Problem 1 (3.1.4). Prove that in the quotient group G/N, $(qN)^{\alpha} = q^{\alpha}N$ for all $\alpha \in \mathbb{Z}$.

Proof. First take $\alpha > 0$. Since G/N is a group we have $(gN)^{\alpha} = gN \cdot gN \cdot \dots \cdot gN$ where there are α gNs. From the generalized associative property and the fact that $gN \cdot gN = (g \cdot g)N$, this reduces to $(g \cdot g \cdot \dots \cdot g)N = g^{\alpha}N$. For $\alpha = 0$ we get $(gN)^0 = N = 1N = g^0N$. Finally, if $\alpha < 0$ then again since G/N is a group we have $(gN)^{\alpha} = ((gN)^{-\alpha})^{-1} = (g^{-\alpha}N)^{-1} = (g^{-\alpha})^{-1}N = g^{\alpha}N$.

Problem 2 (3.1.5). Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Proof. Let n be as defined. We know $g^n \in N$ which means $g^n N = N$. Then using Problem 1, $N = g^n N = (gN)^n$. Since n is the smallest positive integer such that this is true, we must have |gN| = n. If no such n exists, then $g^n \notin N$ for all positive n. Therefore $g^n N \neq N$ for all positive n and thus $|gN| = \infty$.

As an example, let $G = D_8$ and $N = \langle r \rangle$. Then |r| = 4 in G, and |rN| = 1.

Problem 3 (3.1.16). Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that if $G = \langle x, y \rangle$ then $\overline{G} = \langle \overline{x}, \overline{y} \rangle$. Prove more generally that if $G = \langle S \rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S} \rangle$.

Proof. Let $S = \{a_1, \ldots, a_n\}$ be a subset of G such that $G = \langle S \rangle$. Let $\overline{x} \in \overline{G}$. Since $G = \langle S \rangle$ we can write $\overline{x} = a_1^{i_1} a_2^{i_2} \ldots a_n^{i_n}$. Using the generalized associative principle this reduces to $\overline{a_1^{i_1} a_2^{i_2} \ldots a_n^{i_n}}$. Thus any element of \overline{G} can be written as a product of powers of elements in \overline{S} . Therefore $\overline{G} = \langle \overline{S} \rangle$. In particular, if $S = \{x, y\}$ then $G = \langle x, y \rangle$ and $\overline{G} = \langle \overline{x}, \overline{y} \rangle$.

Problem 4 (3.1.17). Let G be the dihedral group of order 16:

$$G = \langle r, s \mid r^8 = s^2 = 1, rs = sr^{-1} \rangle$$

and let $\overline{G} = G/\langle r^4 \rangle$ be the quotient of G by the subgroup generated by r^4 (this subgroup is the center of G, hence is normal).

- (a) Show that the order of \overline{G} is 8.
- (b) Exhibit each element of \overline{G} in the form $\overline{s}^a \overline{r}^b$, for some integers a and b.
- (c) Find the order of each of the elements of \overline{G} exhibited in (b).
- $\underline{(d)}$ Write each of the following elements of \overline{G} in the form $\overline{s}^a \overline{r}^b$, for some integers a and b as in (b): \overline{rs} , $\overline{sr^{-2}s}$, $\overline{s^{-1}r^{-1}sr}$.
- (e) Prove that $\overline{H} = \langle \overline{s}, \overline{r}^2 \rangle$ is a normal subgroup of \overline{G} and \overline{H} is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of \overline{H} in G.
- (f) Find the center of \overline{G} and describe the isomorphism type of $\overline{G}/Z(\overline{G})$.

Proof. (a) From Lagrange's Theorem, $|\overline{G}| = |G|/|\langle r \rangle| = 16/2 = 8$.

(b) We have

$$\begin{split} \overline{G} &= \{x\langle r^4\rangle \mid x \in G\} \\ &= \{\langle r^4\rangle, r\langle r^4\rangle, r^2\langle r^4\rangle, r^3\langle r^4\rangle, s\langle r^4\rangle, sr\langle r^4\rangle, sr^2\langle r^4\rangle, sr^3\langle r^4\rangle\} \\ &= \{\langle r^4\rangle, r\langle r^4\rangle, (r\langle r^4\rangle)^2, (r\langle r^4\rangle)^3, s\langle r^4\rangle, s\langle r^4\rangle r\langle r^4\rangle, s\langle r^4\rangle (r\langle r^4\rangle)^2, s\langle r^4\rangle (r\langle r^4\rangle)^3\} \\ &= \{\overline{1}, \overline{r}, \overline{r}^2, \overline{r}^3, \overline{s}, \overline{sr}, \overline{sr}^2, \overline{sr}^3\} \end{split}$$

- (c) Using Problem 1 and the fact that $\langle r^4 \rangle = \{1, r^4\}$, we have $|\overline{1}| = 1$, $|\overline{r}| = 4$, $|\overline{r}^2| = 2$, $|\overline{s}r^3| = 4$, $|\overline{s}| = 2$, $|\overline{s}r^2| = 2$, $|\overline{s}r^3| = 2$.
 - (d) We have $\overline{rs} = \overline{rs}$, $\overline{sr^{-2}s} = \overline{r^2s^2} = \overline{r^2}$ and $\overline{s^{-1}r^{-1}sr} = \overline{sr^{-1}sr} = \overline{rssr} = \overline{r^2}$.

(e) Note that since $\langle r^4 \rangle \subseteq H$ we have $\langle r^4 \rangle \subseteq H$ and so the Third Isomorphism Theorem applies. That is, $H/\langle r \rangle \leq G/\langle r \rangle$. Now note that $\overline{H} = \{\overline{s}, \overline{r}^2, \overline{sr}^2, \overline{1}\}$. From part (c) we know that each of the nonidentity elements has order 2. Furthermore, $\overline{s} \cdot \overline{r}^2 = \overline{sr}^2$, $\overline{r}^2 \cdot \overline{s} = \overline{sr}^{-2} = \overline{sr}^6 = \overline{sr}^2$, $\overline{s} \cdot \overline{sr}^2 = \overline{r}^2$, $\overline{s} \cdot \overline{sr}^2 = \overline{sr}^2 = \overline{sr}^2$, $\overline{r}^2 \cdot \overline{sr}^2 = \overline{sr}^{-2} \overline{r}^2 = \overline{s}$ and $\overline{sr}^2 \cdot \overline{r}^2 = \overline{sr}^4 = \overline{s}$. We've shown that all the relations hold for \overline{H} being isomorphic the the Klein 4-group.

The preimage of \overline{H} in G is $\{1, r^4, s, sr^4, r^2, r^6, sr^2, sr^6\}$. Renaming r^2 as r we see that $r^4 = s^2 = 1$ and $rs = sr^{-1}$. Thus the preimage of \overline{H} in G is isomorphic to D_8 .

(f) We know $\overline{r}, \overline{s} \notin Z(\overline{G})$ since $\overline{sr} = \overline{r}^{-1}\overline{s}$. The same applies to \overline{r}^3 . Multiplying s by sr^i results in r^i and so these elements are not in $Z(\overline{G})$ either. This only leaves \overline{r}^2 , which obviously commutes with \overline{r} and \overline{r}^3 . Now consider $\overline{r}^2(\overline{sr}^i) = \overline{sr}^{-2+i} = (\overline{sr}^i)\overline{r}^2$. Thus $Z(\overline{G}) = \{\overline{1}, \overline{r}^2\}$. We also have $\overline{G}/Z(\overline{G}) \cong V_4$. This can be seen by noticing $\overline{\overline{r}}^2 = \overline{\overline{r}}^2 = \overline{\overline{1}}$, $\overline{\overline{s}}^2 = \overline{\overline{1}}$ and $\overline{\overline{sr}}^2 = \overline{\overline{sr}}^2 = \overline{\overline{1}}$, and all the elements commute with each other. \square

Problem 5 (3.1.21). Let $G = Z_4 \times Z_4$ be given in terms of the following generators and relations:

$$G = \langle x, y \mid x^4 = y^4 = 1, xy = yx \rangle.$$

Let $\overline{G} = G/\langle x^2y^2\rangle$ (note that every subgroup of the abelian group G is normal).

- (a) Show that the order of \overline{G} is 8.
- (b) Exhibit each element of \overline{G} in the form $\overline{x}^a \overline{y}^b$, for some integers a and b.
- (c) Find the order of each of the elements of \overline{G} exhibited in (b).
- (d) Prove that $\overline{G} \cong Z_4 \times Z_2$.

Proof. (a) Let $N = \langle x^2 y^2 \rangle$. From Lagrange's Theorem we know $|\overline{G}| = |G|/|N| = 16/2 = 8$.

(b) We have

$$\overline{G} = \{N, xN, x^2N, x^3N, yN, yxN, yx^2N, yx^3N\} = \{\overline{1}, \overline{x}, \overline{x}^2, \overline{x}^3, \overline{y}, \overline{yx}, \overline{yx}^2, \overline{yx}^3\}.$$

- (c) We have $|\overline{1}|=1$, $|\overline{x}|=4$, $|\overline{x}^2|=2$, $|\overline{x}^3|=4$, $|\overline{y}|=4$, $|\overline{y}\overline{x}|=2$, $|\overline{y}\overline{x}^2|=4$, $|\overline{y}\overline{x}^3|=4$. (d) Let $Z_4\times Z_2=\langle a,b\mid a^2=b^4=1,ab=\underline{ba}\rangle$. Let $\phi:\overline{G}\to Z_4\times Z_2$ be a function such that $\phi(\overline{x})=b$ and $\phi(\overline{y}\overline{x}^3)=a$. Note that $|\overline{x}|=|b|=4$ and $|\overline{y}\overline{x}^3|=|a|=2$. Furthermore, $\overline{G}=\langle \overline{x},\overline{y}\overline{x}^3\rangle$. To see this, note that $\overline{x}^i \overline{y}^j = (\overline{y} \overline{x}^3)^j (\overline{x})^{-3j+i}$. Since the generators of \overline{G} are mapped to the generators of $Z_4 \times Z_2$ and these groups have the same order, we see ϕ preserves the group structure. Injectivity and surjectivity also follow from this fact and we see that $\overline{G} \cong Z_4 \times Z_2$. \Box

Problem 6 (3.1.24). Prove that if $N \subseteq G$ and H is any subgroup of G then $N \cap H \subseteq H$.

Proof. Let $h \in H$ and let $x \in N \cap H$. Then we have $hxh^{-1} \in N$ since $N \triangleleft G$ and $hxh^{-1} \in H$ since $H \triangleleft G$. Therefore $h(N \cap H)h^{-1} \subseteq N \cap H$ for all $h \in H$. Thus $(N \cap H) \subseteq H$.

Problem 7 (3.1.31). Prove that if $H \leq G$ and N is a normal subgroup of H then $H \leq N_G(N)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal (i.e., is the join of all subgroups H for which $N \triangleleft H$).

Proof. Since $N \subseteq H$, for all $h \in H$ we have $hNh^{-1} = N$. But then $H \subseteq \{g \in G \mid gNg^{-1} = N\} = N_G(N)$. Since this fact is true for any subgroup H for which $N \leq H$, we see that $N_G(N)$ is the join of all such subgroups.

Problem 8 (3.1.36). Prove that if G/Z(G) is cyclic then G is abelian.

Proof. Assume that G/Z(G) is cyclic with generator xZ(G). The left cosets of G/Z(G) partition G, so for $u \in G$, we know $u \in (xZ(G))^a = x^a Z(G)$ for some integer a. But this means we can write $u = x^a z$ for $z \in Z(G)$. Now take $u, v \in G$. Since Z(G) is the set of elements of G which commute with every element of G, we can write $uv = (x^a z_1)(x^b z_2) = x^a x^b z_2 z_1 = x^{a+b} z_2 z_1 = x^b z_2 x^a z_1 = vu$.

Problem 9 (3.1.37). Let A and B be groups. Show that $\{(a,1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by the is subgroup is isomorphic to B.

Proof. Let $N = \{(a,1) \mid a \in A\}$. Let $(x,y) \in A \times B$ and consider $(x,y)(a,1)(x^{-1},y^{-1}) = (xax^{-1},yy^{-1}) = (xax^{-1},1)$. Thus $(x,y)N(x,y)^{-1} \subseteq N$ for all $(x,y) \in A \times B$. Thus $N \subseteq A \times B$. Now consider the function $\varphi: A \times B/N \to B$ such that $\phi((a,b)N) = b$. This function is injective, since $(a_1,b_1)N \neq (a_2,b_2)N$ implies $(a_2^{-1}a_1,b_2^{-1}b_1) \notin N$. Thus $b_2^{-1}b_1 \neq 1$ and $b_1 \neq b_2$. The map is clearly surjective since given $b \in B$ any element of the form (a,b)N will map to it. Suppose we have $(a_1,b_1)N = (a_2,b_2)N$. Then $(a_2^{-1}a_1,b_2^{-1}b_1) \in N$. But this means $b_2^{-1}b_1 = 1$ and $b_1 = b_2$. Thus φ is well defined. Finally, note $\varphi((a_1,b_1)N(a_2,b_2)N) = \varphi((a_1a_2,b_1b_2)N) = b_1b_2 = \varphi((a_1,b_1)N)\varphi((a_2,b_2)N)$. Thus φ is an isomorphism and $A \times B/N \cong B$.

Problem 10 (3.1.41). Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G \rangle$ is a normal subgroup of G and G/N is abelian (N is called the commutator subgroup of G).

Proof. First note that $(x^{-1}y^{-1}xy)-1=y^{-1}x^{-1}yx$. For $g\in G$ we have $g(x^{-1}y^{-1}xy)g^{-1}=gx^{-1}g^{-1}gy^{-1}g^{-1}gxg^{-1}gyg^{-1}=(gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1})$. Thus, conjugation of a single commutator results in another commutator. Now suppose $z=(x_1^{-1}y_1^{-1}x_1y_1)\dots(x_n^{-1}y_n^{-1}x_ny_n)$ is the product of commutators. Then we have $gzg^{-1}=g(x_1^{-1}y_1^{-1}x_1y_1)g^{-1}\dots g(x_n^{-1}y_n^{-1}x_ny_n)g^{-1}$ and from the above result, we know this is then the product of commutators. This is then extended to the case where each commutator is raised to a power. For positive powers, the exact same argument holds. For negative powers, first separate the power into an inverse taken to a positive power, then use the first result of the proof. The conjugation is then a product of commutators. Therefore $gNg^{-1}\subseteq N$ for all $g\in G$ and thus $N\subseteq G$.

Now let $aN, bN \in G/N$. Then $aNbN = abN = \{abx \mid x \in N\}$. Now consider some element of abN, $ab(x^{-1}y^{-1}xy)$. We can write this as $ba(a^{-1}b^{-1}ab)(x^{-1}y^{-1}xy)$. Thus for each element of abN we can find an equivalent element in baN and vice versa. Therefore abN = baN which means aNbN = bNaN and G/N is abelian.

Problem 11 (3.2.4). Show that if |G| = pq for primes p and q (not necessarily distinct) then either G is abelian or Z(G) = 1.

Proof. We know $|Z(G)| \mid |G|$. Assuming that $Z(G) \neq 1$, without loss of generality we either have |Z(G)| = p or |Z(G)| = pq. In the later case we're done since G = Z(G) which is abelian. In the former case, let $x \in G \setminus Z(G)$. Then |y| = q and so $G = Z(G) \cup \langle y \rangle$. Since Z(G) commutes with everything and $\langle y \rangle$ is abelian, G must be abelian.

Problem 12 (3.2.11). Let $H \le K \le G$. Prove that $|G:H| = |G:K| \cdot |K:H|$.

Proof. Note that |K:H| is the number of left cosets of H in K. Also, |G:K| is the number of left cosets of K in G. That is, for each coset K in G, we can further partition this coset into |K:H| cosets of H in G. Since there are |G:K| of these partitions, and this gives all left cosets of H in G, this gives $|G:K| \cdot |K:H| = |G:H|$.

Problem 13 (3.2.19). Prove that if N is a normal subgroup of the finite group G and (|N|, |G:N|) = 1 then N is the unique subgroup of G of order |N|.

Proof. Note that G/N partitions G into |G:N| left cosets each with |N| elements. But since |N| and |G:N| = |G|/|N| are relatively prime, there's only one way to do this.

Problem 14 (4.1.1). Let G act on the set A. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$ (G_a is the stabilizer of a). Deduce that if G acts transitively on A then the kernel of the action is $\bigcap_{a \in G} gG_ag^{-1}$.

Proof. Let $x \in G_b$. Then $x \cdot b = g \cdot a$. Therefore $g \cdot a = x \cdot b = x(g \cdot a)$ and so $a = g^{-1}g \cdot a = g^{-1}xg \cdot a$. Thus $x \in gG_ag^{-1}$. If G acts transitively on A then $b = g \cdot a$ for all $b \in A$ and some $g \in G$. Then for all $b \in A$ we have $G_b = gG_ag^{-1}$ for some $g \in G$. But we know the kernel of the action is $\bigcap_{b \in A} G_b = \bigcap_{g \in G} gG_ag^{-1}$. \square

Problem 15 (4.2.8). Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G:K| \leq n!$.

Proof. Let G act on the set A of left cosets of H by left multiplication. Let π_H be the permutation representation afforded by this action. Then we know $\ker \pi_H = \bigcap_{x \in G} xHx^{-1}$. Let $K = \ker \pi_H$. Then we know K is normal and contained in H. Furthermore, since |G:H| = n, $\pi_H(G) \leq S_n$ and by the first isomorphism theorem $G/K \leq S_n$. Therefore $|G:K| \leq n!$.

Problem 16 (4.2.9). Prove that if p is prime and G is a group of order p^{α} for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

Proof. We know that if q is the smallest prime dividing |G| then any subgroup of order q is normal in G. But since the only prime which divides |G| is p, we know that p is the smallest prime dividing |G| and hence every subgroup of order p is normal in G. Suppose $|G| = p^2$ then there exists $x \in G$ such that $x \neq 1$. Since $\langle x \rangle \mid |G|$ we know $\langle x \rangle = p$. But then $|G: \langle x \rangle| = p$ as well as so $\langle x \rangle \leq G$.

Problem 17 (4.3.7). For n = 3, 4, 6 and 7 make lists of the partitions of n and give representatives for the corresponding conjugacy classes of S_n .

For n = 3 the partitions are (1, 1, 1), (1, 2) and (3) and they have representatives (1), $(1 \ 2)$ and $(1 \ 2 \ 3)$. For n = 4 the partitions are (1, 1, 1, 1), (1, 1, 2), (1, 3), (4) and (2, 2) and they have representatives (1), $(1 \ 2)$, $(1 \ 2 \ 3)$, $(1 \ 2 \ 3 \ 4)$ and $(1 \ 2)(3 \ 4)$.

For n = 6 the partitions are (1, 1, 1, 1, 1, 1), (1, 1, 1, 1, 2), (1, 1, 1, 3), (1, 1, 4), (1, 5), (6), (1, 1, 2, 2), (1, 2, 3), (2, 2, 2), (2, 4) and (3, 3) and they have representatives (1), $(1\ 2)$, $(1\ 2\ 3)$, $(1\ 2\ 3\ 4)$, $(1\ 2\ 3\ 4\ 5)$, $(1\ 2\ 3\ 4\ 5\ 6)$, $(1\ 2)(3\ 4)$, $(1\ 2)(3\ 4)(5\ 6)$, $(1\ 2)(3\ 4\ 5\ 6)$ and $(1\ 2\ 3)(4\ 5\ 6)$.

For n=7 the partitions are (1,1,1,1,1,1,1), (1,1,1,1,1,2), (1,1,1,1,3), (1,1,1,4), (1,1,5), (1,6), (7), (1,1,1,2,2), (1,1,2,3), (1,2,2,2), (1,3,3), (1,2,4), (2,5), and (3,4) and they have representatives (1), $(1\ 2\ 3)$, $(1\ 2\ 3\ 4\ 5)$, $(1\ 2\ 3\ 4\ 5\ 6)$, $(1\ 2\ 3\ 4$

Problem 18 (4.3.26). Let G be a transitive permutation group on the finite set A with |A| > 1. Show that there is some $\sigma \in G$ such that $\sigma(a) \neq a$ for all $a \in A$ (such an element σ is called fixed point free).

Proof. Let $a \in A$. We know that $|\{\sigma(a) \mid \sigma \in G\}| = |G: G_a| = |G|/|G_a|$. But since G acts transitively on A we know that $A = \{\sigma(a) \mid \sigma \in G\}$. Therefore $|G|/|A| = |G_a|$. This is true for all $a \in A$. Furthermore, since |A| > 1 we know that $|G_a| < |G|$ for each $a \in A$. Thus there exists $\sigma \in G$ for each $a \in A$ such that $\sigma(a) \neq a$. Then taking the union $U = \bigcup_{a \in A} G_a$ we can find $\sigma \in G \setminus U$ which doesn't fix any $a \in A$.

Problem 19 (4.3.29). Let p be a prime and let G be a group of order p^{α} . Prove that G has a subgroup of order p^{β} , for every β with $0 \le \beta \le \alpha$.

Proof. For the base case $\alpha=0$ the problem is trivial since |G|=1. Assume the statement is true for groups of order α and suppose that $|G|=p^{\alpha+1}$. Then we know $Z(G)\neq 1$ which means $|Z(G)|=p^{\gamma}$ where $1<\gamma\leq \alpha+1$. Since Z(G) is abelian, we know there exists $x\in Z(G)$ such that |x|=p. Now consider $\overline{G}=|G|/\langle x\rangle$. Note that $\overline{G}\cong H$ for some $H\leq G$. But also $|\overline{G}|=|H|=p^{\alpha}$. Therefore H has subgroups of order p^{β} for each $0\leq \beta\leq \alpha$ and therefore G does as well.

Problem 20. Write the class equation for A_4 .

Proof. From Problem 17 we know that representatives of the cycles types of even permutations of S_4 can be taken to be (1), $(1\ 2\ 3)$ and $(1\ 2)(3\ 4)$. Furthermore we know that

$$C_{S_4}((1\ 2\ 3)) = \{(1\ 2\ 3)^i \tau \mid i = 0, 1 \text{ or } 2 \text{ and } \tau \in S_{4-3}\} = \langle (1\ 2\ 3) \rangle$$

which directly implies $C_{A_4}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$. This group has order 3 and index 4. Since there are 8 3-cycles in A_4 , and four of them are in the conjugacy class of $(1\ 2\ 3)$, there must be another 3-cycle not in this class. Using the same logic as above, we see that the centralizer of this 3-cycle is also of order 3 and so it has index 4. Finally, note that $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \cong V_4$ and so all of these elements commute with each other. Since these are the only elements of A_4 with this cycle type, we see that $|C_{A_4}((1\ 2)(3\ 4))| = 4$ and has index 3. Therefore, the class equation for A_4 is

$$|A_4| = |Z(A_4)| + |A_4 : C_{A_4}((1\ 2\ 3))| + |A_4 : C_{A_4}((1\ 3\ 2))| + |A_4 : C_{A_4}((1\ 2)(3\ 4))| = 1 + 4 + 4 + 3 = 12.$$