1.9.6

The cyclic group of order 6 is the group defined by generators a, b and relations $a^2 = b^3 = a^{-1}b^{-1}ab = e$.

Proof. Let $X = \{a, b\}$ and let $F(X)$ be the free group on X. Consider the normal subgroup N of $F(X)$ generated by the relations $a^2 = e$, $b^3 = e$, and $a^{-1}b^{-1}ab = e$. Then $G \cong F(X)/N$.

We claim that G is cyclic of order 6, i.e., $G \cong \mathbb{Z}/6\mathbb{Z}$. The relation $a^{-1}b^{-1}ab = e$ implies $ab = ba$, so G is abelian. The relations $a^2 = e$ and $b^3 = e$ show that the orders of a and b are 2 and 3, respectively.

Since G is abelian and generated by a and b, every element of $F(X)/N$ can be written as $a^i b^j N$ for $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$, giving $2 \times 3 = 6$ elements, so $|G| \leq 6$.

Define a homomorphism $\varphi : F(X)/N \to \mathbb{Z}/6\mathbb{Z}$ by $\varphi(a) = 3$ and $\varphi(b) = 2$. This is well-defined since $3 + 3 = 0$ and $2 + 2 + 2 = 0$ in $\mathbb{Z}/6\mathbb{Z}$, matching the relations. The commutativity also matches the structure of $\mathbb{Z}/6\mathbb{Z}$.

Since φ is surjective and $|F(X)/N| \leq 6$, it follows that $|F(X)/N| = 6$ and φ is an isomorphism. Thus, $G \cong F(X)/N \cong \mathbb{Z}/6\mathbb{Z}$, as claimed. □

1.9.10

The operation of free product is commutative and associative: for any groups $A, B, C, A * B \cong B * A$ and $(A * B) * C \cong A * (B * C)$.

Proof. Let A, B, C be groups. First, we show that $A * B \cong B * A$. The free product $A * B$ consists of all reduced words formed by alternating elements from A and B, and the same holds for $B * A$. Therefore we can define a homomorphism $\varphi : A * B \to B * A$ where φ is the identity map. The correspondence that sends each reduced word in $A * B$ to the same word in $B * A$ (just swapping the roles of A and B). Clearly we have that φ is surjective. To see that φ is injective, note that if $\varphi(w) = e$ in $B * A$, then w must be the empty word in $A * B$, since the only way for a reduced word to map to the identity is if it is itself the identity. Thus, $\ker(\varphi) = \{e\}$, so φ is injective. Thus, $A * B \cong B * A$.
Next, we show that $(A * B) * C \cong A * (B * C)$. We know that $(A * B) * C$ consists of reduced words alternating among $A * B$ and C, but each letter from $A * B$ is itself a reduced word in A and B. By flattening, every element of $(A * B) * C$ can be written as a reduced word in A, B, and C, with no two consecutive letters from the same group. Likewise, $A * (B * C)$ consists of reduced words alternating among A and $B * C$, and each letter from $B * C$ is a reduced word in B and C. Again, flattening yields reduced words in A, B, and C, with no two consecutive letters from the same group. Define a map $\Phi : (A * B) * C \to A * (B * C)$ as follows: Given a reduced word w in $(A * B) * C$, write w as a sequence of letters $x_1 x_2 \cdots x_n$, where each x_i is either a non-identity element from $A * B$ or C. If x_i is from $A * B$, further decompose it into its reduced word in A and B. Concatenate all these letters to obtain a reduced word in A, B, and C. This word is then interpreted as an element of $A * (B * C)$. Similarly, define the inverse map $\Psi : A * (B * C) \to (A * B) * C$ by grouping consecutive letters from A and B into elements of $A * B$, and letters from C as elements of C, thus forming a reduced word in $(A * B) * C$. To see that Φ and Ψ are well-defined, note that the process of flattening and grouping preserves the reduced word property: no two consecutive letters come from the same group, and the group operation is respected. It is clear that Φ and Ψ are inverses of each other, since flattening and grouping are mutually inverse operations. Therefore, Φ is a bijection. Hence, $(A * B) * C \cong A * (B * C)$.
Hence, the free product is both commutative and associative. □

1.9.11

If N is the normal subgroup of $A * B$ generated by A, then $(A * B)/N \cong B$.

Proof. Let N be the normal subgroup of $A * B$ generated by A. We want to show that $(A * B)/N \cong B$.

The subgroup N is the smallest normal subgroup containing all elements of A, so in the quotient $(A * B)/N$, every element of A becomes identified with the identity. In other words, for any $a \in A$, $aN = N$ in the quotient.

Now, consider any element $w \in A * B$. We can write w as a reduced word $x_1 x_2 \cdots x_n$, where each x_i is either in A or B. In the quotient $(A * B)/N$, any occurrence of $x_i \in A$ can be replaced by the identity, since $x_i N = N$. Therefore, wN is equal to the product of all the x_i that are in B, with all A-letters removed. This product is simply an element of B, since the group operation in B is preserved.

Thus, every coset in $(A * B)/N$ can be uniquely represented by an element bN for some $b \in B$. The identity coset is N, which corresponds to the identity element e_B in B.

Define a map $\varphi : (A * B)/N \to B$ by $\varphi(bN) = b$ for $b \in B$. To see that φ is well-defined, note that every element of $(A * B)/N$ is of the form bN for a unique $b \in B$, as shown above.

Next, we check that φ is a homomorphism. For any $b_1, b_2 \in B$,

$$\varphi(b_1N \cdot b_2N) = \varphi(b_1b_2N) = b_1b_2 = \varphi(b_1N)\varphi(b_2N).$$

So φ preserves the group operation.

To see that φ is surjective, observe that for any $b \in B$, bN is a coset in $(A * B)/N$, and $\varphi(bN) = b$.

To check injectivity, suppose $\varphi(b_1N) = \varphi(b_2N)$. Then $b_1 = b_2$, so $b_1N = b_2N$.

Therefore, φ is a well-defined isomorphism. Thus we conclude that $(A * B)/N \cong B$. □

1.9.12

If G and H each have more than one element, then $G * H$ is an infinite group with center $< e >$.

Proof. Let G and H be groups, each with more than one element. We want to show that their free product $G * H$ is infinite and that its center is trivial.

First, we show that $G * H$ is infinite. Since both G and H have more than one element, pick $g \in G$ and $h \in H$ with $g \neq e_G$ and $h \neq e_H$. Consider the sequence of words $w_n = (gh)^n$ for $n \geq 1$. Each w_n is a reduced word of length $2n$, and no two such words are equal in $G * H$ because the free product imposes no relations between g and h other than those in their respective groups. Thus, for every n, w_n is distinct, and we can construct arbitrarily long reduced words. Therefore, $G * H$ is infinite.

Next, we show that the center of $G * H$ is trivial. Recall that the center $Z(G * H)$ consists of all elements $z \in G * H$ such that $zw = wz$ for all $w \in G * H$. Clearly, the identity element e is in the center. Suppose z is a nontrivial reduced word in $G * H$. We will show that z cannot commute with all elements of $G * H$.

Let z be a reduced word of length $k \geq 1$, say $z = x_1x_2 \cdots x_k$, where each x_i is in G or H, and consecutive x_i are from different groups. Without loss of generality, suppose $x_k \in H$. Pick $h \in H$ with $h \neq e_H$ and $h \neq x_k^{-1}$. Consider the element $w = h$. Then,

$$zw = x_1x_2 \cdots x_kh$$

is a reduced word ending with x_kh (which is not the identity since $h \neq x_k^{-1}$). On the other hand,

$$wz = hx_1x_2 \cdots x_k$$

is a reduced word starting with h, which is distinct from zw because the reduced word structure is different. Thus, $zw \neq wz$. A similar argument applies if $x_k \in G$ by choosing $g \in G$ with $g \neq e_G$ and $g \neq x_k^{-1}$.

Therefore, the only element that commutes with all elements of $G * H$ is the identity. Thus, the center of $G * H$ is trivial:

$$Z(G * H) = \langle e \rangle.$$

□

1.9.15

If $f : G_1 \to G_2$ and $g : H_1 \to H_2$ are homomorphisms of groups, then there is a unique homomorphism $h : G_1 * H_1 \to G_2 * H_2$ such that $h|_{G_1} = f$ and $h|_{H_1} = g$.

Proof. Let $f : G_1 \to G_2$ and $g : H_1 \to H_2$ be group homomorphisms. We wish to construct a homomorphism $h : G_1 * H_1 \to G_2 * H_2$ such that $h|_{G_1} = f$ and $h|_{H_1} = g$, and show that it is unique.

Recall that every element of the free product $G_1 * H_1$ can be written uniquely as a reduced word $a_1a_2 \cdots a_n$, where each a_i is a non-identity element from either G_1 or H_1, and consecutive a_i are from different groups. The empty word corresponds to the identity element.

Define $h : G_1 * H_1 \to G_2 * H_2$ as follows:

- For $g \in G_1$, set $h(g) = f(g)$.
- For $h_1 \in H_1$, set $h(h_1) = g(h_1)$.
- For a reduced word $a_1a_2 \cdots a_n$ in $G_1 * H_1$, where each a_i is in G_1 or H_1, define

$$h(a_1a_2 \cdots a_n) = h(a_1)h(a_2) \cdots h(a_n).$$

- For the identity element (the empty word), set $h(e) = e$.

We first verify that h is a homomorphism. Let $w = a_1a_2\cdots a_n$ and $w' = b_1b_2\cdots b_m$ be reduced words in $G_1 * H_1$. The product ww' is obtained by concatenating the words, and if the last letter of w and the first letter of w' are from the same group, their product is taken in that group and the result is reduced accordingly. Since f and g are homomorphisms, h respects the group operations within G_1 and H_1, and the concatenation of images under h corresponds to the product in $G_2 * H_2$, with reduction occurring in the same way. Thus,

$$h(ww') = h(a_1a_2\cdots a_nb_1b_2\cdots b_m) = h(a_1)h(a_2)\cdots h(a_n)h(b_1)h(b_2)\cdots h(b_m) = h(w)h(w').$$

Therefore, h is a homomorphism.

Next, we check that h restricts to f on G_1 and to g on H_1. For any $g \in G_1$, $h(g) = f(g)$ by definition, and for any $h_1 \in H_1$, $h(h_1) = g(h_1)$. Thus, $h|_{G_1} = f$ and $h|_{H_1} = g$.

Finally, we show that h is unique with these properties. Suppose $h' : G_1 * H_1 \to G_2 * H_2$ is another homomorphism such that $h'|_{G_1} = f$ and $h'|_{H_1} = g$. For any reduced word $a_1a_2\cdots a_n$ in $G_1 * H_1$, we have

$$h'(a_1a_2\cdots a_n) = h'(a_1)h'(a_2)\cdots h'(a_n).$$

But $h'(a_i) = f(a_i)$ if $a_i \in G_1$, and $h'(a_i) = g(a_i)$ if $a_i \in H_1$, which matches the definition of $h(a_i)$. Therefore,

$$h'(a_1a_2\cdots a_n) = h(a_1)h(a_2)\cdots h(a_n) = h(a_1a_2\cdots a_n).$$

Thus, $h' = h$ on all elements of $G_1 * H_1$, so h is unique.

In summary, there exists a unique homomorphism $h : G_1 * H_1 \to G_2 * H_2$ such that $h|_{G_1} = f$ and $h|_{H_1} = g$. □

2.1.10

(a) Show that the additive group of rationals $\mathbb{Q}$ is not finitely gentertated.

(b) Show that $\mathbb{Q}$ is not free.

(c) Conclude that Exercise 9 is false if the hypothesis "finitely generated" is omitted.

(a) *Proof.* Suppose, for contradiction, that $\mathbb{Q}$ is finitely generated as an abelian group. That is, there exist finitely many elements $q_1, q_2, \ldots, q_n \in \mathbb{Q}$ such that every rational number can be written as an integer linear combination of these generators. Write each q_i in lowest terms as $q_i = \frac{a_i}{b_i}$, where $a_i \in \mathbb{Z}$, $b_i \in \mathbb{N}$, and $\gcd(a_i, b_i) = 1$.

Let $k = b_1b_2\cdots b_n$ be the product of all denominators. Consider the subgroup $H = \langle q_1, q_2, \ldots, q_n\rangle \leq \mathbb{Q}$. Any element $q \in H$ can be written as an integer linear combination:

$$q = d_1q_1 + d_2q_2 + \cdots + d_nq_n = \frac{d_1a_1}{b_1} + \frac{d_2a_2}{b_2} + \cdots + \frac{d_na_n}{b_n}$$

for some $d_1, \ldots, d_n \in \mathbb{Z}$. By clearing denominators, we can write this sum as a single fraction with denominator k:

$$q = \frac{d_1a_1\frac{k}{b_1} + d_2a_2\frac{k}{b_2} + \cdots + d_na_n\frac{k}{b_n}}{k}$$

Thus, every element of H is a rational number whose denominator divides k; in other words, $H \subseteq \left\langle \frac{1}{k}\right\rangle$, the subgroup of $\mathbb{Q}$ consisting of all rational numbers with denominator dividing k.

However, $\mathbb{Q}$ contains elements such as $\frac{1}{k+1}$, which cannot be written as an integer linear combination of elements with denominator k. Therefore, $\langle q_1, \ldots, q_n\rangle$ cannot be all of $\mathbb{Q}$, contradicting our assumption that $\mathbb{Q}$ is finitely generated.

Hence, the additive group of rationals $\mathbb{Q}$ is not finitely generated. □

(b) *Proof.* Assume $\mathbb{Q}$ were free, say with a generating set X. Let $\iota : X \to \mathbb{Q}$ be the inclusion map. Define $f : X \to \mathbb{Z}$ by $f(x) = 1$ for all $x \in X$. By the universal property of free abelian groups, there exists a unique homomorphism $\varphi : \mathbb{Q} \to \mathbb{Z}$ such that $\varphi \circ \iota = f$. Then, see that $\varphi(\iota(x)) = f(x) = 1$ for all $x \in X$. Since φ is a homomorphism, for any $q \in \mathbb{Q}$, which can be expressed as a finite integer linear combination of elements from X, we have

$$\varphi(q) = \varphi\left(\sum_{i=1}^{n} d_ix_i\right) = \sum_{i=1}^{n} d_i\varphi(x_i) = \sum_{i=1}^{n} d_i.$$

However, this implies that $\varphi(q)$ is always an integer, which contradicts the fact that $\mathbb{Q}$ contains elements that cannot be mapped to integers in a way that preserves the group structure. For example, consider $q = \frac{1}{2}$. There is no integer n such that $\varphi\left(\frac{1}{2}\right) = n$ while still satisfying the homomorphism property for all elements of $\mathbb{Q}$. Thus, φ cannot be well-defined for all of $\mathbb{Q}$, contradicting the assumption that $\mathbb{Q}$ is free. Therefore, $\mathbb{Q}$ is not a free abelian group. □

(c) Sine $\mathbb{Q}$ is an abelian group where no element (except 0) has finite order, exercise 9 does not hold. This is the case as in (a) we showed that $\mathbb{Q}$ is not finitely generated, and in (b) we showed that $\mathbb{Q}$ is not free. Thus, the hypothesis "finitely generated" is necessary for exercise 9 to hold.

Problem 1

(Algebra Qual, Jan 2016) Let D_k be the dihedral group of order $2k$, where $k \geq 3$.

(a) Show that the number of automorphisms of the grouop D_k is equal to $k \cdot \varphi(k)$. Here φ is the Euler φ-function.

(b) Automorphisms of D_k form a group; let us denote it by $\text{Aut}(D_k)$. What is the structure of $\text{Aut}(D_k)$? Describe the group as explicitly as you can.

(a) *Proof.* Recall that D_k is generated by two elements r and s with relations $r^k = s^2 = e$ and $srs = r^{-1}$. The element r represents a rotation by $\frac{2\pi}{k}$ radians, and s represents a reflection.

An automorphism $\varphi \in \text{Aut}(D_k)$ is determined by its action on the generators r and s. Since φ must preserve the order of elements, we have: - $\varphi(r)$ must be an element of order k. The elements of order k in D_k are precisely the powers of r, i.e., $\{r^m : 1 \leq m < k, \gcd(m,k) = 1\}$. There are $\varphi(k)$ such elements. - $\varphi(s)$ must be an element of order 2. The elements of order 2 in D_k are the reflections, which can be written as sr^j for $0 \leq j < k$. There are exactly k such elements.

Therefore, for each choice of $\varphi(r) = r^m$ (with $\gcd(m,k) = 1$), there are k choices for $\varphi(s)$. Thus, the total number of automorphisms is given by:

$$|\text{Aut}(D_k)| = k \cdot \varphi(k).$$

□

(b) The automorphism group $\text{Aut}(D_k)$ of the dihedral group D_k can be understood by analyzing how automorphisms act on the generators of D_k. Recall that D_k is generated by a rotation r of order k and a reflection s of order 2, with the relation $srs^{-1} = r^{-1}$.

Any automorphism must send r to another element of order k, which must be some power r^a where a is coprime to k (i.e., $a \in (\mathbb{Z}/k\mathbb{Z})^\times$). Similarly, s can be sent to $r^b s$ for some $b \in \mathbb{Z}/k\mathbb{Z}$, since $r^b s$ is also a reflection.

The set of possible choices for a forms the group $(\mathbb{Z}/k\mathbb{Z})^\times$, and the choices for b form the group $\mathbb{Z}/k\mathbb{Z}$. However, the way a and b interact is not independent: the choice of a affects how b acts, so the automorphism group is not a direct product, but a semidirect product.

Therefore, we have:

$$\text{Aut}(D_k) \cong (\mathbb{Z}/k\mathbb{Z})^\times \ltimes \mathbb{Z}/k\mathbb{Z}$$

where $(\mathbb{Z}/k\mathbb{Z})^\times$ acts on $\mathbb{Z}/k\mathbb{Z}$ by multiplication.

Problem 2

(Algebra Qual, Aug 2018) For a finite group G, denote by $s(G)$ the number of its subgroups.

(a) Show that $s(G)$ is finite.

(b) Show that if H is a nontrivial subgroup of G, then $s(G/H) < s(G)$.

(c) Show that $s(g) = 2$ if and only if G is a cyclic of prime order.

(d) Show that $s(G) = 3$ if and only if G is cyclic group whose order is a square of a prime.

Let G be a finite group.

(a) *Proof.* Since G is finite, it has a finite number of elements. Any subgroup $H \leq G$ is determined by a subset of G that is closed under the group operation and taking inverses. The number of subsets of a finite set with n elements is 2^n, which is finite. Since not all subsets are subgroups, the number of subgroups $s(G)$ is at most $2^{|G|}$, which is finite. Therefore, $s(G)$ is finite. □

(b) *Proof.* Let H be a nontrivial subgroup of G. Consider the quotient group G/H. There is a natural correspondence between the subgroups of G/H and the subgroups of G that contain H. Specifically, if K/H is a subgroup of G/H, then K is a subgroup of G containing H. Conversely, if K is a subgroup of G containing H, then K/H is a subgroup of G/H. This correspondence is bijective.

Since H is nontrivial, there exists at least one subgroup of G that contains H, namely H itself. However, not all subgroups of G contain H. Therefore, the number of subgroups of G/H is strictly less than the number of subgroups of G. Hence, we have:

$$s(G/H) < s(G).$$

□

(c) *Proof.* ($\Rightarrow$) Suppose $s(G) = 2$. The only subgroups of G are the trivial subgroup $\langle e \rangle$ and G itself. Then for any $g \in G$ with $g \neq e$, the subgroup $\langle g \rangle$ generated by g must be either $\langle e \rangle$ or G. Since $g \neq e$, we have $\langle g \rangle = G$. Thus, G is cyclic and generated by any of its non-identity elements. Now, if the order of G were composite, say $|G| = mn$ with $m, n > 1$, then G would have a subgroup of order m (by Cauchy's theorem), contradicting the assumption that $s(G) = 2$. Therefore, the order of G must be prime. Hence, $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.

($\Leftarrow$) Conversely, if $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p, then the only subgroups of G are $\langle e \rangle$ and G itself. Thus, $s(G) = 2$.

Hence, we conclude that $s(G) = 2$ if and only if G is cyclic of prime order. □

(d) *Proof.* We prove both directions.

($\Rightarrow$) Suppose G is a cyclic group of order p^2 for some prime p. Then $G \cong \mathbb{Z}/p^2\mathbb{Z}$, and every subgroup of G is cyclic. The subgroups of a cyclic group of order n correspond to the divisors of n. For $n = p^2$, the divisors are 1, p, and p^2. Thus, the subgroups are:

- The trivial subgroup $\langle e \rangle$ of order 1,
- The subgroup $\langle a^p \rangle$ of order p, where a is a generator of G,
- The whole group G itself, of order p^2.

There are no other divisors of p^2, so these are the only subgroups. Therefore, $s(G) = 3$.

($\Leftarrow$) Now suppose G is a finite group with $s(G) = 3$. That is, G has exactly three subgroups: the trivial subgroup, G itself, and one proper nontrivial subgroup H. We claim that G must be cyclic of order p^2 for some prime p.

First, note that every group has the trivial subgroup and itself as subgroups, so the only possibility for $s(G) = 3$ is that there is exactly one proper nontrivial subgroup H. Consider any $a \in G$ with $a \neq e$. The subgroup $\langle a \rangle$ generated by a is a subgroup of G. Since $s(G) = 3$, every non-identity element must generate either G or H. If a generates G, then G is cyclic. If a generates H, then H must be cyclic as well.

Suppose G is not cyclic. Then for every $a \neq e$, $\langle a \rangle$ is a proper subgroup, so must be H. But then H contains all non-identity elements of G, so $H = G$, which is a contradiction. Therefore, G must be cyclic.

Let $|G| = n$. Suppose $n = pq$ for distinct primes p and q. Then G would have subgroups of orders p and q, contradicting the assumption that there is only one proper nontrivial subgroup. Thus, n must be a power of a single prime, say $n = p^k$. If $k \geq 3$, then G would have subgroups of orders p and p^2, again contradicting the assumption. Hence, k must be 1 or 2. If $k = 1$, then G is cyclic of prime order, which has $s(G) = 2$. Thus, k must be 2.

Therefore, G is cyclic of order p^2 for some prime p.

Thus, as desired, $s(G) = 3$ if and only if G is cyclic of order p^2 for some prime p. □