx_ig^{-1})(gy_ig^{-1}) \end{aligned}$$

which is of the form of generating elements of N. So, we have that conjugation of a commutator is also a commutator. Therefore,

$$\begin{aligned} gag^{-1} &= g(x_1^{-1}y_1^{-1}x_1y_1)(x_2^{-1}y_2^{-1}x_2y_2)...(x_k^{-1}y_k^{-1}x_ky_k)g^{-1} \\ &= g(x_1^{-1}y_1^{-1}x_1y_1)g^{-1}g(x_2^{-1}y_2^{-1}x_2y_2)g^{-1}\cdots g(x_k^{-1}y_k^{-1}x_ky_k)g^{-1} \\ &= (gx_1^{-1}y_1^{-1}x_1y_1g^{-1})(gx_2^{-1}y_2^{-1}x_2y_2g^{-1})\cdots(gx_k^{-1}y_k^{-1}x_ky_kg^{-1}) \end{aligned}$$

As previously shown, each $(gx_i^{-1}y_i^{-1}x_iy_ig^{-1})$ is itself a commutator, and therefore $gag^{-1} \in N$. Since a was chosen arbitrarily, we have shown that a is invariant under conjugation, so therefore $N \trianglelefteq G$. □

Proof. We now want to show that G/N is abelian. By definition of quotient groups, we know that the elements of G/N are of the form gN. So, let us take arbitrary $x, y \in G$, and consider the commutator $x^{-1}y^{-1}xy$. Then we have

$$(xN)(yN) = xyN = xy(x^{-1}y^{-1}xy)N = yxN = (yN)(xN).$$

Therefore, we see that G/N is abelian. □

Section 3.2

11 Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$ (do not assume G is finite).

Proof. Recall that the index $|G : H|$ is the number of left cosets of H in G, where $H \leq G$, and similarly for $|G : K|$ and $|K : H|$. We can show our claim by showing that the map $\phi : G/H \times K/H \to G/H$ is bijective. Certainly this is well defined, as if we consider some element $k_2^{-1}k_1 \in H$, then $k_1H = k_2H$, so $gk_1H = gk_2H$, and therefore $\phi(g, k_1H) = \phi(g, k_2H)$. To show surjectivity, consider some $gH \in G/H$. Then $g \in g'K$ for some $g' \in G/H$, say in particular $g' = gh^{-1}$. Then we have that $\phi(g', kH) = gH$ as desired. To show injectivity, suppose that $\phi(g_1, k_1H) = \phi(g_2, k_2H)$. Then $g_1k_1H = g_2k_2H$, in particular $g_1k_1 \in g_2k_2H \subset g_2K$, which gives that $g_1 \in g_2K$ and therefore $g_2^{-1}g_1 \in K$. So we have that $g_1K = g_2K$ implies that $g_1 = g_2$. Therefore we have that $k_1H = k_2H$ as desired. So, we have shown bijectivity, and we are done. □

16 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem, that is if p is prime, then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.

Proof. Recall that Lagrange's Theorem states that if $H \leq G$ for G finite, then $|H|$ divides $|G|$ and the number of left cosets $|G : H| = |G|/|H|$. So, take $G = (\mathbb{Z}/p\mathbb{Z})^\times$, and notice that $|G| = p - 1$, as the order of a group is simply the number of generators of the group; for p prime and the binary operation $(\times)$, we have that this number is $p-1$ since [1] is not a generator. Now take some $a \in G$. Then we can construct the set $H = \{a, a^2, ..., a^k\}$ where $k = |a|$, and we claim that $H \leq G$. Indeed, we have that (1) $1 \in H$, as by definition of order, $a^k \equiv 1 \mod p$, therefore $a^k = 1 \in H$; we have that (2) inverses are in H since for $n \leq k$, we have that $a^{k-n} \in H$, and therefore $a^n \cdot a^{k-n} = a^k \equiv 1 \mod p$; and we have that (3) compositions of elements are contained in H, that is $a^n \cdot a^m \in H$, since $a^n \cdot a^m = a^{n+m}$ (this is clear for $n + m \leq k$, otherwise $n + m$ "rolls around", that is $n + m = qk + r$ for $q \in \mathbb{N}$, and certainly $a^r \in H$ for $r < k$). So indeed, $H \leq G$. Now consider that $|H| = k$. By Lagrange's Theorem, we know that $|H|$ divides $|G|$, that is $k \mid p - 1$, which by definition means that there exists some $x \in \mathbb{Z}$ such that $p - 1 = kx$. So, we have now that

$$a^{p-1} = a^{kx} = (a^k)^x \equiv 1^x \mod p \equiv 1 \mod p.$$

Certainly, $a^{p-1} \equiv 1 \mod p$ is an equivalent statement to $a^p \equiv a \mod p$, so we are done. □