9. This exercise outlines a proof of Cauchy's Theorem due to James McKay (*Another proof of Cauchy's group theorem*, Amer. Math. Monthly, 66(1959), p. 119). Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:

$$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}.$$

(a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p.

Define the relation $\sim$ on $\mathcal{S}$ by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

(b) Show that a cyclic permutation of an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.

(c) Prove that $\sim$ is an equivalence relation on $\mathcal{S}$.

(d) Prove that an equivalence class contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

(e) Prove that every equivalence class has order 1 or p (this uses the fact that p is a *prime*). Deduce that $|G|^{p-1} = k + pd$, where k is the number of classes of size 1 and d is the number of classes of size p.

(f) Since $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element x in G with $x^p = 1$, i.e., G contains an element of order p. [Show $p \mid k$ and so $k > 1$.]

10. Suppose H and K are subgroups of finite index in the (possibly infinite) group G with $|G : H| = m$ and $|G : K| = n$. Prove that l.c.m.$(m, n) \leq |G : H \cap K| \leq mn$. Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.

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

12. Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of H in G onto a right coset of H and gives a bijection between the set of left cosets and the set of right cosets of H in G (hence the number of left cosets of H in G equals the number of right cosets).

13. Fix any labelling of the vertices of a square and use this to identify D_8 as a subgroup of S_4. Prove that the elements of D_8 and $\langle (1\,2\,3) \rangle$ do not commute in S_4.

14. Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3.

15. Let $G = S_n$ and for fixed $i \in \{1, 2, \ldots, n\}$ let G_i be the stabilizer of i. Prove that $G_i \cong S_{n-1}$.

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

17. Let p be a prime and let n be a positive integer. Find the order of $\bar{p}$ in $(\mathbb{Z}/(p^n - 1)\mathbb{Z})^\times$ and deduce that $n \mid \varphi(p^n - 1)$ (here φ is Euler's function).

18. Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

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 $|N|$.

20. If A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G prove that $A \cap B \trianglelefteq AB$.

21. Prove that $\mathbb{Q}$ has no proper subgroups of finite index. Deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index. [Recall Exercise 21, Section 1.6 and Exercise 15, Section 1.]

22. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\varphi(n)} \equiv 1 \bmod n$ for every integer a relatively prime to n, where φ denotes Euler's φ-function.

23. Determine the last two digits of $3^{3^{100}}$. [Determine $3^{100} \bmod \varphi(100)$ and use the previous exercise.]

3.3 THE ISOMORPHISM THEOREMS

In this section we derive some straightforward consequences of the relations between quotient groups and homomorphisms which were discussed in Section 1. In particular we consider the relation between the lattice of subgroups of a quotient group, G/N, and the lattice of subgroups of the group G. The first result restates our observations in Section 1 on the relation of the image of a homomorphism to the quotient by the kernel (sometimes called the Fundamental Theorem of Homomorphisms):

Theorem 16. *(The First Isomorphism Theorem)* If $\varphi : G \to H$ is a homomorphism of groups, then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \varphi(G)$.

Corollary 17. Let $\varphi : G \to H$ be a homomorphism of groups.
(1) φ is injective if and only if $\ker \varphi = 1$.
(2) $|G : \ker \varphi| = |\varphi(G)|$.

Proof: Exercise.

When we consider abstract vector spaces we shall see that Corollary 17(2) gives a formula possibly already familiar from the theory of linear transformations: if $\varphi : V \to W$ is a linear transformation of vector spaces, then $\dim V = \text{rank}\,\varphi + \text{nullity}\,\varphi$.

Theorem 18. *(The Second or Diamond Isomorphism Theorem)* Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.

Proof: By Corollary 15, AB is a subgroup of G. Since $A \leq N_G(B)$ by assumption and $B \leq N_G(B)$ trivially, it follows that $AB \leq N_G(B)$, i.e., B is a normal subgroup of the subgroup AB.

Since B is normal in AB, the quotient group AB/B is well defined. Define the map $\varphi : A \to AB/B$ by $\varphi(a) = aB$. Since the group operation in AB/B is well defined it is easy to see that φ is a homomorphism:

$$\varphi(a_1a_2) = (a_1a_2)B = a_1B \cdot a_2B = \varphi(a_1)\varphi(a_2).$$

Alternatively, the map φ is just the restriction to the subgroup A of the natural projection homomorphism $\pi : AB \to AB/B$, so is also a homomorphism. It is clear from the definition of AB that φ is surjective. The identity in AB/B is the coset $1B$, so the kernel of φ consists of the elements $a \in A$ with $aB = 1B$, which by Proposition 4 are the elements $a \in B$, i.e., $\ker \varphi = A \cap B$. By the First Isomorphism Theorem, $A \cap B \trianglelefteq A$ and $A/A \cap B \cong AB/B$, completing the proof.

Note that this gives a new proof of the order formula in Proposition 13 in the special case that $A \leq N_G(B)$. The reason this theorem is called the Diamond Isomorphism is because of the portion of the lattice of subgroups of G involved (see Figure 6). The markings in the lattice lines indicate which quotients are isomorphic. The "quotient"

AB/A need not be a group (i.e., A need not be normal in AB), however we still have $|AB : A| = |B : A \cap B|$.

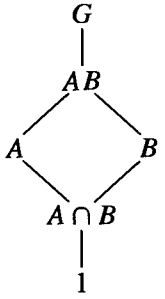


Fig. 6

The third Isomorphism Theorem considers the question of taking quotient groups of quotient groups.

Theorem 19. *(The Third Isomorphism Theorem)* Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$

If we denote the quotient by H with a bar, this can be written

$$\overline{G}/\overline{K} \cong G/K.$$

Proof: We leave as an easy exercise the verification that $K/H \trianglelefteq G/H$. Define

$$\varphi : G/H \to G/K$$
$$(gH) \mapsto gK.$$

To show φ is well defined suppose $g_1H = g_2H$. Then $g_1 = g_2h$, for some $h \in H$. Because $H \leq K$, the element h is also an element of K, hence $g_1K = g_2K$ i.e., $\varphi(g_1H) = \varphi(g_2H)$, which shows φ is well defined. Since g may be chosen arbitrarily in G, φ is a surjective homomorphism. Finally,

$$\begin{aligned}\ker\varphi &= \{gH \in G/H \mid \varphi(gH) = 1K\} \\ &= \{gH \in G/H \mid gK = 1K\} \\ &= \{gH \in G/H \mid g \in K\} = K/H.\end{aligned}$$

By the First Isomorphism Theorem, $(G/H)/(K/H) \cong G/K$.

An easy aid for remembering the Third Isomorphism Theorem is: "invert and cancel" (as one would for fractions). This theorem shows that we gain no new structural information from taking quotients of a quotient group.

The final isomorphism theorem describes the relation between the lattice of subgroups of the quotient group G/N and the lattice of subgroups of G. The lattice for G/N can be read immediately from the lattice for G by collapsing the group N to the identity. More precisely, there is a one-to-one correspondence between the subgroups of G containing N and the subgroups of G/N, so that the lattice for G/N (or rather, an isomorphic copy) appears in the lattice for G as the collection of subgroups of G between N and G. In particular, the lattice for G/N appears at the "top" of the lattice for G, a result we mentioned at the beginning of the chapter.

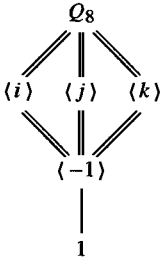
Theorem 20. *(The Fourth or Lattice Isomorphism Theorem)* Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,
(2) if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$,
(3) $\overline{\langle A, B \rangle} = \langle \overline{A}, \overline{B} \rangle$,
(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$, and
(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

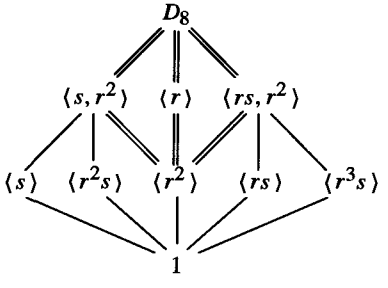
Proof: The complete preimage of a subgroup in G/N is a subgroup of G by Exercise 1 of Section 1. The numerous details of the theorem to check are all completely straightforward. We therefore leave the proof of this theorem to the exercises.

Examples

(1) Let $G = Q_8$ and let N be the normal subgroup $\langle -1 \rangle$. The (isomorphic copy of the) lattice of G/N consists of the double lines in the lattice of G below. Note that we previously proved that $Q_8/\langle -1 \rangle \cong V_4$ and the two lattices do indeed coincide (see Section 2.5 for the lattices of Q_8 and V_4).



(2) The same process gives us the lattice of $D_8/\langle r^2 \rangle$ (the double lines) in the lattice of D_8:



Note that in the second example above there are subgroups of G which do not directly correspond to subgroups in the quotient group G/N, namely the subgroups of G which do not contain the normal subgroup N. This is because the subgroup N projects to a point in G/N and so several subgroups of G can project to the same