

Solutions to Problem Session Questions

Problem: (3.3) Let $f : A \rightarrow B$ be a function. Prove that f is one-to-one if and only if $f(A_1) \cap f(A_2) = f(A_1 \cap A_2)$ for any subsets A_1, A_2 of A .

We know from Ex. 2 that $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. The claim amounts to showing that f is one-to-one if and only if $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$ for any subsets A_1, A_2 of A .

Assume that f is one-to-one. Let A_1, A_2 be arbitrary subsets of A . If $b \in f(A_1) \cap f(A_2)$, then $b = f(a_1)$ for some $a_1 \in A_1$ and $b = f(a_2)$ for some $a_2 \in A_2$. Since $f(a_1) = b = f(a_2)$ and f is one-to-one, $a_1 = a_2$, so $a_1 \in A_1 \cap A_2$, so $b = f(a_1) \in f(A_1 \cap A_2)$. This proves that $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$.

Assume that $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$ for any subsets A_1, A_2 of A . If $a_1 \neq a_2$ are two distinct elements of A , then $\{f(a_1)\} \cap \{f(a_2)\} = f(\{a_1\}) \cap f(\{a_2\}) \subseteq f(\{a_1\} \cap \{a_2\}) = f(\emptyset) = \emptyset$, so $f(a_1) \neq f(a_2)$. This proves that f is one-to-one.

Problem: (7.2) For which $m \in \mathbb{N}$ is $\mathbb{Z}_m \setminus \{\bar{0}\}$ a group under multiplication?

If $m = 1$, then $\mathbb{Z}_m = \mathbb{Z}_1 = \{\bar{0}\}$, so $\mathbb{Z}_m \setminus \{\bar{0}\} = \emptyset$ and $\mathbb{Z}_m \setminus \{\bar{0}\}$ cannot be a group.

If $m > 1$ and m is composite, there are integers a, b satisfying $1 < a < m$, $1 < b < m$ and $ab = m$. In \mathbb{Z}_m , these conditions may be written as $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ and $\overline{ab} = \bar{0}$. Equivalently, $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$, $\bar{b} \in \mathbb{Z}_m \setminus \{\bar{0}\}$ and $\overline{ab} \notin \mathbb{Z}_m \setminus \{\bar{0}\}$. Thus $\mathbb{Z}_m \setminus \{\bar{0}\}$ is not closed under multiplication and $\mathbb{Z}_m \setminus \{\bar{0}\}$ cannot be a group.

The only remaining possibility is that m is a prime number. Suppose that m is prime. Let's check whether $\mathbb{Z}_m \setminus \{\bar{0}\}$ is a group in this case.

(i) For any integers a, b , Euclid's lemma (Lemma 5.15) says that $m \mid ab$ implies $m \mid a$ or $m \mid b$ (because m is prime). Equivalently, if $m \nmid a$ and $m \nmid b$, then $m \nmid ab$. Stated differently, in $\mathbb{Z}_m \setminus \{\bar{0}\}$, if $\bar{a} \neq \bar{0}$ and $\bar{b} \neq \bar{0}$, then $\overline{ab} \neq \bar{0}$. Hence $\mathbb{Z}_m \setminus \{\bar{0}\}$ is closed under multiplication.

(ii) Multiplication in $\mathbb{Z}_m \setminus \{\bar{0}\}$ is associative by Lemma 6.4(7).

(iii) There is $\bar{1} \in \mathbb{Z}_m \setminus \{\bar{0}\}$ and $\bar{a} \cdot \bar{1} = \bar{a}$ for all $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$, so $\bar{1}$ is a right identity in $\mathbb{Z}_m \setminus \{\bar{0}\}$.

(iv) Let $a \in \mathbb{Z}$ with $\bar{a} \neq \bar{0}$. Then a is relatively prime to m and, by Lemma 6.4(9), there is an $\bar{x} \in \mathbb{Z}_m$ with $\bar{a}\bar{x} = \bar{1}$. So every \bar{a} in $\mathbb{Z}_m \setminus \{\bar{0}\}$ has a right inverse \bar{x} in \mathbb{Z}_m . But in fact $\bar{x} \in \mathbb{Z}_m \setminus \{\bar{0}\}$, for otherwise we would have $\bar{x} = \bar{0}$ and $\bar{1} = \bar{a}\bar{x} = \bar{a}\bar{0} = \bar{0}$ by Lemma 6.4(12), yielding the contradiction $m \mid 1$. Thus every \bar{a} in $\mathbb{Z}_m \setminus \{\bar{0}\}$ has a right inverse in $\mathbb{Z}_m \setminus \{\bar{0}\}$.

It follows that $\mathbb{Z}_m \setminus \{\bar{0}\}$ is a group if m is a prime number.

Hence $\mathbb{Z}_m \setminus \{0\}$ a group under multiplication if and only if m is a prime number.

Problem: (8.1) Let G be a group such that $a^2 = 1$ for all $a \in G$. Prove that G is commutative.

By hypothesis, for any $a, b \in G$, we have $a^2 = 1$, $b^2 = 1$ and $(ab)^2 = 1$. Hence

$$\begin{aligned} 1 &= (ab)^2 = abab \\ a &= a \cdot abab = a^2bab = bab \\ ba &= b \cdot bab = b^2ab = ab \end{aligned}$$

for all $a, b \in G$ and G is commutative.

Problem: (9.3) Let $M := \{\alpha \in S_{[0,1]} : 0\alpha = 0 \text{ or } 1\alpha = 1\}$. Is M a subgroup of $S_{[0,1]}$?

Consider the functions α and β in $S_{[0,1]}$ defined by

$$x\alpha = \begin{cases} x & \text{if } x \neq 1/2, x \neq 1, \\ 1/2 & \text{if } x = 1, \\ 1 & \text{if } x = 1/2, \end{cases} \quad x\beta = \begin{cases} x & \text{if } x \neq 1/2, x \neq 0, \\ 1/2 & \text{if } x = 0, \\ 0 & \text{if } x = 1/2. \end{cases}$$

Then $0\alpha = 0$, so $\alpha \in M$; and $1\beta = 1$, so $\beta \in M$. But $0\alpha\beta = 0\beta = 1/2 \neq 0$ and $1\alpha\beta = (1/2)\beta = 0 \neq 1$, so $\alpha\beta \notin M$. Thus M is not closed under composition of functions and M is not a subgroup of $S_{[0,1]}$.

Problem: (9.4) Let $L := \{1, 2, 4, 5, 7, 8\} \subseteq \mathbb{Z}_9$. Show that L is a group under multiplication. Find all subgroups of L . Do the orders of the subgroups divide the order $|L| = 6$ of L ?

Let's make a multiplication table:

\cdot	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

and check the group axioms. [When this problem was assigned, we did not know that \mathbb{Z}_n^\times is a group.]

(i) The table consists of 1, 2, 4, 5, 7, 8, so L is closed under multiplication.

(ii) Multiplication in $L \subseteq \mathbb{Z}_9$ is associative by Lemma 6.4(7).

(iii) The column of $1 \in L$ is identical with the column of the names (below the sign \cdot), i.e., $a1 = a$ for all $a \in L$. Thus 1 is a right identity in L .

(iv) The element 1 appears in every row, i.e., for each $a \in L$, there is a right inverse $x \in L$ satisfying $ax = 1$. Thus every element of L has a right inverse.

Hence L is indeed a group under multiplication.

Now let's find the subgroup of L . Since L is finite, they are the multiplicatively closed subsets of L . In particular, if a is in a subgroup, then all the powers of a will be in the same subgroup. Let's write down powers of the elements of L .

1	1					
2	1	2	4	8	7	5
4	1	4	7			
5	1	5	7	8	4	2
7	1	7	4			
8	1	8				

Let H be a nontrivial subgroup of L . So there is an $a \neq 1$ in H . We can make some observations here.

- If $2 \in H$ or $5 \in H$, then $L \subseteq H$, so $H = L$.
- Assume $2 \notin H$ and $5 \notin H$. Then both 4 and 8 cannot be in H , similarly both 7 and 8 cannot be in H , because $4 \cdot 8 = 5 \notin H$ and $7 \cdot 8 = 2 \notin H$.
 - If $4 \in H$ or $7 \in H$, then $\{1, 4, 7\} \subseteq H$. Also $8 \notin H$, so the group H must be the set $\{1, 4, 7\}$. Since $\{1, 4, 7\}$ is multiplicatively closed, it is indeed a group and we have $H = \{1, 4, 7\}$.
 - If $4 \notin H$ and $7 \notin H$, then $8 \in H$, so the group H must be the set $\{1, 8\}$. Since $\{1, 8\}$ is multiplicatively closed, it is indeed a group and we have $H = \{1, 8\}$.

Hence all the subgroups of L are $\{1\}$, $\{1, 8\}$, $\{1, 4, 7\}$, $\{1, 2, 4, 5, 7, 8\}$. [This is how you could answer this question at the time of its assignment. Today you have a complete description of subgroups of a cyclic group and you can answer this and similar questions much more shortly.]

The order of any subgroup of L is one of the numbers 1, 2, 3, 6, so it is a divisor of 6. [Today, we would obtain it by a reference to Lagrange's theorem.]

Problem: (9.5) Let G be a group and $H \leq G$, $K \leq G$. Show that $H \cup K$ is not a subgroup of G unless $H \cup K = K$ or $H \cup K = H$.

Let's prove the contrapositive of this assertion. So if $H \not\subseteq K$ and $K \not\subseteq H$, then we are to prove that $U := H \cup K$ is not a subgroup of G .

Suppose $K \not\subseteq H$ and $H \not\subseteq K$ and $U \leq G$. Then there is a $k \in K \setminus H$ and an $h \in H \setminus K$. This hk cannot be an element of H , for otherwise $k = h^{-1}(hk)$ would be in H , contrary to the choice of k . In the same manner, hk cannot be an element of K , for otherwise $h = (hk)k^{-1}$ would be in K , contrary to the choice of h . We see that $kh \notin H$ and $kh \notin K$, so $hk \notin U$. But $h \in U$, $k \in U$ and, by hypothesis, U is a subgroup of G and U is closed under multiplication, so $hk \in U$. We obtained the contradiction $hk \notin U$ and $hk \in U$. This contradiction shows that, if $H \not\subseteq K$ and $K \not\subseteq H$, then $H \cup K \not\leq G$.

Problem: (9.7) Let G be a group and let a be a fixed element of G . Determine whether the subset $C := \{g \in G : ga = ag\}$ of G is a subgroup of G .

Since $1a = a = a1$, we have $1 \in C$, so $C \neq \emptyset$. Now we can use the subgroup criterion.

(i) Let $g, h \in C$. Then $ga = ag$ and $ha = ah$, so $(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$ and $gh \in C$. Thus C is closed under multiplication.

(ii) Let $g \in C$. Then $ga = ag$, so we have

$$\begin{aligned} g^{-1}ga &= g^{-1}ag \\ a &= g^{-1}ag \\ ag^{-1} &= g^{-1}agg^{-1} \\ ag^{-1} &= g^{-1}a \end{aligned}$$

and $g^{-1}a = ag^{-1}$, so $g^{-1} \in C$. Thus C is closed under the forming of inverses.

It follows that C is a subgroup of G .

Problem: (10.4) Why don't we use the "mapping" $\mathcal{R} \rightarrow \mathcal{L}$, $Ha \mapsto aH$ in the proof of the assertion that $|\mathcal{R}| = |\mathcal{L}|$?

This "mapping" need not be a mapping at all. It is not necessarily well-defined. It is well-defined if and only if $Ha = Hb$ implies $aH = bH$, so if and only if $ab^{-1} \in H$ implies $b^{-1}a \in H$ (for all $a, b \in G$). Equivalently, it is well-defined if and only if $ab \in H$ implies $ba \in H$ (for all $a, b \in G$). In a non-commutative group G , this implication is not necessarily true.

Problem: (12.2) Construct the multiplication tables of \mathbb{Z}_n^\times for $n = 2, 4, 6, 10, 12$.

\cdot	1	\cdot	1	3	\cdot	1	5	\cdot	1	3	7	9	\cdot	1	5	7	11
1	1	1	1	3	1	1	5	1	1	3	7	9	1	1	5	7	11
		3	3	1	5	5	1	3	3	9	1	7	5	5	1	11	7
								7	7	1	9	3	7	7	11	1	5
								9	9	7	3	1	11	11	7	5	1

Problem: (12.6) Find the order of 3 in $\mathbb{Z}_8^\times, \mathbb{Z}_{16}^\times, \mathbb{Z}_{32}^\times, \mathbb{Z}_{64}^\times$.

In \mathbb{Z}_8^\times . The first few powers of 3 are $3^1 = 3 \neq 1$, $3^2 = 9 = 1$, so 2 is the least positive integer s with $3^s = 1$, so $o(3) = 2$.

In \mathbb{Z}_{16}^\times . The first few powers of 3 are $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^3 = 27 = 11 \neq 1$, $3^4 = 11 \cdot 3 = 33 = 1$, so 4 is the least positive integer s with $3^s = 1$, so $o(3) = 4$.

In \mathbb{Z}_{32}^\times . The first few powers of 3 are, hmmm, $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^3 = 27 \neq 1$, $3^4 = 81 = 17 \neq 1$, $3^5 = 17 \cdot 3 = 51 = 19 \neq 1$, $3^6 = 19 \cdot 3 = 57 = 25 \neq 1$, hmmm, this is too much work. Do I have to carry out so many computations? In any case, I know that $o(3) \mid |\mathbb{Z}_{32}^\times| = \varphi(32) = 16$, so $o(3)$ is one of the divisors 1, 2, 4, 8, 16 of 16. Computing $3^3, 3^5, 3^6$ was redundant. Fortunately, I noticed this before making further unnecessary computations with $3^7, 3^9, 3^{10}$ and so on. I computed above that $3^1 \neq 1, 3^2 \neq 1, 3^4 \neq 1$. So there remains 3^8 and 3^{16} to consider. Since $3^8 = (3^4)^2 = 17^2 = 289 = -31 = 1$, I see that 8 is the least positive integer s with $3^s = 1$, so $o(3) = 8$.

In \mathbb{Z}_{64}^\times . Now I'll be more careful and more clever than before. I know that $o(3) \mid |\mathbb{Z}_{64}^\times| = \varphi(64) = 32$, so $o(3)$ is one of the divisors 1, 2, 4, 8, 16, 32 of 32. Besides, from the previous calculations, I know that $3^4 \not\equiv 1 \pmod{32}$, all the more so $3^4 \not\equiv 1 \pmod{64}$, so $o(3) > 4$. So there remains $3^8, 3^{16}, 3^{32}$ to examine. I find $3^8 = (3^4)^2 = 17^2 = 289 = -31 = 33 \neq 1$ and $3^{16} = (3^8)^2 = 33^2 = 1089 = 1$, so 16 is the least positive integer s with $3^s = 1$, so $o(3) = 16$.

Problem: (12.8) Show that \mathbb{Z}_{pq}^\times is not cyclic if p and q are distinct positive odd prime numbers. [Hint: what is $\varphi(pq)$ and what is $a^{(p-1)(q-1)/2}$ congruent to (mod pq) if a is an integer relatively prime to pq ?]

Let's start with $\varphi(pq)$. It is the number of integers among

$$1, 2, 3, \dots, pq \tag{a}$$

that are relatively prime to pq . Among them,

$$p, 2p, 3p, \dots, pq$$

are not relatively prime to p and

$$q, 2q, 3q, \dots, pq$$

are not relatively prime to q . There are q numbers in the first list, p numbers in the second one, and only one number, namely pq , is common to both lists. Therefore the number of integers in (a) that are *not* relatively prime to pq is $q + p - 1$, and the number of integers in (a) that *are* relatively prime to pq is $pq - (q + p - 1) = pq - p - q + 1 = (p - 1)(q - 1)$. Thus $\varphi(pq) = (p - 1)(q - 1)$.

If a is relatively prime to pq , then a is relatively prime to p and to q , so

$$\begin{aligned} a^{p-1} &\equiv 1, & (a^{p-1})^{(q-1)/2} &\equiv 1^{(q-1)/2}, & a^{(p-1)(q-1)/2} &\equiv 1 \pmod{p}, \\ a^{q-1} &\equiv 1, & (a^{q-1})^{(p-1)/2} &\equiv 1^{(p-1)/2}, & a^{(p-1)(q-1)/2} &\equiv 1 \pmod{q}. \end{aligned}$$

As both p and q divide $a^{(p-1)(q-1)/2} - 1$ and as p and q are relatively prime, we get $pq \mid a^{(p-1)(q-1)/2} - 1$. Thus $a^{(p-1)(q-1)/2} \equiv 1 \pmod{pq}$.

We see that $\bar{a}^{(p-1)(q-1)/2} = \bar{1}$ for every $\bar{a} \in \mathbb{Z}_{pq}^\times$, so the order $o(\bar{a})$ of every element \bar{a} of \mathbb{Z}_{pq}^\times is a divisor of, and smaller than or equal to, $\frac{1}{2}(p-1)(q-1)$. Thus

$$\begin{aligned} |\langle a \rangle| &\leq \frac{1}{2}(p-1)(q-1) < (p-1)(q-1) = \varphi(pq) = |\mathbb{Z}_{pq}^\times|, \\ \langle a \rangle &< \mathbb{Z}_{pq}^\times, \\ \langle a \rangle &\neq \mathbb{Z}_{pq}^\times \end{aligned}$$

for every \bar{a} in \mathbb{Z}_{pq}^\times . Thus no $\bar{a} \in \mathbb{Z}_{pq}^\times$ can generate \mathbb{Z}_{pq}^\times , consequently \mathbb{Z}_{pq}^\times is not cyclic.

Problem: (13.6) A halfturn $\sigma_P = \sigma_{(a,b)}$ about a point $P = (a, b)$ is defined as the mapping given by

$$(x, y) \mapsto (2a - x, 2b - y) \quad \text{for all points } (x, y) \in E.$$

Show that any halfturn is an isometry of order 2. Prove that the product of three halfturns is a halfturn.

If $(x, y)\sigma_P = (u, v)\sigma_P$, then $(2a - x, 2b - y) = (2a - u, 2b - v)$, so $2a - x = 2a - u$ and $2b - y = 2b - v$, so $x = u$ and $y = v$, so $(x, y) = (u, v)$. Thus σ_P is one-to-one.

For any $(x, y) \in E$, there is $(2a - x, 2b - y)$ in E such that $(2a - x, 2b - y)\sigma_P = (2a - (2a - x), 2b - (2b - y)) = (x, y)$, so σ_P is onto E .

I see that σ_P is a bijection. What is its order? Is it of order 2? Since $(x, y)\sigma_P\sigma_P = (2a - x, 2b - y)\sigma_P = (2a - (2a - x), 2b - (2b - y)) = (x, y)$ for all $(x, y) \in E$, we have $(\sigma_P)^2 = \sigma_P\sigma_P = \text{id}_E$, whereas $\sigma_P \neq \text{id}_E$, so $o(\sigma_P) = 2$.

Well, what did I do? I repeated much of the argument establishing surjectivity of σ_P . Actually, the equation $\sigma_P\sigma_P = \text{id}_E$ shows that σ_P has an inverse function, so it is a bijection. If I had thought of it before, I would have saved myself the first two paragraphs of this solution. I'd better think a bit before starting answering a problem.

Let me see if it is an isometry. Well, for all $(x, y), (u, v) \in E$,

$$\begin{aligned} d((x, y)\sigma_P, (u, v)\sigma_P) &= d((2a - x, 2b - y), (2a - u, 2b - v)) \\ &= \sqrt{[(2a - u) - (2a - x)]^2 + [(2b - v) - (2b - y)]^2} \\ &= \sqrt{(u - x)^2 + (v - y)^2} = d((x, y), (u, v)), \end{aligned}$$

so σ_P is an isometry.

Finally, let's examine the product of three halfturns $\sigma_{(a,b)}$, $\sigma_{(c,d)}$ and $\sigma_{(e,f)}$. For any $(x, y) \in E$, there holds

$$\begin{aligned} (x, y)(\sigma_{(a,b)}\sigma_{(c,d)}\sigma_{(e,f)}) &= ((x, y)\sigma_{(a,b)})(\sigma_{(c,d)}\sigma_{(e,f)}) \\ &= (2a - x, 2b - y)(\sigma_{(c,d)}\sigma_{(e,f)}) \\ &= ((2a - x, 2b - y)\sigma_{(c,d)})\sigma_{(e,f)} \\ &= (2c - (2a - x), 2d - (2b - y))\sigma_{(e,f)} \\ &= (x + 2c - 2a, y + 2d - 2b)\sigma_{(e,f)} \\ &= (2e - (x + 2c - 2a), 2f - (y + 2d - 2b)) \\ &= (2(a - c + e) - x, 2(b - d + f) - y) \\ &= (x, y)\sigma_{(a-c+e, b-d+f)}, \end{aligned}$$

so $\sigma_{(a,b)}\sigma_{(c,d)}\sigma_{(e,f)}$ is the halfturn $\sigma_{(a-c+e, b-d+f)}$.

Problem: (15.6) Construct multiplication tables of S_1 , S_2 , S_3 .

The table of S_1 and S_2 are given below, that of S_3 is given in the book, and appears also later in this solution key.

·	id
id	id

·	id	(12)
id	id	(12)
(12)	(12)	id

Problem: (15.5, 15.7) Write all elements of S_3 , S_4 . Find the orders of all elements in S_3 , S_4 .

The order of a cycle is its length, the order of a product of disjoint cycles is the least common multiple of the orders (lengths) of the factors. Let's proceed systematically. We can start with id. Then we can consider cycles of length 2, 3, 4,

then products of a cycle of length 2 by a cycle of length 2, then products of a cycle of length 2 by a cycle of length 3, then products of a cycle of length 2 by a cycle of length 4, \dots , then products of a cycle of length 3 by a cycle of length 3, then products of a cycle of length 3 by a cycle of length 4, \dots and so on.

		el'ts of S_4		orders	
		id	1		
		(12)	2		
		(13)	2	el'ts of S_4	orders
elements of S_3	orders	(14)	2	(1234)	4
id	1	(23)	2	(1243)	4
(12)	2	(24)	2	(1324)	4
(13)	2	(34)	2	(1342)	4
(23)	2	(123)	3	(1423)	4
(123)	3	(132)	3	(1432)	4
(132)	3	(124)	3	(12)(34)	$[2, 2] = 2$
		(142)	3	(13)(24)	$[2, 2] = 2$
		(134)	3	(14)(23)	$[2, 2] = 2$
		(143)	3		
		(234)	3		
		(243)	3		

I can write down the elements of S_5 just as systematically, too.

Problem: (15.15) Show that, for any $\sigma \in S_n$ ($n \geq 3$), there holds $\sigma^{-1}(123)\sigma = (abc)$ with suitable a, b, c . How are a, b, c related to σ ?

We have $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1\sigma & 2\sigma & 3\sigma & 4\sigma & \dots & n\sigma \end{pmatrix}$ and

$$\begin{aligned} & \sigma^{-1}(123)\sigma \\ &= \begin{pmatrix} 1\sigma & 2\sigma & 3\sigma & 4\sigma & \dots & n\sigma \\ 1 & 2 & 3 & 4 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1\sigma & 2\sigma & 3\sigma & 4\sigma & \dots & n\sigma \end{pmatrix} \\ &= \begin{pmatrix} 1\sigma & 2\sigma & 3\sigma & 4\sigma & \dots & n\sigma \\ 2\sigma & 3\sigma & 1\sigma & 4\sigma & \dots & n\sigma \end{pmatrix} = (1\sigma \ 2\sigma \ 3\sigma) = (abc), \end{aligned}$$

where $a := 1\sigma$, $b := 2\sigma$ and $c := 3\sigma$.

Problem: (16.6) Construct multiplication tables of A_2, A_3, A_4 .

·	id	·	id	(123)	(132)
id	id	id	id	(123)	(132)
id	id	(123)	(123)	(132)	id
		(132)	(132)	id	(123)

As the table of A_4 does not fit in this page, it is given as a separate document.

Problem: (17.3) Write down the multiplication table of $GL(2, \mathbb{Z}_2)$. Compare it (eventually after reordering the rows and columns) with the multiplication table of S_3 .

On putting $g1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $g2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $g3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $g4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $g5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $g6 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, we find the multiplication table of $GL(2, \mathbb{Z}_2)$ below. It is almost the same table as that of S_3 , where we put $h1 = \text{id}$, $h2 = (123)$, $h3 = (132)$, $h4 = (12)$, $h5 = (13)$, $h6 = (23)$.

$x \backslash y$	g1	g2	g3	g4	g5	g6
g1	g1	g2	g3	g4	g5	g6
g2	g2	g3	g1	g6	g4	g5
g3	g3	g1	g2	g5	g6	g4
g4	g4	g5	g6	g1	g2	g3
g5	g5	g6	g4	g3	g1	g2
g6	g6	g4	g5	g2	g3	g1

$x \backslash y$	h1	h2	h3	h4	h5	h6
h1	h1	h2	h3	h4	h5	h6
h2	h2	h3	h1	h6	h4	h5
h3	h3	h1	h2	h5	h6	h4
h4	h4	h5	h6	h1	h2	h3
h5	h5	h6	h4	h3	h1	h2
h6	h6	h4	h5	h2	h3	h1

Figure 1: Tables of $GL(2, \mathbb{Z}_2)$ and S_3

Problem: (17.14) Let $H := \left\{ \begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$. Prove that H is closed under addition and multiplication. Prove that $H \setminus \{0\}$ is a group under multiplication.

For any $\begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix}, \begin{pmatrix} c & \bar{d} \\ -d & \bar{c} \end{pmatrix} \in H$, we have

$$\begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix} + \begin{pmatrix} c & \bar{d} \\ -d & \bar{c} \end{pmatrix} = \begin{pmatrix} a+c & \bar{b}+\bar{d} \\ -b-d & \bar{a}+\bar{c} \end{pmatrix} = \begin{pmatrix} a+c & \overline{b+d} \\ -(b+d) & \overline{a+c} \end{pmatrix} \in H$$

and

$$\begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix} \begin{pmatrix} c & \bar{d} \\ -d & \bar{c} \end{pmatrix} = \begin{pmatrix} ac - \bar{b}d & a\bar{d} + \bar{b}c \\ -bc - \bar{a}d & -b\bar{d} + \bar{a}c \end{pmatrix} = \begin{pmatrix} ac - \bar{b}d & \overline{\bar{a}d + bc} \\ -(\bar{a}d + bc) & \overline{ac - \bar{b}d} \end{pmatrix} \in H,$$

so H is closed under addition and multiplication.

In order to prove that $H \setminus \{0\}$ is a group under multiplication, we must show, among other things, that matrices in $H \setminus \{0\}$ are invertible, so we must verify that their determinants are different from 0. If $A \in H$ and $\det A = 0$, say if $A = \begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix}$, then $0 = \det A = a\bar{a} + \bar{b}b = |a|^2 + |b|^2$ yields $a = 0$, $b = 0$ and this forces $A = \begin{pmatrix} 0 & \bar{0} \\ -0 & \bar{0} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0 \in H$. We see that 0 is the only matrix in H of determinant 0. So $H \setminus \{0\} \subseteq GL(2, \mathbb{C})$. Consequently, we can apply our subgroup criterion and check whether $H \setminus \{0\}$ is a subgroup of $GL(2, \mathbb{C})$.

(i) Let $A, B \in H \setminus \{0\}$. Then $AB \in H$ by the closure of H under multiplication. Also $\det A \neq 0$, $\det B \neq 0$ and $\det AB = (\det A)(\det B) \neq 0$. Since 0 is the only

matrix in H of determinant 0, from $AB \in H$ and $\det AB \neq 0$ we get $AB \neq 0$. So $AB \in H \setminus \{0\}$ and $H \setminus \{0\}$ is closed under multiplication.

(ii) Let $A = \begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix} \in H \setminus \{0\}$. Then $\det A = |a|^2 + |b|^2 \in \mathbb{R} \setminus \{0\}$. We put $d := 1/\det A \in \mathbb{R}$. Since $d \in \mathbb{R}$, we have $\bar{d} = d$ and

$$A^{-1} = \begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix}^{-1} = \begin{pmatrix} d\bar{a} & -d\bar{b} \\ db & da \end{pmatrix} = \begin{pmatrix} d\bar{a} & -d\bar{b} \\ \bar{d}b & \bar{d}a \end{pmatrix} = \begin{pmatrix} d\bar{a} & \overline{-db} \\ -(-\bar{d}b) & \bar{d}a \end{pmatrix} \in H.$$

Of course A^{-1} is invertible, so $A^{-1} \neq 0$, so $A^{-1} \in H \setminus \{0\}$. Therefore $H \setminus \{0\}$ is closed under forming inverses.

Hence $H \setminus \{0\}$ is a subgroup of $\text{GL}(2, \mathbb{C})$.

Problem: (18.2) *Let $H \leq G$. Prove that $H \trianglelefteq G$ if and only if $Ha \subseteq aH$ for all $a \in G$.*

If $H \trianglelefteq G$, then $Ha = aH$ for all $a \in G$, in particular $Ha \subseteq aH$ for all $a \in G$.

Conversely, suppose that, for all $a \in G$, we have $Ha \subseteq aH$. Fix any $a \in G$. We have $Ha^{-1} \subseteq a^{-1}H$, so for any $h \in H$, there holds $h^{-1}a^{-1} \in Ha^{-1} \subseteq a^{-1}H$ and there is an $h' \in H$ with $(ah)^{-1} = h^{-1}a^{-1} = a^{-1}h'$. Taking inverses, we find $ah = h'^{-1}a \in Ha$. Since $ah \in Ha$ for all $h \in H$, we get $aH \subseteq Ha$. The reverse inclusion holds by hypothesis, so $aH = Ha$. This holds for every $a \in G$, so $H \trianglelefteq G$.

Problem: (18.3) *Prove that, if $H \leq G$ and $a \in G$ and if Ha is a left coset of H in G , then $Ha = aH$*

In any case, since $a = 1a \in Ha$, we know that Ha is a subset of G that contains a . There is a unique left coset of H in G that contains a , namely aH , for distinct left cosets are disjoint. Therefore, if Ha happens to be a left coset of H in G , then it must be equal to the unique left coset aH of H in G that a belongs to.

Problem: (18.6) *Determine whether the following are normal subgroups in the groups indicated.*

$$\begin{aligned} A &:= \{g \in \text{GL}(2, \mathbb{R}) : \det g \geq 5\} && \text{in } \text{GL}(2, \mathbb{R}) \\ B &:= \{g \in \text{GL}(2, \mathbb{R}) : \det g \geq 0\} && \text{in } \text{GL}(2, \mathbb{R}) \\ C &:= \{g \in \text{GL}(2, \mathbb{R}) : \det g > 0\} && \text{in } \text{GL}(2, \mathbb{R}) \\ D &:= \{g \in \text{GL}(2, \mathbb{C}) : \det g = 1\} && \text{in } \text{GL}(2, \mathbb{C}) \\ E &:= \{g \in \text{GL}(2, \mathbb{C}) : (\det g)^{18} = 1\} && \text{in } \text{GL}(2, \mathbb{C}) \\ F &:= \{g \in \text{GL}(2, \mathbb{Z}_{11}) : \det g \in \{1, 3, 4, 5, 9\}\} && \text{in } \text{GL}(2, \mathbb{Z}_{11}) \end{aligned}$$

We have $g := \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix} \in A$ since $\det g = 8 \geq 5$, but $g^{-1} = \begin{pmatrix} 1/8 & 0 \\ 0 & 1 \end{pmatrix} \notin A$ since $\det(g^{-1}) = \frac{1}{\det g} = 1/8 < 5$. So A is not closed under the forming of inverses and A is not a subgroup of $\text{GL}(2, \mathbb{R})$. All the more so, A is not a normal subgroup of $\text{GL}(2, \mathbb{R})$.

We have $B = \{g \in \text{Mat}_2(\mathbb{R}) : \det g \neq 0 \text{ and } \det g \geq 0\} = \{g \in \text{Mat}_2(\mathbb{R}) : \det g > 0\} = \{g \in \text{GL}(2, \mathbb{R}) : \det g > 0\} = C$, so it is enough to examine C .

If $g, h \in C$, then $\det g > 0$ and $\det h > 0$. But then gh and g^{-1} are matrices in $\text{GL}(2, \mathbb{R})$ with $\det gh = (\det g)(\det h) > 0$ and $\det g^{-1} = (\det g)^{-1} > 0$. Therefore C is closed under multiplication and under forming inverses, so $C \leq \text{GL}(2, \mathbb{R})$. Besides, for any $x \in \text{GL}(2, \mathbb{R})$ and for any $g \in C$, we have $\det(x^{-1}gx) = (\det x)^{-1}(\det g)(\det x) = (\det x)^{-1}(\det x)(\det g) = \det g > 0$, so $x^{-1}gx \in C$. Thus $C \trianglelefteq \text{GL}(2, \mathbb{R})$.

We know that $D = \text{SL}(2, \mathbb{R}) \trianglelefteq \text{GL}(2, \mathbb{R})$ from Example 18.5(j)

If $g, h \in E$, then $(\det g)^{18} = 1$ and $(\det h)^{18} = 1$. But then gh and g^{-1} are matrices in $\text{GL}(2, \mathbb{C})$ with $(\det gh)^{18} = [(\det g)(\det h)]^{18} = (\det g)^{18}(\det h)^{18} = 1 \cdot 1 = 1$ and $(\det g^{-1})^{18} = [(\det g)^{-1}]^{18} = (\det g)^{-18} = [(\det g)^{18}]^{-1} = 1^{-1} = 1$. Therefore E is closed under multiplication and under forming inverses, so $E \leq \text{GL}(2, \mathbb{C})$. Besides, for any $x \in \text{GL}(2, \mathbb{C})$ and for any $g \in E$, we have $[\det(x^{-1}gx)]^{18} = [(\det x)^{-1}(\det g)(\det x)]^{18} = (\det g)^{18} = 1$, so $x^{-1}gx \in E$. Thus $E \trianglelefteq \text{GL}(2, \mathbb{C})$.

Put $T := \{1, 3, 4, 5, 9\} \subseteq \mathbb{Z}_{11}^\times$. The multiplication table

\cdot	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

shows that T is closed under multiplication. Since T is a finite subset of the group \mathbb{Z}_{11}^\times , it is a subgroup of \mathbb{Z}_{11}^\times . If $g, h \in F$, then $\det g \in T$ and $\det h \in T$. But then gh and g^{-1} are matrices in $\text{GL}(2, \mathbb{Z}_{11})$ with $\det gh = (\det g)(\det h) \in T$ and $\det g^{-1} = (\det g)^{-1} \in T$. Therefore F is closed under multiplication and under forming inverses, so $F \leq \text{GL}(2, \mathbb{Z}_{11})$. Besides, for any $x \in \text{GL}(2, \mathbb{Z}_{11})$ and for any $g \in F$, we have $\det(x^{-1}gx) = (\det x)^{-1}(\det g)(\det x) = (\det x)^{-1}(\det x)(\det g) = \det g \in T$, so $x^{-1}gx \in F$. Thus $F \trianglelefteq \text{GL}(2, \mathbb{Z}_{11})$.

Problem: (19.3) Let A, B, C be subgroups of a group G , with $A \leq C$. Prove that $A(B \cap C) = AB \cap C$.

Does the instructor believe that we take no look at his book? This is Lemma 27.12 on page 294.

Problem: (20.1) Show that the mapping $x \mapsto e^x$ is an isomorphism from $(\mathbb{R}, +)$ onto $(\mathbb{R}^{>0}, \cdot)$

The exponential function $\exp : \mathbb{R} \longrightarrow \mathbb{R}^{>0}$ has the inverse $\log : \mathbb{R}^{>0} \longrightarrow \mathbb{R}$, so it is one-to-one and onto. It is also a homomorphism, because $\exp(a+b) = e^{a+b} = e^a e^b = \exp(a) \exp(b)$ for all $a, b \in \mathbb{R}$. So \exp is an isomorphism.

Problem: (20.3) Find an isomorphism from $(\mathbb{Q} \setminus \{0\}, \cdot)$ onto the group $(\mathbb{Q} \setminus \{1\}, *)$, where $a * b = ab - a - b + 2$ for all $a, b \in \mathbb{Q} \setminus \{1\}$.

Consider the maps $\varphi : \mathbb{Q} \setminus \{0\} \longrightarrow \mathbb{Q} \setminus \{1\}$ and $\psi : \mathbb{Q} \setminus \{1\} \longrightarrow \mathbb{Q} \setminus \{0\}$ defined

by $a\varphi = a + 1$ for all $a \in \mathbb{Q}$, $a \neq 0$ and $x\psi = x - 1$ for all $x \in \mathbb{Q}$, $x \neq 1$. As

$$\begin{aligned} a\varphi\psi &= (a + 1)\psi = (a + 1) - 1 = a && \text{for all } a \in \mathbb{Q} \setminus \{0\}, \\ x\psi\varphi &= (x - 1)\varphi = (x - 1) + 1 = x && \text{for all } x \in \mathbb{Q} \setminus \{1\}, \end{aligned}$$

we have $\varphi\psi = \text{id}_{\mathbb{Q} \setminus \{0\}}$ and $\psi\varphi = \text{id}_{\mathbb{Q} \setminus \{1\}}$. So φ has an inverse function and φ is bijective. Since $a\varphi * b\varphi = (a + 1) * (b + 1) = (a + 1)(b + 1) - (a + 1) - (b + 1) + 2 = ab - a - b + 1 - a - 1 - b - 1 + 2 = ab + 1 = (ab)\varphi$ for any $a, b \in \mathbb{Q} \setminus \{0\}$, we see that φ is a homomorphism. Thus φ is an isomorphism from $\mathbb{Q} \setminus \{0\}$ onto $\mathbb{Q} \setminus \{1\}$.

Problem: (20.4) Find an isomorphism from $(\mathbb{Z}, +)$ onto the group $(\mathbb{Z}, *)$, where $a * b = a + b + 2$ for all $a, b \in \mathbb{Z}$.

Consider the maps $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ and $\psi : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $a\varphi = a - 2$ for all $a \in \mathbb{Z}$ and $x\psi = x + 2$ for all $x \in \mathbb{Z}$. As

$$\begin{aligned} a\varphi\psi &= (a - 2)\psi = (a - 2) + 2 = a && \text{for all } a \in \mathbb{Z}, \\ x\psi\varphi &= (x + 2)\varphi = (x + 2) - 2 = x && \text{for all } x \in \mathbb{Z}, \end{aligned}$$

we have $\varphi\psi = \text{id}_{\mathbb{Z}}$ and $\psi\varphi = \text{id}_{\mathbb{Z}}$. So φ has an inverse function and φ is bijective. Since $(a + b)\varphi = (a + b) - 2 = (a - 2) + (b - 2) + 2 = (a - 2) * (b - 2) = a\varphi * b\varphi$ for any $a, b \in \mathbb{Z}$, we see that φ is a homomorphism. Thus φ is an isomorphism from $(\mathbb{Z}, +)$ onto $(\mathbb{Z}, *)$.

Problem: (20.12) Let $n \in \mathbb{N}$ and let X be a set of n elements. Prove that $S_X \cong S_n$.

We put $Y := \{1, 2, \dots, n\}$. By definition, $S_n = S_Y$. By hypothesis, there is a bijection $\mu : X \rightarrow Y$. We know that μ has an inverse $\mu^{-1} : Y \rightarrow X$.

For any $\varphi \in S_X$, the composition $\mu^{-1}\varphi\mu$ is a bijection from Y onto Y , because inverses and compositions of bijective functions are bijective. Similarly, for any $\sigma \in S_Y$, the map $\mu\sigma\mu^{-1}$ is a bijection from X onto X . Hence there are functions

$$T : S_X \rightarrow S_Y, \quad \varphi T = \mu^{-1}\varphi\mu \quad \text{and} \quad U : S_Y \rightarrow S_X, \quad \sigma U = \mu\sigma\mu^{-1}.$$

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X \\ \mu^{-1} \uparrow & & \downarrow \mu \\ Y & & Y \end{array} \quad \begin{array}{ccc} X & & X \\ \mu^{-1} \uparrow & & \downarrow \mu \\ Y & \xleftarrow{\sigma} & Y \end{array}$$

φT and σU

As $\varphi T U = (\mu^{-1}\varphi\mu)U = \mu(\mu^{-1}\varphi\mu)\mu^{-1} = \varphi$ for all $\varphi \in S_X$ and $\sigma U T = (\mu\sigma\mu^{-1})T = \mu^{-1}(\mu\sigma\mu^{-1})\mu = \sigma$ for all $\sigma \in S_Y$, we have $TU = \text{id}_{S_X}$ and $UT = \text{id}_{S_Y}$. Thus φ is invertible and φ is a bijection. Also, φ is a homomorphism, because $(\varphi\psi)T = \mu^{-1}(\varphi\psi)\mu = \mu^{-1}\varphi\mu \cdot \mu^{-1}\psi\mu = \varphi T \psi T$ for all φ, ψ in S_X . Thus $T : S_X \rightarrow S_Y$ is an isomorphism and $S_X \cong S_Y = S_n$.

Problem: (20.13) Prove that $(\mathbb{R} \setminus \{0\})/\mathbb{R}^{>0} \cong C_2$.

The signum function $\text{sgn} : \mathbb{R} \setminus \{0\} \rightarrow \{1, -1\}$ is a homomorphism from the group $\mathbb{R} \setminus \{0\}$ (under ordinary multiplication) into the cyclic group $\{1, -1\}$ (under ordinary multiplication) of order 2, as we have seen in Example 20.2(e). Since $\text{Ker sgn} = \{x \in \mathbb{R} \setminus \{0\} : \text{sgn}(x) = 1\} = \{x \in \mathbb{R} : x > 0\}$ and $\text{Im sgn} = \{1, -1\} \cong C_2$, the formula

$$(\mathbb{R} \setminus \{0\})/\text{Ker sgn} \cong \text{Im sgn}$$

yields

$$(\mathbb{R} \setminus \{0\})/\mathbb{R}^{>0} \cong C_2.$$

Problem: (21.1) Let $A \trianglelefteq C \leq G$ and $B \leq G$. Prove that $A \cap B \trianglelefteq C \cap B$ and $(C \cap B)/(A \cap B) \cong A(C \cap B)/A$.

This is Lemma 27.13 on page 295.

Problem: (21.2) Let $A \trianglelefteq C \leq G$ and $B \leq G$ and let $\varphi : G \rightarrow H$ be a group homomorphism. Prove that $A\varphi \trianglelefteq C\varphi$. Choosing φ to be the natural homomorphism $\nu : G \rightarrow G/B$, prove that $AB \trianglelefteq G$.

By Theorem 20.6, we know that $A\varphi = \text{Im}(\varphi|_A)$ and $C\varphi = \text{Im}(\varphi|_C)$ are subgroups of H . Since $A \leq C$, we have $a \in C$ and $a\varphi \in C\varphi$ for any $a \in A$, therefore $A\varphi \subseteq C\varphi$. We obtain $A\varphi \leq C\varphi$.

Now let's prove that $A\varphi \trianglelefteq C\varphi$. Take any $x \in A\varphi$ and any $y \in C\varphi$. There are $a \in A$ with $x = a\varphi$ and $c \in C$ with $y = c\varphi$, so $y^{-1}xy = (c\varphi)^{-1}(a\varphi)(c\varphi) = (c^{-1}ac)\varphi$. But $A \trianglelefteq C$, so $c^{-1}ac \in A$ and $y^{-1}xy = (c^{-1}ac)\varphi \in A\varphi$. As $y^{-1}xy \in A\varphi$ for all $x \in A\varphi$ and for all $y \in C\varphi$, we infer that $A\varphi \trianglelefteq C\varphi$.

Let's take φ to be the natural homomorphism $\nu : G \rightarrow G/B$. We have

$$\begin{aligned} A\nu &= \{a\nu \in G/B : a \in A\} \\ &= \{Ba \in G/B : a \in A\} \\ &= \{Bba \in G/B : a \in A, b \in B\} \\ &= \{Bx \in G/B : x \in BA\} \\ &= \{Bx \in G/B : x \in AB\} \quad [\text{because } B \trianglelefteq G \text{ (see Lemma 19.4(2))}] \\ &= AB/B \end{aligned}$$

and similarly $C\nu = CB/B$. From $A\nu \trianglelefteq C\nu$, we get $AB/B \trianglelefteq CB/B$, and by Theorem 21.2, we get $AB \trianglelefteq CB$.

Problem: (22.2) Show that C_{mn} is not isomorphic to $C_m \times C_n$ if $(m, n) \neq 1$.

Let $l = [m, n]$ be the least common multiple of m and n . For any (a, b) in $C_m \times C_n$, we have $a \in C_m$, $a^m = 1 \in C_m$ and $a^l = 1$. Similarly $b^l = 1 \in C_n$. So $(a, b)^l = (a^l, b^l) = (1_{C_m}, 1_{C_n}) = 1_{C_m \times C_n}$ and $o(a, b) \mid l$. In particular, $o(a, b) \leq l$ for all $(a, b) \in C_m \times C_n$.

Suppose C_{mn} is isomorphic to $C_m \times C_n$. Then $C_m \times C_n$ is a cyclic group of order mn and there is a generator (a_0, b_0) of $C_m \times C_n$ having order $o(a_0, b_0) =$

$|C_m \times C_n| = mn$. By what we have found above, we get $mn = o(a_0, b_0) \leq l = \frac{mn}{(m,n)}$, so $(m, n) \leq 1$, so $(m, n) = 1$. Therefore, if C_{mn} is isomorphic to $C_m \times C_n$, then $(m, n) = 1$. Equivalently, if $(m, n) \neq 1$, then C_{mn} is not isomorphic to $C_m \times C_n$.

Problem: (22.3) Find three nonisomorphic abelian groups of order 8 and two nonisomorphic abelian groups of order 12.

$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ are three abelian groups of order 8. In C_8 , there is an element of order 8, whereas there is no element of order 8 in $C_4 \times C_2$, nor in $C_2 \times C_2 \times C_2$, so $C_8 \not\cong C_4 \times C_2$ and $C_8 \not\cong C_2 \times C_2 \times C_2$. Similarly, there is an element of order 4 in $C_4 \times C_2$, whereas every element of $C_2 \times C_2 \times C_2$ has order 1 or 2, so $C_4 \times C_2 \not\cong C_2 \times C_2 \times C_2$. Hence $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ are three nonisomorphic groups of order 8.

C_{12} and $C_6 \times C_2$ are two abelian groups of order 12. In C_{12} , there is an element of order 12, whereas there is no element of order 12 in $C_6 \times C_2$, so $C_{12} \not\cong C_6 \times C_2$. Hence C_{12} and $C_6 \times C_2$ are two nonisomorphic groups of order 12.

Problem: (22.6) Let H, K be normal subgroups of G . Find a one-to-one homomorphism from $G/(H \cap K)$ into $G/H \times G/K$.

Let's denote by \widehat{g} the coset of H in G determined by g , and by \overline{g} the coset of K in G determined by g . Thus $\widehat{g} = Hg \in G/H$ and $\overline{g} = Kg \in G/K$. Consider the function $\varphi : G \rightarrow G/H \times G/K$ that maps g to $(\widehat{g}, \overline{g})$. Since $(ab)\varphi = (\widehat{ab}, \overline{ab}) = (\widehat{a}\widehat{b}, \overline{a}\overline{b}) = (\widehat{a}, \overline{a})(\widehat{b}, \overline{b}) = a\varphi \cdot b\varphi$ for all $a, b \in G$, this function φ is a homomorphism. Its kernel is

$$\begin{aligned} \text{Ker } \varphi &= \{g \in G : g\varphi = 1 \in G/H \times G/K\} \\ &= \{g \in G : (\widehat{g}, \overline{g}) = (\widehat{1}, \overline{1})\} \\ &= \{g \in G : \widehat{g} = \widehat{1}, \overline{g} = \overline{1}\} \\ &= \{g \in G : Hg = H, Kg = K\} \\ &= \{g \in G : g \in H, g \in K\} \\ &= H \cap K. \end{aligned}$$

According to the fundamental theorem on homomorphisms (Theorem 20.15), the function $\psi : G/(H \cap K) \rightarrow G/H \times G/K$ given by $(H \cap K)g \mapsto g\varphi = (\widehat{g}, \overline{g}) = (Hg, Kg)$ is a one-to-one homomorphism.

$$\begin{array}{ccc} & G/(H \cap K) & \\ \nu \nearrow & & \searrow \psi \\ G & \xrightarrow{\varphi} & G/H \times G/K \end{array}$$

Alternatively, we could verify that

$$\psi : G/(H \cap K) \rightarrow G/H \times G/K, \quad (H \cap K)g \mapsto (Hg, Kg)$$

is well-defined, one-to-one and is a homomorphism.

Problem: (22.7) Let $\varphi_i : G_i \longrightarrow H_i$ be group homomorphisms ($i = 1, 2$). Define

$$\psi : G_1 \times G_2 \longrightarrow H_1 \times H_2, \quad (g_1, g_2) \mapsto (g_1\varphi_1, g_2\varphi_2).$$

Show that ψ is a homomorphism and $\text{Ker } \psi = \text{Ker } \varphi_1 \times \text{Ker } \varphi_2$ and $\text{Im } \psi = \text{Im } \varphi_1 \times \text{Im } \varphi_2$.

For any $(a, b), (c, d) \in G_1 \times G_2$, there holds

$$\begin{aligned} [(a, b)(c, d)]\psi &= (ac, bd)\psi = ((ac)\varphi_1, (bd)\varphi_2) \\ &= (a\varphi_1 \cdot c\varphi_1, b\varphi_2 \cdot d\varphi_2) = (a\varphi_1, b\varphi_2)(c\varphi_1, d\varphi_2) \\ &= (a, b)\psi \cdot (c, d)\psi, \end{aligned}$$

so ψ is a homomorphism.

The kernel of ψ is

$$\begin{aligned} \text{Ker } \psi &= \{(a, b) : (a, b)\psi = 1 \in H_1 \times H_2\} \\ &= \{(a, b) : (a\varphi_1, b\varphi_2) = (1_{H_1}, 1_{H_2})\} \\ &= \{(a, b) : a\varphi_1 = 1_{H_1}, b\varphi_2 = 1_{H_2}\} \\ &= \{(a, b) : a \in \text{Ker } \varphi_1, b \in \text{Ker } \varphi_2\} \\ &= \text{Ker } \varphi_1 \times \text{Ker } \varphi_2. \end{aligned}$$

The image of ψ is

$$\begin{aligned} \text{Im } \psi &= \{(a, b)\psi \in H_1 \times H_2 : (a, b) \in G_1 \times G_2\} \\ &= \{(a\varphi_1, b\varphi_2) \in H_1 \times H_2 : a \in G_1, b \in G_2\} \\ &= \{(x, y) \in H_1 \times H_2 : x = a\varphi_1 \text{ for some } a \in G_1, y = b\varphi_2 \text{ for some } b \in G_2\} \\ &= \{(x, y) \in H_1 \times H_2 : x \in \text{Im } \varphi_1, y \in \text{Im } \varphi_2\} \\ &= \text{Im } \varphi_1 \times \text{Im } \varphi_2. \end{aligned}$$

Problem: (29.2) Let $(R, +, \cdot)$ be a ring. On the group $(R, +)$, we define an operation \circ by declaring $a \circ b = ba$ for all $a, b \in R$. Show that $(R, +, \circ)$ is a ring.

All we have to do is to show that R is closed under \circ , that \circ is associative and distributive over addition. For any $a, b, c \in R$, we have

$$\begin{aligned} a \circ b &= ba \in R, \\ (a \circ b) \circ c &= (ba) \circ c = c(ba) = (cb)a = a \circ (cb) = a \circ (b \circ c), \\ a \circ (b + c) &= (b + c)a = ba + ca = a \circ b + a \circ c, \\ (b + c) \circ a &= a(b + c) = ab + ac = b \circ a + c \circ a, \end{aligned}$$

so R is indeed a ring with respect to $+$ and \circ .

Problem: (29.3) On the group $\mathbb{Z} \oplus \mathbb{Z}$, we define a multiplication by $(a, b)(c, d) = (ac, b)$ for all $(a, b), (c, d) \in \mathbb{Z} \oplus \mathbb{Z}$. Does $\mathbb{Z} \oplus \mathbb{Z}$ become a ring with this multiplication?

Since $(0, 1)[(0, 0) + (0, 0)] = (0, 1)(0, 0) = (0, 1) \neq (0, 2) = (0, 1) + (0, 1) = (0, 1)(0, 0) + (0, 1)(0, 0)$, the equation $(a, b)[(c, d) + (e, f)] = (a, b)(c, d) + (a, b)(e, f)$ is not true for all $(a, b), (c, d), (e, f)$ in $\mathbb{Z} \oplus \mathbb{Z}$. Therefore, $\mathbb{Z} \oplus \mathbb{Z}$ is not a ring with respect to the usual addition and this multiplication.

Problem: (29.7) *Let R be a ring without identity, and let $S = R \oplus \mathbb{Z}$. On the commutative group S , we define a multiplication by $(r, a)(r', b) = (rr' + ar' + br, ab)$ for all $(r, a), (r', b) \in S$. Prove that S is a ring with identity.*

First of all, we have to show that S is closed under multiplication and that the multiplication on S is associative and distributive over addition.

(i) Since R is a group under $+$, for any $n \in \mathbb{Z}$ and for any $r \in R$, we have $nr \in R$. Consequently, if $r, r' \in R$ and $a, b \in \mathbb{Z}$, then rr', ar', br and $rr' + ar' + br$ belong to R , and ab belongs to \mathbb{Z} . So

$$(r, a)(r', b) = (rr' + ar' + br, ab) \in R \times \mathbb{Z} = S \quad \text{for all } (r, a), (r', b) \in S$$

and S is closed under multiplication.

(ii) For all $(r, a), (r', b), (r'', c) \in S$, we have

$$\begin{aligned} [(r, a)(r', b)](r'', c) &= (rr' + ar' + br, ab)(r'', c) \\ &= ((rr' + ar' + br)r'' + (ab)r'' + c(rr' + ar' + br), (ab)c) \\ &= (rr'r'' + ar'r'' + br'r'' + (ab)r'' + crr' + car' + cbr, abc) \\ &= (r(r'r'' + br'' + cr') + a(r'r'' + br'' + cr') + (bc)r, a(bc)) \\ &= (r, a)(r'r'' + br'' + cr', bc) \\ &= (r, a)[(r', b)(r'', c)], \end{aligned}$$

so the multiplication on S is associative.

(iii) For all $(r, a), (r', b), (r'', c) \in S$, we have

$$\begin{aligned} (r, a)[(r', b) + (r'', c)] &= (r, a)(r' + r'', b + c) \\ &= (r(r' + r'') + a(r' + r'') + (b + c)r, a(b + c)) \\ &= (rr' + rr'' + ar' + ar'' + br + cr, ab + ac) \\ &= ((rr' + ar' + br) + (rr'' + ar'' + cr), ab + ac) \\ &= (rr' + ar' + br, ab) + (rr'' + ar'' + cr, ac) \\ &= (r, a)(r', b) + (r, a)(r'', c) \end{aligned}$$

and

$$\begin{aligned} [(r', b) + (r'', c)](r, a) &= (r' + r'', b + c)(r, a) \\ &= ((r' + r'')r + (b + c)r + a(r' + r''), (b + c)a) \\ &= (r'r + r''r + br + cr + ar' + ar'', ba + ca) \\ &= ((r'r + br + ar') + (r''r + cr + ar''), ba + ca) \\ &= (r'r + br + ar', ba) + (r''r + cr + ar'', ca) \\ &= (r', b)(r, a) + (r'', c)(r, a), \end{aligned}$$

so the multiplication on S is distributive over addition in S .

This shows that S is a ring. Does it have a (two-sided) identity? From

$$\begin{aligned}(r, a)(0, 1) &= (r0 + a0 + 1r, a1) = (r, a) && \text{for all } (r, a) \in S, \\ (0, 1)(r, a) &= (0r + 1r + a0, 1a) = (r, a) && \text{for all } (r, a) \in S,\end{aligned}$$

we see that $(0, 1)$ is an identity in S . Thus S is a ring with identity.

Problem: (30.1) *Let R be a ring. The center of R is defined to be the set $Z(R) = \{z \in R : za = az \text{ for all } a \in R\}$. Is $Z(R)$ a subring or an ideal of R ?*

First we apply the subring criterion in order to find out whether $Z(R)$ is a subring of R . Since $0a = 0 = a0$ for all $a \in R$, we have $0 \in Z(R)$ and $Z(R) \neq \emptyset$.

(i) If $z, u \in Z(R)$, then $za = az$ and $ua = au$ for all $a \in R$, so $(z + u)a = za + ua = az + au = a(z + u)$ for all $a \in R$, so $z + u \in Z(R)$, so $Z(R)$ is closed under addition.

(ii) If $z \in Z(R)$, then $za = az$ for all $a \in R$, so $(-z)a = -(za) = -(az) = a(-z)$ for all $a \in R$, so $-z \in Z(R)$, so $Z(R)$ is closed under forming opposites.

(iii) If $z, u \in Z(R)$, then $za = az$ and $ua = au$ for all $a \in R$, so $(zu)a = z(ua) = z(au) = (za)u = (az)u = a(zu)$ for all $a \in R$, so $zu \in Z(R)$, so $Z(R)$ is closed under multiplication.

Thus $Z(R)$ is a subring of R .

Let's find $Z(\text{Mat}_2(\mathbb{Z}))$. If $A := \begin{pmatrix} z & y \\ x & u \end{pmatrix} \in Z(\text{Mat}_2(\mathbb{Z}))$, then

$$\begin{aligned}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} z & y \\ x & u \end{pmatrix} &= \begin{pmatrix} z & y \\ x & u \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} z & y \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} z & 0 \\ x & 0 \end{pmatrix} \\ y = 0, x = 0\end{aligned}$$

and A is a diagonal matrix $\begin{pmatrix} z & 0 \\ 0 & u \end{pmatrix}$. Moreover,

$$\begin{aligned}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} z & 0 \\ 0 & u \end{pmatrix} &= \begin{pmatrix} z & 0 \\ 0 & u \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & z \\ 0 & 0 \end{pmatrix} \\ u = z\end{aligned}$$

and A is a scalar matrix $\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$. Therefore $Z(\text{Mat}_2(\mathbb{Z}))$ is a subset of the set

$\left\{ \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} : z \in \mathbb{Z} \right\}$ of scalar matrices. Conversely, if $\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$ is a scalar matrix, then

$$\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} za & zb \\ zc & zd \end{pmatrix} = \begin{pmatrix} az & bz \\ cz & dz \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(\mathbb{Z})$, so $\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} \in Z(\text{Mat}_2(\mathbb{Z}))$.

We found $Z(\text{Mat}_2(\mathbb{Z})) = \left\{ \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} : z \in \mathbb{Z} \right\}$. Since $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in Z(\text{Mat}_2(\mathbb{Z}))$, $\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \in \text{Mat}_2(\mathbb{Z})$ and $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 4 & 6 \end{pmatrix} \notin Z(\text{Mat}_2(\mathbb{Z}))$, we see that $Z(\text{Mat}_2(\mathbb{Z}))$ is not an ideal of $\text{Mat}_2(\mathbb{Z})$.

Thus $Z(R)$ is not necessarily an ideal of R .

Problem: (30.6) Show that if K is a field, then $\{0\}$ and K are the only ideals of K .

Take any ideal of K different from $\{0\}$ and call it A . Since $A \neq \{0\}$, there is an $a \in A$ with $a \neq 0$, and since $a \neq 0$, there is an inverse a^{-1} of a in K . As A has the absorbing property, and $a^{-1} \in K$ and $a \in A$, we have $1 = a^{-1}a \in A$. For any $k \in K$, we get then $k = k1 \in A$, so $K \subseteq A$, so $A = K$. Therefore K is the only ideal of K distinct from $\{0\}$.

Problem: (30.7) Let D be a division ring. Find all ideals of $\text{Mat}_2(D)$.

Let A be an ideal of $\text{Mat}_2(D)$ different from $\{0\}$. Then there exist $a, b, c, d \in D$, not all 0 $\in D$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A$. Then we get

$$\begin{aligned} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A, \\ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in A, \\ \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A, \\ \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in A, \end{aligned}$$

and

$$\begin{aligned} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in A, \\ \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} \in A, \\ \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in A. \end{aligned}$$

It follows that there is an $x \in \{a, b, c, d\}$ with $x \neq 0$ and $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in A$. Since

$x \in D \setminus \{0\} = D^\times$, there is an $x^{-1} \in D$ satisfying $xx^{-1} = 1$. We obtain

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & 0 \end{pmatrix} \in A, \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in A, \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in A \end{aligned}$$

and consequently

$$\text{for all } \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{Mat}_2(D) : \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A$$

and $\text{Mat}_2(D) \subseteq A$, so $A = \text{Mat}_2(D)$. This shows that $\{0\}$ and $\text{Mat}_2(D)$ are the only ideals of $\text{Mat}_2(D)$.

Problem: (30.13) *An element a in a ring R is said to be nilpotent if there is an $m \in \mathbb{N}$ such that $a^m = 0$. Prove that, if a and b are nilpotent elements in a ring and if $ab = ba$, then $a + b$ is nilpotent.*

By hypothesis, there are $m, n \in \mathbb{N}$ with $a^m = 0$ and $b^n = 0$. Since $ab = ba$, the usual binomial formula holds for the powers of $a + b$. In particular,

$$(a + b)^{m+n} = a^{m+n} + \binom{m+n}{1} a^{m+n-1} b + \dots + b^{m+n}$$

is a sum of terms of the form integer $\cdot a^{m+n-k} b^k$ with $0 \leq k \leq m+n$. For all such k , we have $m+n-k \geq m$ or $k \geq n$, so we have $a^{m+n-k} = a^m a^{n-k} = 0 a^{n-k} = 0$ or $b^k = b^n b^{k-n} = 0 b^{k-n} = 0$, so $a^{m+n-k} b^k = 0$ for all k . Each term on the right side of the binomial formula is 0 and $(a + b)^{m+n} = 0$. Thus $a + b$ is nilpotent, too.

Problem: (30.14) *Let R be a commutative ring. Show that the set N of nilpotent elements in R is an ideal of R and that the factor ring R/N has no nilpotent elements other than 0.*

Let's use the ideal criterion.

(i) Let $a, b \in N$. Since $ab = ba$, the previous problem yields that $a + b \in N$. So N is closed under addition.

(ii) If $a \in N$, there is an $m \in \mathbb{N}$ for which $a^m = 0$. We have $(-a)^m = a^m = 0$ or $(-a)^m = -a^m = -0 = 0$ according as m is even or odd. In any case, $(-a)^m = 0$ and $-a \in N$. So N is closed under the forming of opposites.

(iii) If $a \in N$, there is an $m \in \mathbb{N}$ for which $a^m = 0$, and for any $r \in R$, we have $(ar)^m = a^m r^m$ by the commutativity of multiplication. So $(ar)^m = a^m r^m = 0 r^m = 0$ for all $r \in R$ and $ra = ar \in N$. So N has the absorbing property, too.

Thus N is an ideal of R .

Suppose that the coset $r + N \in R/N$ is a nilpotent element of R/N . Then $(r + N)^m = 0 + N$ for some $m \in \mathbb{N}$. But $(r + N)^m = r^m + N$, so $r^m + N = 0 + N$ and $r^m \in N$. Therefore there is an $n \in \mathbb{N}$ with $(r^m)^n = 0$. This yields $r^{mn} = 0$, so $r \in N$, so $r + N = 0 + N$. Thus any nilpotent element of R/N is equal to the zero element of R/N .

Problem: (30.15) Find rings R, S with identities $1_R, 1_S$ respectively, and a ring homomorphism $\varphi : R \rightarrow S$ such that $(1_R)\varphi \neq 1_S$.

We know that \mathbb{Z} is a ring with identity 1, and $\text{Mat}_2(\mathbb{Z})$ is a ring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The mapping $\varphi : \mathbb{Z} \rightarrow \text{Mat}_2(\mathbb{Z})$, $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is a ring homomorphism, because

$$\begin{aligned} (a+b)\varphi &= \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = a\varphi + b\varphi \\ (ab)\varphi &= \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = a\varphi \cdot b\varphi \end{aligned}$$

for all $a, b \in \mathbb{Z}$. In this case, we have $1\varphi = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Problem: (30.16) If R, S are rings with identities $1_R, 1_S$ respectively, and if $\varphi : R \rightarrow S$ is a ring homomorphism onto S , prove that $(1_R)\varphi = 1_S$.

For any $s \in S$, there is an $r \in R$ with $r\varphi = s$, and there holds

$$\begin{aligned} 1\varphi \cdot r\varphi &= (1r)\varphi = r\varphi = (r1)\varphi = r\varphi \cdot 1\varphi, \\ 1\varphi \cdot s &= s = s \cdot 1\varphi, \end{aligned}$$

so 1φ is a two-sided identity of R . Since an identity of a ring, if it exists, is uniquely determined, and since 1_S is the identity of S , we get $1\varphi = 1_S$.

Problem: (31.1) Let $D_1 := \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$, $D_2 := \{a + 2bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$, $E := \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{C} : a, b, c \in \mathbb{Z}\}$. Show that D_1, D_2, E are integral domains and describe, as simply as you can, the elements in the field of fractions of these integral domains.

Partial solution

We define $\mathbb{Q}(i) := \{p + qi \in \mathbb{C} : p, q \in \mathbb{Q}\}$.

Let F_1 be the field of fractions of D_1 . Any element of F_1 has the form

$$\frac{a + bi}{c + di} = \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{(ac + bd) + (-ad + bc)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{-ad + bc}{c^2 + d^2} i \in \mathbb{Q}(i)$$

where $a, b, c, d \in \mathbb{Z}$ and c, d are not both 0. This proves $F_1 \subseteq \mathbb{Q}(i)$. On the other hand, any element of $\mathbb{Q}(i)$ has the form

$$p + qi = \frac{a}{b} + \frac{c}{d}i = \frac{ad + bci}{bd + 0i}$$

with $a, b, c, d \in \mathbb{Z}$, so $ad, bc, bd \in \mathbb{Z}$ and $p + qi \in F_1$. This proves $\mathbb{Q}(i) \subseteq F_1$. Hence $F_1 = \mathbb{Q}(i)$ and every element of F_1 has the form $p + qi$ where $p, q \in \mathbb{Q}$.

An analogous argument shows that the field of fractions of D_2 is also $\mathbb{Q}(i)$. As for E , you compute

$$\begin{aligned} \frac{a + b\sqrt[3]{2} + c\sqrt[3]{4}}{e + f\sqrt[3]{2} + g\sqrt[3]{4}} &= \frac{a + b\sqrt[3]{2} + c\sqrt[3]{4}}{e + f\sqrt[3]{2} + g\sqrt[3]{4}} \cdot \frac{e + f\sqrt[3]{2}\omega + g\sqrt[3]{4}\omega^2}{e + f\sqrt[3]{2}\omega + g\sqrt[3]{4}\omega^2} \cdot \frac{e + f\sqrt[3]{2}\omega^2 + g\sqrt[3]{4}\omega}{e + f\sqrt[3]{2}\omega^2 + g\sqrt[3]{4}\omega} \\ &= \frac{(a + b\sqrt[3]{2} + c\sqrt[3]{4})((e^2 - 2fg) + (2g^2 - eg)\sqrt[3]{2} + (f^2 - eg)\sqrt[3]{4})}{e^3 + 2f^3 + 4g^3 - 6efg} \end{aligned}$$

and conclude that the field of fractions F_E of E is contained in $\mathbb{Q}(\sqrt[3]{2}) := \{p + q\sqrt[3]{2} + r\sqrt[3]{4} \in \mathbb{R} : p, q, r \in \mathbb{Q}\}$. It is easier to show that $\mathbb{Q}(\sqrt[3]{2}) \subseteq F_E$. Hence every element of F_E has the form $p + q\sqrt[3]{2} + r\sqrt[3]{4}$, where $p, q, r \in \mathbb{Q}$.

Problem: Let D be an integral domain, a and b elements of D . Suppose that there are two relatively prime positive integers m, n such that $a^m = b^m$ and $a^n = b^n$. Show that $a = b$.

If $a = 0$, then $b^m = a^m = 0^m = 0$ and since D contains no zero divisors, we get $b = 0$. Thus $b = 0 = a$ in this case.

Suppose now $a \neq 0$. Since m and n are relatively prime, there are positive integers x, y such that $mx - ny = 1$. Then

$$\begin{aligned} aa^{ny} &= a^{1+ny} = a^{mx} = (a^m)^x = (b^m)^x = b^{mx} \\ &= b^{1+ny} = b(b^n)^y = b(a^n)^y = ba^{ny} \end{aligned}$$

and $(a - b)a^{ny} = 0$. Since D has no zero divisors and since $a \neq 0$, consequently $a^{ny} \neq 0$, we get $a - b = 0$. Thus $b = a$ in this case, too.

Problem: (31.3) Prove that, if D is a division ring, then $Z(D)$ is a field.

From Problem 31.1, we know that $Z(D)$ is a subring of D . In order to show that it is a field, we must show that it is commutative, has an identity, and that its nonzero elements have inverses in it.

(i) For any $z \in Z(D)$ and for any $u \in D$, we have $zu = uz$. Therefore we have $zu = uz$ for all $z \in D, u \in Z(D)$. Thus $Z(D)$ is commutative.

(ii) We know that D has an identity 1_D and $1_D z = z 1_D$ for all $z \in D$, in particular for all $z \in Z(D)$. So $1_D \in D$ and $1_D z = z 1_D$ for all $z \in Z(D)$. Thus $Z(D)$ is a ring with identity.

(iii) Any nonzero $z \in Z(D) \subseteq D$ has an inverse $z^{-1} \in D$, because D is a division ring. Moreover, the equation $zu = uz$ (for all $u \in D$) implies $z^{-1}u = z^{-1}uzz^{-1} = z^{-1}zuz^{-1} = uz^{-1}$ (for all $u \in D$), hence $z^{-1} \in Z(D)$. Therefore every nonzero element of $Z(D)$ has an inverse in $Z(D)$.

Hence $Z(D)$ is a field.

Problem: (30.11) Let R be a ring. An ideal P of R is said to be prime if $P \neq R$ and if, for any two ideals A, B of R , the implication

$$AB \subseteq P \implies A \subseteq P \text{ or } B \subseteq P$$

is valid, where $AB := \{\sum_{i=1}^n a_i b_i : a_i \in A, b_i \in B, n \in \mathbb{N}\}$. Prove the following statements.

(i) Let P be an ideal of R , $P \neq R$. If, for any $a, b \in R$,

$$ab \in P \implies a \in P \text{ or } b \in P,$$

then P is a prime ideal of R .

(ii) Let R be commutative. If P is a prime ideal of R , then for any $a, b \in R$,

$$ab \in P \implies a \in P \text{ or } b \in P.$$

(iii) If R is an integral domain, then $\{0\}$ is a prime ideal of R .

(iv) Let R be a commutative ring with identity and P an ideal of R . Then P is a prime ideal of R if and only if R/P is an integral domain.

(i) Let A and B be ideals of R such that $AB \subseteq P$. We wish to show that $A \subseteq P$ or $B \subseteq P$. In case $A \subseteq P$, there is nothing to prove. Assume therefore $A \not\subseteq P$ and take $a_0 \in A$ with $a_0 \notin P$. For every $b \in B$, we have $a_0b \in AB \subseteq P$, and our present hypothesis yields $a_0 \in P$ or $b \in P$; but “ $a_0 \in P$ ” is excluded by the choice of a_0 , so $b \in P$. This proves $B \subseteq P$.

For any ideals A and B of R , we see that $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$. This means that P is a prime ideal of R .

(ii) Let R be commutative, P a prime ideal of R . Take any $a, b \in R$ with $ab \in P$. Denoting by (x) the ideal of R generated by x (Example 30.6(h)), we get $(a)(b) \subseteq (ab) \subseteq P$, so $(a) \subseteq P$ or $(b) \subseteq P$ by primality of P , so $a \in P$ or $b \in P$.

(iii) From (i) and (ii), we learn that in a commutative ring R , in particular in an integral domain R , an ideal P is prime if and only if $ab \in P$ forces $a \in P$ or $b \in P$. Since an integral domain has no zero divisor, we always have $ab \in \{0\} \implies a \in \{0\}$ or $b \in \{0\}$, so $\{0\}$ is a prime ideal of R .

(iv) Suppose R is a commutative ring with identity and P is a prime ideal of R . By Example 30.9(c), R/P is a commutative ring with identity. Since P is prime, $P \neq R$ and $|R/P| \neq 1$ and R/P is not the null ring. In order to prove that R/P is an integral domain, all we have to do is show that R/P has no zero divisors. Since $ab \in P \implies a \in P$ or $b \in P$ (for all $a, b \in R$), we have $\bar{a} \cdot \bar{b} = \bar{0} \implies \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ (for all $\bar{a} = a + P \in R/P$ and $\bar{b} = b + P \in R/P$), so indeed R/P has no zero divisors. This proves that R/P is an integral domain.

Conversely, let R be a commutative ring with identity and P an ideal of R such that R/P is an integral domain. Then R/P is not the null ring, so $|R/P| \neq 1$ and $P \neq R$. Also, R/P has no zero divisor, i.e., for any $a, b \in R$, we have

$$(a + P)(b + P) = 0 + P \implies a + P = 0 + P \text{ or } b + P = 0 + P \quad (\text{in } R/P),$$

or, equivalently,

$$ab \in P \implies a \in P \text{ or } b \in P;$$

this shows, in virtue of (i), that P is a prime ideal of R .

Problem: (32.1) Let D be an integral domain and $\pi \in D$, $\pi \neq 0$, $\pi \notin D^\times$. Prove that π is a prime element of D if and only if $D\pi$ is a prime ideal of D .

$$\begin{aligned}
\pi \text{ is a prime element of } D &\iff \forall a, b \in D, \pi \mid ab \implies \pi \mid a \text{ or } \pi \mid b \\
&\iff \forall a, b \in D, ab \in D\pi \implies a \in D\pi \text{ or } b \in D\pi \\
&\iff D\pi \text{ is a prime ideal of } D,
\end{aligned}$$

the last statement being a consequence of (i) and (ii) in the previous problem (Problem 30.11).

Problem: (32.2) *Let D be a principal ideal domain and $\pi \in D$, $\pi \neq 0$, $\pi \notin D^\times$. Prove that π is an irreducible element of D if and only if $D\pi \subset D$ and there is no ideal A of D satisfying $D\pi \subset A \subset D$.*

$$\begin{aligned}
\pi \text{ is irreducible in } D &\iff \pi \notin D^\times \text{ and there is no } \alpha \in D \text{ with } \alpha \neq 1, \alpha \neq \pi, \alpha \mid \pi \\
&\iff D\pi \neq D \text{ and there is no } \alpha \in D \text{ with } D\alpha \neq D, D\alpha \neq D\pi, D\pi \subseteq D\alpha \\
&\iff D\pi \subset D \text{ and there is no } \alpha \in D \text{ with } D\pi \subset D\alpha \subset D \\
&\iff D\pi \subset D \text{ and there is no ideal } A \text{ of } D \text{ with } D\pi \subset A \subset D,
\end{aligned}$$

since any ideal A of D is a principal ideal, that is to say, an ideal of the form $D\alpha$ with some suitable $\alpha \in D$.

Problem: (32.7) *Find the decomposition into irreducible elements of 2 in $\mathbb{Z}[i]$ and of 3 in $\mathbb{Z}[\omega]$.*

First we show that, if $\alpha \in \mathbb{Z}[i]$ (or $\alpha \in \mathbb{Z}[\omega]$) and $N(\alpha)$ is prime in \mathbb{Z} , then α is irreducible in $\mathbb{Z}[i]$ (or in $\mathbb{Z}[\omega]$). Indeed, if $N(\alpha)$ is a prime number, then $N(\alpha) \neq 0$ and $N(\alpha) \neq 1$, so $\alpha \neq 0$ and α is not a unit in $\mathbb{Z}[i]$ (or in $\mathbb{Z}[\omega]$). Besides, from any factorization $\alpha = \beta\gamma$ of α in $\mathbb{Z}[i]$ (or in $\mathbb{Z}[\omega]$), we get $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$, and as $N(\alpha)$ is a prime number, one of the positive integers $N(\beta)$, $N(\gamma)$ must equal 1, so β or γ must be a unit in $\mathbb{Z}[i]$ (or in $\mathbb{Z}[\omega]$). Hence α has no nontrivial factorization and α is irreducible in $\mathbb{Z}[i]$ (or in $\mathbb{Z}[\omega]$).

Now it is easy to find the decomposition of 2 and 3.

We note

$$2 = 1^2 + 1^2 = N(1 + i) = (1 + i)(1 - i) = (1 + i) \cdot (-i)(1 + i) = (-i)(1 + i)^2,$$

where $1 + i \in \mathbb{Z}[i]$, having the prime norm 2, is irreducible in $\mathbb{Z}[i]$. Thus $2 \in \mathbb{Z}[i]$ is associate to the square of an irreducible element of $\mathbb{Z}[i]$.

Similarly,

$$\begin{aligned}
3 &= 1^2 - 1 \cdot (-1) + (-1)^2 = N(1 - \omega) = (1 - \omega)(1 - \omega^2) \\
&= (1 - \omega) \cdot (-\omega^2)(1 - \omega) = -\omega^2(1 - \omega)^2,
\end{aligned}$$

where $1 - \omega \in \mathbb{Z}[\omega]$, having the prime norm 3, is irreducible in $\mathbb{Z}[\omega]$. Thus $3 \in \mathbb{Z}[\omega]$ is associate to the square of an irreducible element of $\mathbb{Z}[\omega]$.

Problem: (33.4) Let R be a commutative ring with identity and let $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a zero-divisor in $R[x]$. Show that there is a $b \neq 0$ in R such that $ba_n = ba_{n-1} = \cdots = ba_1 = ba_0 = 0$.

By hypothesis, there is a nonzero polynomial, say $b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$ such that

$$(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0)(b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0) = 0.$$

This polynomial equation yields

$$\begin{aligned} a_0 b_0 &= 0 \\ a_0 b_1 + a_1 b_0 &= 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 \\ \cdots &= 0 \\ a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0 &= 0. \end{aligned}$$

On multiplying the second equation by b_0 , the third by b_0^2 , \dots , $(n+1)$ st equation by b_0^n , we find

$$\begin{aligned} a_0 b_0 &= 0 \\ a_0 b_0 b_1 + a_1 b_0^2 &= 0 \\ a_0 b_0^2 b_2 + a_1 b_0^2 b_1 + a_2 b_0^3 &= 0 \\ \cdots &= 0 \\ a_0 b_0^n b_n + a_1 b_0^n b_{n-1} + a_2 b_0^n b_{n-2} + \cdots + a_n b_0^{n+1} &= 0, \end{aligned}$$

from which we successively get

$$\begin{aligned} a_0 b_0 &= 0 \\ a_1 b_0^2 &= 0 \\ a_2 b_0^3 &= 0 \\ \cdots &= 0 \\ a_n b_0^{n+1} &= 0. \end{aligned}$$

On setting $b := b_0^{n+1}$, we get $ba_0 = ba_1 = ba_2 = \cdots = ba_n = 0$.

This is fine in case $b_0^{n+1} \neq 0$. The assertion must be established differently if $b_0^{n+1} = 0$, but it is too long to appear as an exam question!

Problem: (34.6) Find a content of

$$\begin{aligned} 65x^4 + 26x^2 - 9x + 143 &\in \mathbb{Z}[x] \\ (5+i)x^3 + (-1+5i)x + (-4+7i) &\in (\mathbb{Z}[i])[x] \\ (1+\omega)x^4 + (-1+2\omega)x^3 + (1-2\omega)x^2 + 3x + (2+3\omega) &\in (\mathbb{Z}[\omega])[x] \\ 8x^4 + 24x^3 - 32x^2 - 48x + 56 &\in \mathbb{Q}[x] \\ 3x^2 + 5x + 7 &\in \mathbb{Z}_{97}[x]. \end{aligned}$$

A greatest common divisor of the numbers $65 = 5 \cdot 13$, $26 = 2 \cdot 13$, $-9 = (-1)3 \cdot 3$ and $143 = 11 \cdot 13$ is 1, therefore a content of $65x^4 + 26x^2 - 9x + 143$ is 1.

Since $5 + i$ and $-1 + 5i = -i(5 + i)$ are associate in $\mathbb{Z}[i]$, a greatest common divisor of $5 + i$, $-1 + 5i$ and $-4 + 7i$ is the same thing as a greatest common divisor of $5 + i$ and $-4 + 7i$. We can use the euclidean algorithm to find it. We have

$$\frac{-4 + 7i}{5 + i} = \frac{-4 + 7i}{5 + i} \frac{5 - i}{5 - i} = \frac{-13 + 39i}{26} = -\frac{1}{2} + \frac{3}{2}i$$

and we can choose 0 and 2 as closest integers to $-1/2$ and $3/2$ (other choices are possible in this particular case). So we have

$$\frac{-4 + 7i}{5 + i} = (0 + 2i) + \left(-\frac{1}{2} - \frac{1}{2}i\right)$$

and multiplying by $5 + i$, we get the first equation in our euclidean algorithm:

$$-4 + 7i = (2i)(5 + i) + (-2 - 3i).$$

To find the next equation, we compute

$$\frac{5 + i}{2 + 3i} = \frac{5 + i}{2 + 3i} \frac{2 - 3i}{2 - 3i} = \frac{13 - 13i}{13} = 1 - i$$

and obtain

$$5 + i = (-1 + i)(-2 - 3i) + 0.$$

Therefore the euclidean algorithm consists of two equations only:

$$\begin{aligned} -4 + 7i &= (2i)(5 + i) + (-2 - 3i) \\ 5 + i &= (-1 + i)(-2 - 3i) + 0 \end{aligned}$$

with $-2 - 3i$ as the last nonzero remainder. Hence $-2 - 3i$ (or $2 + 3i$) is a greatest common divisor of $5 + i$, $-4 + 7i$ and a content of $(5 + i)x^3 + (-1 + 5i)x + (-4 + 7i) \in (\mathbb{Z}[i])[x]$.

As $1 + \omega = -\omega^2$ is a unit in $\mathbb{Z}[\omega]$, a greatest common divisor of the elements $1 + \omega$, $-1 + 2\omega$, $1 - 2\omega$, 3 , $2 + 3\omega$ of $\mathbb{Z}[\omega]$ is necessarily a unit, so a content of $(1 + \omega)x^4 + (-1 + 2\omega)x^3 + (1 - 2\omega)x^2 + 3x + (2 + 3\omega)$ is 1.

The numbers 8, 24, -32 , -48 , 56 are all units in \mathbb{Q} , so a content of $8x^4 + 24x^3 - 32x^2 - 48x + 56$ in \mathbb{Q} is 1.

Since 97 is a prime number, \mathbb{Z}_{97} is a field, its elements 3, 5, 7 are units and a content of $3x^2 + 5x + 7$ is $1 \in \mathbb{Z}_{97}$.