101 Discrete Algebraic Structures
Stack Exchange

Karl-Heinz Zimmermann
Hamburg University of Technology
21071 Hamburg, Germany

November 3, 2017

Abstract

The problems treated in this report are from the website "Mathematics Stack Exchange". This is a question-and-answer website, where questions, answers, and users are subject to a reputation award process. The questions are strongly related to the two-hour lecture "Discrete Algebraic Structures" including a two-hour lab held for first-year Bachelor students of Computer Science at the Hamburg University of Technology. The problems encountered should give some deeper insight into the field. Enjoy the read!

Contents

Prof. Dr. Karl-Heinz Zimmermann
Hamburg University of Technology
21071 Hamburg
Germany

urn:nbn:de:gdv:830-88217195

Chapter 1

Propositional Logic

1. Let P, Q, and R be propositions. Show that the implications $(P \Rightarrow Q) \Rightarrow R$ and $P \Rightarrow (Q \Rightarrow R)$ are not logically equivalent.

   Proof. Suppose all three propositions are false. Then $((f \Rightarrow f) \Rightarrow f) \equiv (t \Rightarrow f) \equiv f$ and $(f \Rightarrow (f \Rightarrow f)) \equiv (f \Rightarrow t) \equiv t$. □

2. How to prove $(P \Leftrightarrow Q) \Leftrightarrow (P \vee Q) \Rightarrow (P \wedge Q)$?

   Proof. Truth table:

P	Q	$P \Leftrightarrow Q$	$P \vee Q$	$P \wedge Q$	$(P \vee Q) \Rightarrow (P \wedge Q)$
0	0	1	0	0	1
0	1	0	1	0	0
1	0	0	1	0	0
1	1	1	1	1	1

   Transformation:

$$\begin{aligned} (P \Leftrightarrow Q) &\Leftrightarrow (\neg P \wedge \neg Q) \vee (P \wedge Q) \quad \text{(check)} \\ &\Leftrightarrow \neg(P \vee Q) \vee (P \wedge Q) \quad \text{(De Morgan)} \\ &\Leftrightarrow (P \vee Q) \Rightarrow (P \wedge Q) \quad \text{(check).} \end{aligned}$$

   □

Chapter 2

Sets

1. Let A and B be sets. Simplify $(A \setminus B) \cap B$.

   Explanation. We have

   $$\begin{aligned} x \in (A \setminus B) \cap B &\iff x \in A \setminus B \wedge x \in B \\ &\iff (x \in A \wedge x \notin B) \wedge x \in B \\ &\iff x \in A \wedge (x \notin B \wedge x \in B). \end{aligned}$$

   The assertion $(x \notin B \wedge x \in B)$ is false and so the whole assertion is false. Thus $(A \setminus B) \cap B = \emptyset$. ♢

2. Why isn't it true that $M \cap P(M) = \emptyset$ for all sets M?

   Explanation. Each power set $P(M)$ contains the empty set $\emptyset$. So if $\emptyset \in M$, then $\emptyset$ is a common element of M and $P(M)$.

   For instance, if $M = \{\emptyset, \{\emptyset\}\}$, then $P(M) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ and so $M \cap P(M) = M$. ♢

3. Let A and B be subsets of a universe U. Show that if $A \cup B = U$ and $A \cap B = \emptyset$, then $A = \overline{B}$, where $\overline{B} = U \setminus B$.

   Proof. For each $A \subseteq U$, we have $\overline{A} = U \setminus A$.

   We have $A \cup B = U$ and so by De Morgan, $\overline{A} \cap \overline{B} = \emptyset$. Adding A at both sides gives $A \cup (\overline{A} \cap \overline{B}) = A \cup \emptyset = A$. Thus $A \cup \overline{B} = A$ and hence $\overline{B} \subseteq A$. Similarly, $A \subseteq \overline{B}$. Hence, $A = \overline{B}$. □

4. Let A and B be subsets of a universe U. Show that $A \setminus (A \setminus B) = B \setminus (B \setminus A)$.

Proof. Write $\overline{B} = U \setminus B$. Then we have

$$\begin{aligned} A \setminus (A \setminus B) &= A \setminus (A \cap \overline{B}) \\ &= A \cap \overline{(A \cap \overline{B})} \\ &= A \cap (\overline{A} \cup B) \\ &= (A \cap \overline{A}) \cup (A \cap B) \\ &= \emptyset \cup (A \cap B) \\ &= A \cap B. \end{aligned}$$

Similarly, $B \setminus (B \setminus A) = B \cap A$. Hence, both sets are equal. □

5. Let A, B, and C be subsets of a universe U. Show that $(A \setminus B) \cup (B \setminus C) = (A \cup B) \cap (A \cup \overline{C}) \cap \overline{B \cap C}$.

Proof. We have

$$\begin{aligned} &(A \setminus B) \cup (B \setminus C) \\ &= (A \cap \overline{B}) \cup (B \cap \overline{C}) \\ &= ((A \cap \overline{B}) \cup B) \cap ((A \cap \overline{B}) \cup \overline{C}) \\ &= ((A \cup B) \cap (\overline{B} \cup B)) \cap ((A \cup \overline{C}) \cap (\overline{B} \cup \overline{C})) \\ &= (A \cup B) \cap (A \cup \overline{C}) \cap (\overline{B} \cup \overline{C}) \\ &= (A \cup B) \cap (A \cup \overline{C}) \cap \overline{B \cap C}. \end{aligned}$$

□

6. Let A and B be subsets of a universe U. Show that if $\overline{A} \subseteq B$, then $\overline{B} \subseteq A$.

Proof. Note that the inclusion $\overline{A} \subseteq B$ means $\forall x \in U[x \notin A \Rightarrow x \in B]$. Equivalently, by contrapostion, $\forall x \in U[x \notin B \Rightarrow x \in A]$.

Let $b \in U$ with $b \in \overline{B}$. Then $b \notin B$. Thus (above) $b \in A$ and hence $\overline{B} \subseteq A$. □

7. Let A, B, and C be subsets of a universe U. Prove $A \setminus (\overline{B} \cup \overline{C}) \subseteq B \cap C$.

Proof. We have

$$\begin{aligned} x \in A \setminus (\overline{B} \cup \overline{C}) &\Leftrightarrow x \in A \wedge x \notin \overline{B} \cup \overline{C} \\ &\Leftrightarrow x \in A \wedge x \in \overline{\overline{B} \cup \overline{C}} \quad \text{(tertium non datur)} \\ &\Leftrightarrow x \in A \wedge x \in B \cap C \quad \text{(De Morgan)} \\ &\Leftrightarrow x \in A \wedge (x \in B \wedge x \in C) \quad (P \wedge Q \Rightarrow Q) \\ &\Rightarrow x \in B \wedge x \in C. \end{aligned}$$

□

8. Let A, B and C be sets. Prove that $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Proof. We have $(a, b) \in A \times (B \setminus C)$ iff $a \in A$ and $b \in B \setminus C$ iff $(a, b) \in A \times B$ and $(a, b) \notin A \times C$ iff $(a, b) \in (A \times B) \setminus (A \times C)$. $\square$

Chapter 3

Relations

1. If A is a non-empty set, the empty relation on A is not reflexive.

   Proof. Since A is non-empty, there is an element $a \in A$. If R is the empty relation, then aRa does not hold. Hence, R is not reflexive. □

2. The empty relation on a set A is symmetric and transitive.

   Proof. Symmetry and transitivity are defined by conditional statements. In case of the empty relation, the antecedents of these statements are false making the whole statements true. □

3. Consider the binary relation on the real numbers,

   $$xRy \quad :\Longleftrightarrow \quad x - y \in \mathbb{Z}, \quad x, y \in \mathbb{R}.$$

   This is an equivalence relation. Describe the equivalence classes.

   Explanation. We have xRy iff $x - y = k$ for some integer k. That means, $x = y + k$ for some integer k. Thus the equivalence class of $y \in \mathbb{R}$ is the set of all elements of the form $y + k$, where k ranges over the integers; i.e., $\bar{y} = \{y + k \mid k \in \mathbb{Z}\}$. ♢

4. Find the transitive closure of the binary relation

   $$R = \{(a, a), (b, b), (b, c), (c, a), (c, c)\}.$$

   Explanation. The transitive closure of R is $R^+ = \bigcup_{n \geq 1} R^n$. We have

   $$\begin{aligned} R^2 &= R \circ R = \{(b, c), (b, a), (c, a)\}, \\ R^3 &= R^2 \circ R = \{(b, a), (b, c), (b, a), (c, a)\}, \end{aligned}$$

   and so on. We obtain $R^+ = R \cup \{(b, a)\}$. ♢

5. An equivalence relation R has three equivalence classes of sizes 8, 10, and 12. What is the cardinality of the relation R?

   Explanation. The relation R is the disjoint union of its classes. Thus the size of R is $8 + 10 + 12 = 30$. ♢

6. Let X be a subset of $\mathbb{Z}$. Define a relation $\equiv$ on the power set 2^X such that for all elements $A, B \in 2^X$, $A \equiv B$ if and only if the sum of the elements in A equals the sum of the elements in B. Show that $\equiv$ is an equivalence relation and for $X = \{0, 1, 2, 3\}$ write down the equivalence classes.

   Explanation. It is easy to check that the relation is reflexive, transitive, and symmetric. The equivalence classes are defined by the possible values of the sums of elements of the subsets of X. We have $0, 1, \ldots, 6$ as possible values. Thus the equivalence classes are as follows:

   $$\{\emptyset, \{0\}\},$$
   $$\{\{1\}, \{0, 1\}\},$$
   $$\{\{2\}, \{0, 2\}\},$$
   $$\{\{3\}, \{1, 2\}, \{0, 3\}, \{0, 1, 2\}\},$$
   $$\{\{1, 3\}, \{0, 1, 3\}\},$$
   $$\{\{2, 3\}, \{0, 2, 3\}\},$$
   $$\{\{1, 2, 3\}, \{0, 1, 2, 3\}\}.$$

   ♢

7. If $R = \{(a, 2a) \mid a \in \mathbb{Z}\}$ and $S = \{(b, 3b) \mid b \in \mathbb{Z}\}$, then $R \circ S = \{(c, 6c) \mid c \in \mathbb{Z}\}$.

   Proof. Put $M = \{(c, 6c) \mid c \in \mathbb{Z}\}$. Let $(a, 2a) \in R$ with $a \in \mathbb{Z}$. Then $(2a, 6a) = (2a, 3(2a)) \in S$ and so by composition $(a, 6a) \in R \circ S$. Thus $R \circ S \subseteq M$.

   Conversely, let $(c, 6c) \in M$ with $c \in \mathbb{Z}$. Since $(c, 2c) \in R$ and $(2c, 6c) = (2c, 3(2c)) \in S$, we obtain by composition $(c, 6c) \in R \circ S$. Thus $M \subseteq R \circ S$. □

8. Find the transitive closure of the binary relation $R = \{(i, j) \in \mathbb{N}_0 \mid i - 10 = j\}$.

   Explanation. The transitive closure of R is $R^+ = \bigcup_{n \geq 1} R^n$; its the smallest transitive relation containing R. For instance, $(10, 0) \in R$ and $(20, 10) \in R$, so $(20, 0) \in R^2$. By induction, one can show that for each $n \geq 1$, $R^n = \{(i, j) \in \mathbb{N}_0 \mid i - n \cdot 10 = j\}$. ♢

9. Consider the partially ordered set (poset) $(\{0,1\}^n, \leq_n)$, where $x \leq_n y$ means that $x_i \leq y_i$ for all $1 \leq i \leq n$. What is the largest chain of this poset?

   Explanation. For $n = 3$, we have $(1,0,0) \leq_3 (1,0,1)$ but not $(1,0,0) \leq_3 (0,1,0)$. An example of a longest chain is

   $$(1,0,0,\ldots,0) \leq_n (1,1,0,\ldots,0) \leq_n \ldots \leq_n (1,\ldots,1,0) \leq_n (1,1,\ldots,1).$$

   Each longest chain has $n+1$ elements. $\diamondsuit$

Chapter 4

Induction

1. Let a be an odd positive integer. Show that for each integer $n \geq 1$, a^n is odd.

   Proof. Base case $n = 1$: $a^1 = a$ is odd.
   Induction step $n \geq 1$: Let a^n be odd for $n \geq 1$. Then $a^{n+1} = a \cdot a^n$ is also odd, since the product of two odd numbers is also odd. □

2. Prove that if $a+1/a$ is an integer for some real number a, then a^n+a^{-n} is an integer for each $n \geq 2$.

   Proof. Base case $n = 2$: $a^2 + a^{-2} = (a + 1/a)^2 - 2$ is an integer.
   Induction step $n \geq 2$: $a^{n+1} + a^{-(n+1)} = (a^n + a^{-n})(a + 1/a) - (a^{n-1} + a^{-(n-1)})$ is an integer. □

3. Define the integer sequence $(a_n)_{n\geq 1}$ recursively by $a_1 = 1$, $a_2 = 4$, $a_3 = 9$, and $a_n = a_{n-1} - a_{n-2} + a_{n-3} + 2(2n - 3)$ for all $n \geq 4$. Show that $a_n = n^2$ for all $n \geq 1$.

   Proof. Base case: $a_1 = 1^2 = 1$, $a_2 = 2^2 = 4$, and $a_3 = 3^2 = 9$.
   Induction step $n \geq 3$: $a_{n+1} = a_n - a_{n-1} + a_{n-2} + 2(2(n + 1) - 3)$ by definition. By induction, the last expression equals $n^2 - (n - 1)^2 + (n - 2)^2 + 4n - 2$, which simplifies to $n^2 + 2n + 1$ and equals $(n + 1)^2$ as claimed. □

4. Define the sequence $(s_n)_{n\geq 0}$ as follows: $s_0 = 0$, $s_1 = 4$, and $s_n = 6s_{n-1} - 5s_{n-2}$ for all $n \geq 2$. Show that $s_n = 5^n - 1$ for all $n \geq 0$.

   Proof. Base case: $s_0 = 5^0 - 1 = 1$ and $s_1 = 5^1 - 1 = 4$.
   Induction step $n \geq 2$: We have $s_n = 6s_{n-1} - 5s_{n-2}$. By induction, $s_n = (5+1) \cdot (5^{n-1} - 1) - 5 \cdot (5^{n-2} - 1) = 5^n - 5 + 5^{n-1} - 1 - 5^{n-1} + 5 = 5^n - 1$. □

5. Prove that for any integer $b \geq 0$, if $2^{3b-1} + 5 \cdot 3^b$ is divisible by 11, then $2^{3(b+2)-1} + 5 \cdot 3^{b+2}$ is divisible by 11. Does the statement "$2^{3b-1} + 5 \cdot 3^b$ is divisible by 11" hold for each even or each odd natural number b?

   Proof. Let $P(b)$ be the assertion that $2^{3b-1} + 5 \cdot 3^b$ is divisible by 11. We show that $P(b) \Rightarrow P(b+2)$. Indeed, we have

   $$2^{3(b+2)-1} + 5 \cdot 3^{b+2} = 64 \cdot 2^{3b-1} + 9 \cdot 5 \cdot 3^b = 55 \cdot 2^{3b-1} + 9 \cdot (2^{3b-1} + 5 \cdot 3^b),$$

   since $64 = 55 + 9$. So if $P(b)$ holds, the right-hand side is divisible by 11. Hence, $P(b+2)$ holds.

   For $b = 1$, $2^{3b-1} + 5 \cdot 3^b = 19$ and for $b = 2$, $2^{3b-1} + 5 \cdot 3^b = 77$. Thus the statement "$2^{3b-1} + 5 \cdot 3^b$ is divisible by 11" holds for each even natural number $b \geq 2$. □

6. Show that $4^n - 1$ is divisible by 3.

   Proof. Base step $n = 0$: 3 divides $4^0 - 1 = 0$.
   Induction step $n \geq 0$: We have $4^{n+1} - 1 = 4 \cdot 4^n - 1 = 3 \cdot 4^n + (4^n - 1)$. By induction, 3 divides $4^n - 1$. Since 3 divides $3 \cdot 4^n$, 3 divides also $4^{n+1} - 1$. □

Chapter 5

Numbers (Summation)

1. How would I express the quantity $|1+1+1|+|1+1-1|+|1+1+1|+|1-1+1|+|1-1-1|+|-1+1+1|+|-1+1-1|+|-1-1+1|+|-1-1-1|$ in summation notation?

   Explanation. $\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1}|(-1)^i+(-1)^j+(-1)^k|$
   or $\sum_{a=\pm1}\sum_{b=\pm1}\sum_{c=\pm1}|a+b+c|$
   or $\sum_{n=0}^{7}|(-1)^{\lfloor n/4\rfloor}+(-1)^{\lfloor n/2\rfloor}+(-1)^n|$, where $\lfloor x\rfloor$ is the largest integer smaller than or equal to x. ♢

2. How to prove that $2^0+2^1+2^2+\ldots+2^n=2^{n+1}-1$?

   Proof. Express each power 2^k in binary. You get kth bit 1 and the rest is 0. When you sum up these numbers, you get a number with all bits 1. Adding 1 to this number yield a number with most significant bit 1 and the rest is 0.

   Example ($n=6$):

2^0	0000001
2^1	0000010
2^2	0000100
2^3	0001000
2^4	0010000
2^5	0100000
2^6	1000000
$\sum$	1111111
$+$	1
2^7	10000000

   □

3. If $a^2+b^2=c^2$ and c is even, prove that a and b are both even.

Proof. Let c be even. Then $c^2 = 4n$ for some integer n. Now if a and b are both odd, then $a^2 + b^2 = (2k+1)^2 + (2l+1)^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4m + 2$ for some numbers k, l, and m. But $4m + 2$ is not divisible by 4 and so $a^2 + b^2$ cannot be even. Similarly, if a is even and b is odd or a is odd and b is even, then $a^2 + b^2$ is odd. □

4. Show that $\frac{200!}{(10!)^{20}}$ is an integer.

Proof. Let m and n be natural numbers. Then $(mn)!$ is divisible by $(n!) \cdot (m!)^n$. To see this, the following product divides $(mn)!$:

$$\begin{array}{rcrcrcr} mn & \cdot & (m-1)n & \cdot & (m-2)n & \cdots & 1n \\ m(n-1) & \cdot & (m-1)(n-1) & \cdot & (m-2)(n-1) & \cdots & 1(n-1) \\ \vdots & & \vdots & & \vdots & & \\ m2 & \cdot & (m-1)2 & \cdot & (m-2)2 & \cdots & 2 \\ m & \cdot & (m-1) & \cdot & (m-2) & \cdots & 1 \end{array}$$

Each row is divisible by $m!$ and since there are n rows, the product is divisible by $(m!)^n$. Moreover, the product of the factors in the last column is $n!$.

Put $n = 20$ and $m = 10$. Then $\frac{200!}{20!(10!)^{20}}$ is an integer. Multiplying by $20!$ shows that $\frac{200!}{(10!)^{20}}$ is an integer. □

5. My six-year old asked me tonight about the last number before the googolplex. How does a math-challenged dad answer this?

Explanation. The googolplex is $10^{\left(10^{100}\right)}$. The last integer before this number is

$$10^{\left(10^{100}\right)} - 1 = \underbrace{999999\ldots999999}_{10^{100}\text{ digits of nine}}.$$

This number is so large that even if every digit of nine could be written using just one electron, then one would still need one hundred billion billion copies of the universe just to write down this number! ♢

6. Show that for each integer $n \geq 1$, $\prod_{k=0}^{n} \binom{n}{k} = (n!)^{n+1} / \prod_{k=0}^{n} (k!)^2$.

Proof. We have $\prod_{k=0}^{n} \binom{n}{k} = \prod_{k=0}^{n} \frac{n!}{k!(n-k)!}$. Since $\prod_{k=0}^{n}(n-k)! = \prod_{k=0}^{n} k!$, we get $\prod_{k=0}^{n} \binom{n}{k} = \prod_{k=0}^{n} \frac{n!}{(k!)^2} = (n!)^{n+1} \prod_{k=0}^{n} \frac{1}{(k!)^2}$ as claimed. □

7. Show that $|x|^p \leq p^p(e^x + e^{-x})$ for all $x \in \mathbb{R}$ and $p > 0$.

Proof. By symmetry between the cases $x > 0$ and $x < 0$, we may assume that $x > 0$. The case $x = 0$ is trivial. Claim that

$$\left(\frac{x}{p}\right)^p < \left(\exp\frac{x}{p}\right)^p = e^x < e^x + e^{-x}.$$

Indeed, the left-hand inequality holds because

$$t < 1 + t + \frac{1}{2}t^2 + \frac{1}{6}t^3 + \ldots = \exp t$$

for all $t > 0$. The right-hand inequality holds because e^{-x} is positive for all x. Multiplying both sides by p^p gives the requested result. □

8. Give a combinatorial proof of the identity $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Proof. Since $\binom{n}{k} = \binom{n}{n-k}$, we obtain $\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}$. Consider a committee consisting of n Democrats and n Republicans, and one will choose a subcommittee of n members. For this, one may choose k Democrats and $n-k$ Republicans in $\binom{n}{k} \cdot \binom{n}{n-k}$ ways. The sum then gives the total number of ways to choose n out of $2n$. □

9. Determine which of the numbers $\sqrt{2}^{\sqrt{3}}$ and $\sqrt{3}^{\sqrt{2}}$ is greater.

Explanation. Consider $\sqrt{2}^{\sqrt{3}}$ vs. $\sqrt{3}^{\sqrt{2}}$. Taking logarithms gives $(\sqrt{3}/2)\ln 2$ vs. $(\sqrt{2}/2)\ln 3$. Multiplying by 2 yields $\sqrt{3}\ln 2$ vs. $\sqrt{2}\ln 3$ and by rearranging $\sqrt{3/2}$ vs. $(\ln 3)/(\ln 2) = \log_2 3$. Now $2^{\sqrt{3/2}} < 2^{3/2} = 2\sqrt{2} < 3$. Thus $\sqrt{3/2} < \log_2 3$ and hence we conclude that $\sqrt{2}^{\sqrt{3}} < \sqrt{3}^{\sqrt{2}}$ by chasing back the comparisons. Note that $\sqrt{2}^{\sqrt{3}} = 1.585$ and $\sqrt{3}^{\sqrt{2}} = 2.175$. ♢

10. Compare π^e and e^π.

Explanation. We use the facts that $\pi \neq e$ and $e^x > 1 + x$ for $x \neq 0$. We have $e^{\pi/e-1} > 1 + (\pi/e - 1) = \pi/e$ and so $e^{\pi/e} > \pi$. Thus $e^\pi > \pi^e$. Note that is proof is not specific to π. Note that $e^\pi = 23.141$ and $\pi^e = 22.459$. ♢

11. Is there an elementary proof that for $n > 1$, $\sum_{k=1}^{n} \frac{1}{k}$ is never an integer?

Proof. There is a unique denominator 2^K having maximal power of 2, upon multiplying all terms through by 2^{K-1} one deduces the contra-

diction that $1/2 = c/d$ with d odd. For instance,

$$\begin{aligned} m &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{\mathbf{1}}{\mathbf{4}} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} \\ 2m &= 2 + 1 + \frac{2}{3} + \frac{\mathbf{1}}{\mathbf{2}} + \frac{2}{5} + \frac{2}{6} + \frac{2}{7} \\ -\frac{1}{2} &= 2 + 1 + \frac{2}{3} - 2m + \frac{2}{5} + \frac{2}{6} + \frac{2}{7}. \end{aligned}$$

Here we have $K = 2$. The right-hand side of the last equation has all odd denominators and so reduces to a fraction with odd denominator $d = 3 \cdot 5 \cdot 7$. □

12. Show that the set of all finite subsets of $\mathbb{N}$ is countable.

Proof. Consider an enumeration of the prime numbers by $n \mapsto p_n$. Then a subset $\{n_1, \ldots, n_k\}$ of $\mathbb{N}$ is mapped to the product $p_{n_1} \cdots p_{n_k}$.

For instance, if we enumerate the primes increasingly with $p_1 = 2$, $p_2 = 3$, and so on, then $\{1, 3, 4\} \mapsto p_1 \cdot p_3 \cdot p_4 = 2 \cdot 5 \cdot 7 = 70$.

To complete the proof, one needs the facts that there are countably infinite many prime numbers and the uniqueness of prime factorization. Then the mapping is well-defined and one-to-one. It is easy to check that the mapping is onto and hence a bijection. □

Chapter 6

Fibonacci Numbers

The sequence of Fibonacci numbers $(f_n)_{n\geq 0}$ is defined by $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-2} + f_{n-1}$ for $n \geq 2$. The first few entries of the sequence are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

1. Show that any positive integer can be expressed as a sum of distinct Fibonacci numbers, no two of which have consecutive Fibonacci indices. For instance, $79 = 55 + 21 + 3$.

   Proof. Base case: It holds for the number $f_1 = 1$.
   Induction step for $n \geq 2$. Suppose by induction any number between 1 and f_n can be written as given. Claim that any number between 1 and f_{n+1} can be written as given. Indeed, we must only prove it for numbers between f_n and f_{n+1}. For this, pick an number a between f_n and f_{n+1}. It can be written as $a = f_n + b$, where b is a number between 1 and f_{n-1} by definition of the Fibonacci sequence. Since b is smaller than f_n, it can be written as sum of distinct Fibonacci not including f_n. So when we add the Fibonacci numbers in b with f_n, we get the desired representation of a. □

2. Show that the nth Fibonacci number f_n satisfies $f_n > 2n$ for $n > 7$.

   Proof. Base case: It holds for $f_8 = 21 > 2 \cdot 8 = 16$.
   Induction step for $n \geq 8$. We have $f_{n+1} = f_n + f_{n-1}$ and so by induction, $f_{n+1} > 2n + 2(n-1) = 4n - 2 > 2(n+1)$. □

3. Prove that the squares of the Fibonacci numbers satisfy the recurrence relation $a_{n+3} - 2a_{n+2} - 2a_{n+1} + a_n = 0$, and solve this recurrence relation with the correct initial conditions.

   Proof. We show that $a_n = f_n^2$ for all $n \geq 0$ with (base case) $a_0 = f_0^2 = 0$ and $a_1 = f_1^2 = 1$.

Induction step: $f_{n+3}^2 = (f_{n+2} + f_{n+1})^2 = f_{n+2}^2 + 2f_{n+2}f_{n+1} + f_{n+1}^2 = a_{n+2} + f_{n+2}(f_{n+2} - f_n) + (f_{n+1} + f_n)f_{n+1} + a_{n+1} = a_{n+2} + f_{n+2}^2 - f_{n+2}f_n + f_{n+1}^2 + f_n f_{n+1} + a_{n+1} = 2a_{n+2} + 2a_{n+1} + f_n(-f_{n+2} + f_{n+1}) = 2a_{n+2} + 2a_{n+1} - f_n^2 = 2a_{n+2} + 2a_{n+1} - a_n$. Thus we get $a_{n+3} = 2a_{n+2} + 2a_{n+1} - a_n$. □

4. Show that the nth term in the Fibonacci sequence satisfies Binet's formula

$$f_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}, \quad n \geq 0.$$

Proof. Using the golden ratio $\phi = \frac{1}{2}(1+\sqrt{5})$, the formula can be written as

$$f_n = \frac{1}{\sqrt{5}}(\phi^n - (-\phi)^{-n}),$$

since $\frac{1}{2}(1-\sqrt{5}) = -\phi^{-1}$.
Base case: correct for $n = 0, 1$.
Induction step for $n \geq 2$:

$$\begin{aligned} f_{n+2} - f_{n+1} - f_n = & \\ = & \frac{1}{\sqrt{5}}[\phi^{n+2} - (-\phi)^{-n-2} - \phi^{n+1} + (-\phi)^{-n-1} - \phi^n + (-\phi)^{-n}] \\ = & \frac{1}{\sqrt{5}}[\phi^n(\phi^2 - \phi - 1) - (-\phi)^{-n}(\phi^2 - \phi - 1)]. \end{aligned}$$

But $\phi^2 - \phi - 1 = 0$ and so the expression is zero. □

5. Prove that $\lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \frac{1}{2}(1+\sqrt{5})$.

Proof. Write $a = 1+\sqrt{5}$ and $b = 1-\sqrt{5}$. Then by Binet's formula, $f_n = \frac{1}{2^n\sqrt{5}}(a^n - b^n)$ for each $n \geq 0$. Thus

$$\frac{f_{n+1}}{f_n} = \frac{1}{2}\frac{a^{n+1} - b^{n+1}}{a^n - b^n} = \frac{1}{2}\frac{a - \frac{b^{n+1}}{a^n}}{1 - \frac{b^n}{a^n}}.$$

Since $\left|\frac{b}{a}\right| < 1$, we have $\frac{b^n}{a^n} \to 0$ and $\frac{b^{n+1}}{a^n} = \frac{b^n}{a^n}b \to 0$ as $n \to \infty$. □

Chapter 7

Functions

1. What is the domain of the function $f(x) = \sqrt{2x-8}$ defined on the real numbers?

   Explanation. The square root expression must be nonnegative to give a real number. We have $2x - 8 \geq 0$ iff $x \geq 4$. Hence, the domain is $[4, \infty)$. ♢

2. What is the range of the function $f(x) = \frac{2x-1}{x+2}$ for $x \in [-1, 2]$?

   Explanation. We have

   $$\frac{2x-1}{x+2} = \frac{2x+4-5}{x+2} = 2 - \frac{5}{x+2}.$$

   Thus, since $-1 \leq x \leq 2$, we obtain

   $$2 - \frac{5}{-1+2} \leq 2 - \frac{5}{x+2} \leq 2 - \frac{5}{2+2}$$

   or

   $$-3 \leq \frac{2x-1}{x+2} \leq \frac{3}{4}.$$

   ♢

3. Find real-valued functions f and g with the properties that $\mathrm{dom}(fg) = \mathbb{R}$ and $\mathrm{dom}(gf) = \emptyset$.

   Explanation. Suppose the domain of fg (first g, then f) is $\mathbb{R}$. Then g is defined for all real numbers. By hypothesis, f is defined for at least one value, say $x_0 = g(12) \in \mathbb{R}$. Since g is defined for all real numbers, it is defined at $f(x_0)$. Thus gf is defined at x_0 and hence its domain cannot be $\emptyset$. ♢

4. Is the function $f : \mathbb{Z} \to [0, 1]$ defined by $f(z) = z\pi - \lfloor z\pi \rfloor$ injective?

   Explanation. Let $f(z) = f(z')$ for some integers z, z'. Then $z\pi - \lfloor z\pi \rfloor = z'\pi - \lfloor z'\pi \rfloor$ and so $(z - z')\pi = \lfloor z\pi \rfloor - \lfloor z'\pi \rfloor$. But the left-hand side is irrational and the right-hand side is an integer from which it follows that f is one-to-one. ♢

5. Is the real-valued function $f(x) = \frac{1-x^2}{4+x^2}$ bounded?

   Explanation. Rewrite

$$f(x) = \frac{5 - (4 + x^2)}{4 + x^2} = -1 + \frac{5}{4 + x^2}.$$

   So the tightest possible bound is

$$-1 < f(x) \leq -1 + \frac{5}{4} = \frac{1}{4}.$$

   ♢

6. Can the inverse of a real-valued function be the same as the original function?

   Explanation. If $g(x) = 2 - x$, then $g^{-1}(y) = 2 - y$, since $(g^{-1}g)(x) = g^{-1}(2 - x) = 2 - (2 - x) = x$; similarly, $(gg^{-1})(x) = x$. Another function is $f(x) = \frac{1}{x} = f^{-1}(x)$. ♢

7. Determine whether the integral functions $f(m, n) = m^2 - n^2$ and $g(m, n) = 6m - 27n$ are surjective?

   Proof. In view of the function f, not every integer can be expressed as $m^2 - n^2 = (m - n)(m + n)$. For instance, the integer 6 cannot written this way. Hence, the function is not onto.

   In view of the function g, we have $6m - 27n = 3(2m - 9n)$. Thus each function value is a multiple of 3 and hence the function is not onto. □

8. Find the compositions fg and gf for the real-valued functions $f(x) = \sqrt{1 - \sin(x)}$ and $g(x) = \frac{x}{1+x}$.

   Explanation. We have

$$f(g(x)) = \sqrt{1 - \sin \frac{x}{1 + x}}$$

   with domain $\mathbb{R} \setminus \{-1\}$ and

$$g(f(x)) = \frac{\sqrt{1 - \sin x}}{1 + \sqrt{1 - \sin x}}$$

   with domain $\mathbb{R}$. ♢

9. How to compare a^b and b^a when a, b are real-valued and positive.

   Explanation. Suppose we want to determine if $a^b < b^a$. Taking logarithms gives $b \log a < a \log b$ or $\frac{\log a}{a} < \frac{\log b}{b}$. Using $f(x) = (\log x)/x$ we obtain $f(a) < f(b)$. The function f is increasing on $x < e$ and decreasing on $x > e$.

   If $a < b < e$ or $e < b < a$, then $a^b < b^a$. For instance, $4^3 < 3^4$ for $e < 3 < 4$.

   If $a < e < b$, then $f(a)$ and $f(b)$ need to be compared. For instance, $f(5) \approx 0.322$ and $f(2) \approx 0.347$. Thus $f(5) < f(2)$ and so $5^2 < 2^5$. ♢

10. Can we find real numbers x and y such that $x^x = y^y$?

    Explanation. Consider the function $\mathbb{R}_{\geq 0} \to \mathbb{R} : x \mapsto x^x$ in the sub-domain $[0, 1]$. Here you will find $x, y \in [0, 1]$ with $x^x = y^y$. For instance, $0^0 = 1 = 1^1$ using $\lim_{x^+ \to 0} x^x = 1$. ♢

11. Solve $x^y = y^x$ for positive integers x and y.

    Explanation. For instance, we have $2^4 = 4^2$. Is there any other pair of positive integers x, y with $x \neq y$?

    Suppose $x^y = y^x$ with $x > y > 0$. Taking logarithms gives $y \log x = x \log y$ and thus $(\log x)/x = (\log y)/y$. Consider the function $f(x) = (\log x)/x$. Then the equality becomes $f(x) = f(y)$. The function f is increasing for $x < e$ and decreasing for $x > e$. So if $x^y = y^x$ has a solution, then $x > e > y$. Thus y must be 1 or 2. But $y = 1$ doesn't work and $y = 2$ gives $x = 4$. ♢

12. Let C be a positive real number. Why does $Ce^x = e^{x + \ln C}$ hold for any real number x.

    Explanation. The e-function and the ln-function are inverse to each other. Thus we have $Ce^x = e^{\ln(Ce^x)} = e^{\ln C + \ln e^x} = e^{\ln C + x}$. ♢

13. Find a bijection between $(0, 1)$ and $(0, 1]$.

    Explanation. Take the set $X = \{\frac{1}{n} \mid n \in \mathbb{N}\}$. Then X is a subset of $(0, 1]$ and so we can define the mapping $f : (0, 1] \to (0, 1)$ by setting $f\left(\frac{1}{n}\right) = f\left(\frac{1}{n+1}\right)$ for all $n \in \mathbb{N}$ and $f(x) = x$ for all $x \in (0, 1] \setminus X$. It is clear that f is bijective. ♢

14. Is there a bijective map from $(0, 1)$ to $\mathbb{R}$?

    Explanation. The map $f : (-\pi/2, \pi/2) \to \mathbb{R} : x \mapsto \tan x$ is a bijection. By shifting and scaling, the map $f : (0, 1) \to \mathbb{R} : x \mapsto \tan(\pi x - \pi/2)$ is bijective. The map $f : (0, 1) \to \mathbb{R} : x \mapsto \ln(1/x - 1)$

is bijective with inverse $g(y) = 1/(1+e^y)$. The map $f : (0,1) \to \mathbb{R} : x \mapsto \ln(-\ln(x))$ is bijective with inverse $g(y) = e^{-e^y}$. ♢

15. How can the real numbers be bijectively mapped to the irrationals?

Explanation. Let $(a_i)_{i\geq 0}$ be an enumeration of the rationals and $(b_i)_{i\geq 0}$ be a countable sequence of irrationals such as $b_i = \frac{1}{2^i}\sqrt{2}$ for all $i \geq 0$. Then define the mapping $f : \mathbb{R} \to (\mathbb{R} \setminus \mathbb{Q})$ by

$$f(x) = \begin{cases} b_{2i} & \text{if } x \text{ is rational with } x = a_i \text{ for some } i, \\ b_{2i+1} & \text{if } x \text{ is irrational with } x = b_i \text{ for some } i, \\ x & \text{otherwise.} \end{cases}$$

This mapping is bijective (Cantor, 1877). ♢

16. Show that $M = \{A \subseteq \mathbb{N} \mid A \text{ or } \mathbb{N} \setminus A \text{ is finite}\}$ is countable.

Proof. Let $M_{\text{fin}} = \{A \subseteq \mathbb{N} \mid A \text{ is finite}\}$ and $M_{\text{cof}} = \{A \subseteq \mathbb{N} \mid A^c = \mathbb{N} \setminus A \text{ is finite}\}$.

The mapping $f : M_{\text{fin}} \to M_{\text{cof}}$ defined by $A \mapsto A^c$ is a bijection. Thus M_{fin} and M_{cof} have the same cardinality. Moreover, $M = M_{\text{fin}} \cup M_{\text{cof}}$ and so for proving that M is countable it is enough to prove that M_{fin} is countable.

Write $M_{\text{fin}} = \bigcup_{n\geq 0} M_n$ where M_n denotes the collection of all subsets of $\mathbb{N}$ that have cardinality n. For each $n \geq 0$, the set M_n is countable and so the set M as a countable union of countable sets is also countable. □

Chapter 8

Algebraic Operations

1. Is there a binary operation with $a * (a * a) \neq (a * a) * a$?

   Explanation. Consider the set of integers $\mathbb{Z}$ together with the binary operation $(m, n) \mapsto m - n$. Then $(n * n) * n = (n - n) - n = -n$ and $n * (n * n) = n - (n - n) = n$ for all $n \in \mathbb{Z}$.

   Consider the set of positive reals $\mathbb{R}_{>0}$ together with the binary operation $(x, y) \mapsto x^y$. Then $(x * x) * x = (x^x)^x$ and $x * (x * x) = x^{(x^x)}$. Take $x = 3$ to see that both expressions are different.

   Consider the set of positive reals $\mathbb{R}_{>0}$ together with the binary operation $(x, y) \mapsto x/y$. Then $(x * x) * x = (x/x)/x = 1/x$ and $x * (x * x) = x/(x/x) = x$.

   An operation with $a*(a*a) \neq (a*a)*a$ cannot be commutative, since taking $b = a * a$ gives $a * b \neq b * a$.

2. Given the binary operation $x \odot y = x + y + xy$ on $\mathbb{R}$. Show that for each $n \geq 2$ and $x \in \mathbb{R}$, $x^{\odot^n} = (1 + x)^n - 1$.

   Proof. Note that the operation $\odot$ is commutative and associative. The associativity allows to evaluate powers $x^{\odot^n}$ in any order.
   Base case: $x^{\odot^2} = x \odot x = 2x + x^2 = (1 + x)^2 - 1$.
   Induction step for $n \geq 2$: $x^{\odot^{n+1}} = x^{\odot^n} \odot x = ((1 + x)^n - 1) \odot x = (1 + x)^n - 1 + x + ((1 + x)^n - 1)x = (1 - x)^n(1 + x) - 1 + x - x = (1 - x)^{n+1} - 1$. □

3. Is the binary operation $a * b = \frac{1}{2}ab$ on $\mathbb{Q}$ both commutative and associative?

   Explanation. The operation is commutative, since $a * b = \frac{1}{2}ab = \frac{1}{2}ba = b * a$.

The operation is associative, since

$$\begin{aligned}(a * b) * c &= \left(\frac{1}{2}ab\right) * c = \frac{1}{2}\left(\frac{1}{2}ab\right)c = \frac{1}{2}a\left(\frac{1}{2}bc\right) \\ &= a * \left(\frac{1}{2}bc\right) = a * (b * c).\end{aligned}$$

4. Is the Boolean XOR operation both commutative and associative?

Explanation. The XOR operation is commutative, since

a	b	$a \oplus b$	$b \oplus a$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

The XOR operation is associative, since

a	b	c	$a \oplus b$	$(a \oplus b) \oplus c$	$b \oplus c$	$a \oplus (b \oplus c)$
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	1
0	1	1	1	0	0	0
1	0	0	1	1	0	1
1	0	1	1	0	1	0
1	1	0	0	0	1	0
1	1	1	0	1	0	1

5. Has the following operation on $\mathbb{R}$ an identity element?

$$x * y = \min\{x + 1, y + 1\} = \min\{x, y\} + 1.$$

Explanation. The identity element $e \in \mathbb{R}$ must satisfy $x*e = e*x = x$; that is, $\min\{x, e\} + 1 = \min\{e, x\} + 1 = x$ for all $x \in \mathbb{R}$. For a specific $x_0 \in \mathbb{R}$, this requires that $e \geq x_0 - 1$. For another element $x_1 \in \mathbb{R}$, we need $e \geq x_1 - 1$. Thus there is no unique element $e \in \mathbb{R}$ such that for all $x \in \mathbb{R}$, $x * e = x = e * x$. $\diamondsuit$

Chapter 9

Monoids

1. Let M be a commutative monoid. Show that

$$U = \{a \in M \mid a^k \text{ is idempotent for some } k \geq 1\}$$

is a submonoid of M.

Proof. An element $a \in M$ is idempotent if $a^2 = a$. Let $a, b \in U$, i.e., a^k and b^l are idempotent for some $k, l \geq 1$. Then $(ab)^{kl}$ is idempotent, since $(ab)^{kl}(ab)^{kl} = (a^{2k})^l(b^{2l})^k = (a^k)^l(b^l)^k = (ab)^{kl}$. Thus $ab \in U$. Moreover, the identity element $e \in M$ is idempotent, since $e^2 = e$, and so lies in U. □

2. Let M be a finite monoid. Does M admit a surjection from a free monoid?

Explanation. Consider the monoid $(M, \cdot, e)$ and take the free monoid Σ^* with alphabet $\Sigma = M$. The elements of Σ^* are the strings $a_1a_2 \ldots a_k$ with $a_i \in M$, $1 \leq i \leq k$, $k \geq 0$. The mapping

$$\phi : \Sigma^* \to M : a_1a_2 \ldots a_k \mapsto a_1 \cdot a_2 \cdot \ldots \cdot a_k$$

is surjective and a homomorphism.

As an example, take the commutative monoid $M = \{e, a\}$ with unit element e and $a^2 = a$. Put $\Sigma = M$. The surjection $\phi : \Sigma^* \to M$ maps $eeee$ to e and $eaeaa$ to $a^3 = a$. ♢

3. Prove that the monoid $(\mathbb{R}^{n\times n}, \cdot)$ is isomorphic to the opposite monoid $(\mathbb{R}^{n\times n}, *)$, where $M * N = N \cdot M$ for all $M, N \in \mathbb{R}^{n\times n}$.

Proof. The mapping $\phi : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ defined by matrix transposition $\phi(M) = M^t$ is a bijection. Moreover, let $M, N \in \mathbb{R}^{n\times n}$. Then $\phi(M \cdot N) = (M \cdot N)^t = N^t \cdot M^t = M^t * N^t = \phi(M) * \phi(N)$. Finally, the identity matrix $I \in \mathbb{R}^{n\times n}$ satisfies $\phi(I) = I^t = I$. □

Chapter 10

Groups

1. Let G be a group with $a^2 = a$ for all $a \in G$. Is the group G abelian?

   Explanation. Let $a, b \in G$. We have $abab = ab$ and so $aba = a$, which gives both $ab = e$ and $ba = e$.

   As an example, consider the Klein four-group $V_4 = \{e, a, b, c\}$ which is isomorphic to $S_2 \times S_2$. ♢

2. Find a group G and three proper subgroups H, K, and L such that $G = H \cup K \cup L$.

   Explanation. The Klein-4 group $V_4 = \{e, a, b, c\}$ has subgroups $H = \{e, a\}$, $K = \{e, b\}$, and $L = \{e, c\}$ and so satisfies the above equality. ♢

3. Let G be a group. Show that the function $f : G \to G$ defined by $x \mapsto x^{-1}$ is bijective.

   Proof. In view of injectivity, let $a^{-1} = b^{-1}$. Multiplying both sides of this equation by b on the right gives $a^{-1}b = b^{-1}b = e$. Multiplying both sides of this equation by a on the left yields $aa^{-1}b = ae = a$, which gives $b = a$.

   In view of surjectivity, take $b \in G$. Then $f(b^{-1}) = (b^{-1})^{-1} = b$ and so b^{-1} is the preimage of b. □

4. Define the binary operation $\oplus$ as $a \oplus b = a + b + 3ab$. Show that $Q = \mathbb{Q} \setminus \{-\frac{1}{3}\}$ forms together with $\oplus$ an abelian group.

   Proof. The operation is well-defined, since we deal only with elementary operations in $\mathbb{Q}$ which are closed in $\mathbb{Q}$.

We must check if the result can be $-\frac{1}{3}$. If so, we get $a+b+3ab = -\frac{1}{3}$. Then $1+3a+3b+9ab = 0$ and so $(1+3a)(1+3b) = 0$ which cannot happen since $a, b \in Q$. Hence, the operation is closed in Q.

The operation is associative as it is easy to check that $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ for all $a, b, c \in Q$.

The operation is commutative, since $a \oplus b = a+b+3ab = b+a+3ba = b \oplus a$ for all $a, b \in Q$.

The neutral element is $e = 0$, since $a \oplus e = a + e + 3ae = a$.

The inverse of $a \in Q$ is $a' = -\frac{a}{3a+1}$. Indeed, the inverse a' of a has to satisfy $a \oplus a' = e$; i.e., $a + a' + 3aa' = 0$. Thus $a' = -\frac{a}{3a+1}$ which is always well-defined. □

5. Let $n \geq 3$. Show that $H = \{\pi \in S_n \mid \pi(1) = 1, \pi(2) = 2\}$ is a subgroup of S_n. Find the order of H.

   Proof. Let $\pi, \sigma \in H$. Then $\pi\sigma \in H$, since $(\pi\sigma)(i) = \pi(\sigma(i)) = \pi(i) = i$ for $i = 1, 2$. It is clear that the identity permutation id of S_n lies in H. Moreover, the inverse of π satisfies $\pi^{-1}\pi = \mathrm{id}$ and so $i = \mathrm{id}(i) = (\pi^{-1}\pi)(i) = \pi^{-1}(\pi(i)) = \pi^{-1}(i)$ for $i = 1, 2$. Thus $\pi^{-1} \in H$ and hence H is a subgroup of S_n. The group H consists of all permutations on the set $\{1, \ldots, n\}$ which fix 1 and 2. The other elements can be permuted in $(n-2)!$ ways. Henceforth, H has order $(n-2)!$. □

6. Give an example of a group G with elements x and y such that $(xy)^{-1} \neq x^{-1}y^{-1}$.

   Explanation. Note that in any group we have $(xy)^{-1} = y^{-1}x^{-1}$. Take $G = S_3$, x as a transposition, and y as a 3-cycle. This is sort of a minimal example. ♢

7. Find all elements of order 2 in the symmetric group S_5.

   Explanation. Each element of order 2 in S_5 can be written as either a transposition (x_1x_2) or a product of transpositions $(x_1x_2)(x_3x_4)$, where all x_i's are distinct. Now count ... ♢

8. Is the group $\mathbb{Z}_4 \times S_3$ isomorphic to the group S_4?

   Explanation. Both groups have the same number of elements; i.e., both have order 24, and both are non-cyclic and non-abelian. However, $\mathbb{Z}_4 \times S_3$ has elements of order 12 such as $(1, (123))$ and $(3, (132))$, while every element in S_4 has order at most 4. Hence, the groups cannot be isomorphic. ♢

9. Let H be a subgroup of $(\mathbb{Q}^*, \cdot, 1)$ such that $\mathbb{Z} \setminus \{0\}$ is contained in H. Show that $H = \mathbb{Q}^*$.

   Proof. Let $p, q \in \mathbb{Z} \setminus \{0\}$. Then $p, q \in H$ and so $p, q^{-1} \in H$ and consequently $pq^{-1} \in H$. But $pq^{-1} = \frac{p}{q}$ and so $\frac{p}{q} \in H$. This shows that each nonzero rational number lies in H and so $H = \mathbb{Q}^*$. □

10. Represent the unit group of $\mathbb{Z}_{10}$ as a permutation group.

    Explanation. We have $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ and the multiplication table is as follows:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

    Take the symmetric group $S_4 = \{1, 3, 7, 9\}$. The elements $u \in \mathbb{Z}_{10}^*$ are identified with the left multiplications $\ell_u : S_4 \to S_4 : x \mapsto ux$. Thus we have

$$\begin{aligned} 1 &\mapsto (1, 3, 7, 9) = (1)(3)(7)(9), \\ 3 &\mapsto (3, 9, 7, 1) = (1397), \\ 7 &\mapsto (7, 1, 9, 3) = (1793), \\ 9 &\mapsto (9, 7, 3, 1) = (19)(37). \end{aligned}$$

    ♢

11. Find the symmetry group of an isosceles triangle, a triangle, and a square.

    Explanation. An isosceles triangle has one axis of symmetry. If the vertices are denoted by 1, 2 and 3, then (without restriction) the symmetry axis (reflection) fixes 3 and exchanges 1 and 2. So the symmetry group is $S_2 = \{(1)(2), (12)\}$.

    A rectangle has two axes of symmetry (reflections) and the symmetry group is the Klein four-group $V_4 = S_2 \times S_2$.

    A square has four axes of symmetry (reflections) and its invariant under rotation. The symmetry group is the Dihedral group $D_4 = C_4 \wr S_2$ (semidirect product) of order $4 \cdot 2 = 8$ (with 4 rotations and 4 reflections). ♢

12. Does the empty set form a group?

    Explanation. Its not a group, since each group contains a unique identity element. However, its a semigroup, since univeral statements are true on empty domains. ♢

13. Show that if in a group G, we have $(ab)^2 = a^2b^2$ for all $a, b \in G$, the group is abelian.

Proof. We have $aabb = (ab)^2 = abab$ and so $a^{-1}aabbb^{-1} = a^{-1}ababb^{-1}$. Thus $eabe = ebae$ with unit element e and hence $ab = ba$. □

14. Suppose a group G satisfies $\forall a, b \in G[(ab)^i = a^ib^i]$ for three consecutive integers i. Show that G is abelian.

Proof. Let i, $i+1$, and $i+2$ be the three consecutive integers. From $a^{i+1}b^{i+1} = (ab)^{i+1} = (ab)(ab)^i = aba^ib^i$ we get $a^ib = ba^i$. The same argument with i replaced by $i+1$ gives $a^{i+1}b = ba^{i+1}$. Then $ab = aba^ia^{-i} = aa^iba^{-i} = a^{i+1}ba^{-i} = ba^{i+1}a^{-i} = ba$. □

15. Why are two permutations conjugate if and only if they have the same cycle structure?

Explanation. Let π and σ be conjugate permutations in S_n, i.e, $\sigma = \tau\pi\tau^{-1}$ for some permutation τ. If $\pi(i) = j$, then $\sigma\tau(i) = \tau\pi\tau^{-1}\tau(i) = \tau\pi(i) = \tau(j)$. Thus the cycle structure of σ is the same as the cycle structure of π replacing each entry i with $\tau(i)$.

Conversely, suppose π and σ have the same cycle structure. List the cycles of π above the cycles of σ aligning cycles of the same length with one another. Now interpret this as the two-line representation of a permutation τ. Then $\sigma = \tau\pi\tau^{-1}$.

For instance, if $\pi = (1,3,2,4)(5,6)$ and $\sigma = (5,2,3,1)(6,4)$, then write

$$\begin{array}{cccccc} 1 & 3 & 2 & 4 & 5 & 6 \\ 5 & 2 & 3 & 1 & 6 & 4 \end{array}$$

Take the associated permutation $\tau = (1,5,6,4)(2,3)$. Then $\sigma = \tau\pi\tau^{-1}$. ♢

16. Find the smallest subgroup of $(\mathbb{Q}, +, 0)$ containing $\frac{1}{2}$ and the smallest subgroup of $(\mathbb{Q}^*, \cdot, 1)$ containing $\frac{1}{2}$.

Explanation. For $(\mathbb{Q}, +, 0)$, the subgroup consists of the additive multiples of $\frac{1}{2}$:

$$\left\langle \frac{1}{2} \right\rangle = \left\{ \frac{a}{2} \mid a \in \mathbb{Z} \right\}.$$

For $(\mathbb{Q}^*, \cdot, 1)$, the subgroup consists of the multiplicative multiples of $\frac{1}{2}$:

$$\left\langle \frac{1}{2} \right\rangle = \{2^a \mid a \in \mathbb{Z}\}.$$

♢

17. What is $\sum_\pi \operatorname{sgn}(\pi)$ where π runs over all permutations of degree n?

Explanation. In case of $n = 1$, we have $S_1 = \{(1)\}$ with $\operatorname{sgn}(1) = 1$. Hence, the sum is 1.

In case of $n \geq 2$, the mapping $\operatorname{sgn} : S_n \to \{\pm 1\} : \pi \mapsto \operatorname{sgn}(\pi)$ is an epimorphism. But for a group homomorphism, each image is taken on the same number of times! Thus $|\operatorname{sgn}^{-1}(1)| = |\operatorname{sgn}^{-1}(-1)| = \frac{n!}{2}$ and hence $\sum_\pi \operatorname{sgn}(\pi) = \frac{n!}{2} \cdot 1 + \frac{n!}{2} \cdot (-1) = 0$.

18. The groups $(\mathbb{R}^*, \cdot)$ and $(\mathbb{R}, +)$ are not isomorphic.

Proof. An isomorphism transports the order of an element. The group $(\mathbb{R}^*, \cdot)$ has one element of order 2 namely -1, since $(-1)^2 = 1$. There is no such element in $(\mathbb{R}, +)$, since if $0 \neq x \in \mathbb{R}$, then $2x \neq 0$. □

19. Show that the identity permutation cannot be expressed as a product of an odd number of permutations.

Proof. Let $n \geq 2$. The sign mapping $\operatorname{sgn} : S_n \to \{\pm 1\}$ is a group epimorphism. The identity permutation $\tau = \mathrm{id}$ has $\operatorname{sgn}(\tau) = 1$, while a permutation π consisting of an odd number of permutations has $\operatorname{sgn}(\pi) = -1$. □

20. Let f be a permutation of S_n with $n \geq 3$. Show that if for each permutation $g \in S_n$ we have $fg = gf$, then $f = \mathrm{id}$.

Proof. Suppose f is not the identity. Then $f(a) = b$ for some $a \neq b$. Let c be a third element with $a \neq c \neq b$. Take a permutation g with $g(a) = a$ and $g(b) = c$. Then $g(f(a)) = g(b) = c$ and $f(g(a)) = f(a) = b$ proving that $fg \neq gf$. □

21. Show that for any real-valued interval (a, b) there is an algebraic operation $*$ such that (a, b) together with $*$ forms a group.

Proof. Any open interval is equinumerous to $\mathbb{R}$, i.e., there is a bijection $\phi : (a, b) \to \mathbb{R}$. The bijections

$$f : (-\pi/2, \pi/2) \to \mathbb{R} : x \mapsto \tan(x)$$

and

$$g : (a, b) \to (-\pi/2, \pi/2) : x \mapsto mx + t$$

with $m = -\frac{\pi}{a-b}$ and $t = \frac{1}{2}\frac{\pi(a+b)}{a-b}$ provide a bijection $\phi : (a, b) \to \mathbb{R}$ by composition $\phi = fg$.

The real numbers form a group under addition, i.e., $(\mathbb{R}, +, 0)$ is a group. Then define

$$s * t = \phi^{-1}(\phi(s) + \phi(t)), \quad s, t \in (a, b).$$

Claim that the interval (a, b) together with the operation $*$ forms an abelian group. Indeed, the operation is associative, since

$$\begin{aligned} r * (s * t) &= r * \phi^{-1}(\phi(s) + \phi(t)) \\ &= \phi^{-1}(\phi(r) + \phi(\phi^{-1}(\phi(s) + \phi(t)))) \\ &= \phi^{-1}(\phi(r) + (\phi(s) + \phi(t))) \\ &= \phi^{-1}((\phi(r) + \phi(s)) + \phi(t)) \quad \text{(associativity of } +) \\ &= \phi^{-1}(\phi(\phi^{-1}(\phi(r) + \phi(s))) + \phi(t)) \\ &= \phi^{-1}(\phi(r) + \phi(s)) * t \\ &= (r * s) * t. \end{aligned}$$

The operation is commutative, since

$$s * t = \phi^{-1}(\phi(s) + \phi(t)) = \phi^{-1}(\phi(t) + \phi(s)) = t * s.$$

The unit element is $e = \phi^{-1}(0)$, since

$$s * e = \phi^{-1}(\phi(s) + \phi(\phi^{-1}(0))) = \phi^{-1}(\phi(s) + 0) = \phi^{-1}(\phi(s)) = s.$$

The inverse of $s \in (a, b)$ is $t = \phi^{-1}(-\phi(s))$, since

$$s * t = \phi^{-1}(\phi(s) + \phi(\phi^{-1}(-\phi(s)))) = \phi^{-1}(\phi(s) - \phi(s)) = \phi^{-1}(0) = e.$$

□

22. Do the irrationals form a group?

Explanation. The number $\sqrt{2}$ is irrational. Indeed, suppose that $\sqrt{2}$ is rational. Then $\sqrt{2} = p/q$ for some positive integers p, q which have no common divisor. Thus $2q^2 = p^2$. By the unique factorization of integers as products of prime powers, the multiplicity of 2 in $2q^2$ is odd and the multiplicity of 2 in q^2 is even. A contradiction.

The set of irrational numbers is not closed under addition and multiplication, e.g., $\sqrt{2} \cdot \sqrt{2} = 2$ and $\sqrt{2} - \sqrt{2} = 0$.

Consider the abelian group $(\mathbb{R}, +, 0)$, take a bijection $\phi : (\mathbb{R} \setminus \mathbb{Q}) \to \mathbb{R}$, and define the operation

$$a * b = \phi^{-1}(\phi(a) + \phi(b)), \quad a, b \in \mathbb{R} \setminus \mathbb{Q}.$$

In this way, the irrationals form an abelian group under the operation $*$. The unit element is $e = \phi^{-1}(0)$ and the inverse of s is $\phi^{-1}(\phi(-s))$. ♢

23. Show that the additive groups $\mathbb{Z}_2 \times \mathbb{Z}_{10}$ and $\mathbb{Z}_4 \times \mathbb{Z}_5$ are not isomorphic.

Proof. Let G and H be groups. The direct product $G \times H = \{(g, h) \mid g \in G, h \in H\}$ forms a group with the component-wise operation $(g, h) * (g', h') = (gg', hh')$. If G and H are finite, the product group $G \times H$ has the order $|G| \cdot |H|$.

The group $\mathbb{Z}_2 \times \mathbb{Z}_{10}$ has two elements $(1, 0)$ and $(0, 5)$ of order 2, whereas the group $\mathbb{Z}_4 \times \mathbb{Z}_5$ has exactly one element $(2, 0)$ of order 2. Since an isomorphism transports the order, the groups cannot be isomorphic. □

Chapter 11

Elementary Number Theory

1. Find the number of common divisors of 463050 and 2425500.

   Explanation. The Euclidean algorithm gives $(463050, 2425500) = 22050$. The prime factorization of this number is $22050 = 2^1 3^2 5^2 7^2$. So the number of common divisors is $\tau(22050) = (1+1)(2+1)(2+1)(2+1) = 54$. ♢

2. Compute $(24, 54 + 24^7)$.

   Explanation. By the Euclidean algorithm, $24^7 + 54 = (24^6 + 2) \cdot 24 + 6$ and $24 = 4 \cdot 6 + 0$. Hence, $(24, 54 + 24^7) = 6$. ♢

3. Show that $3^{105} + 4^{105} \equiv 0 \mod 13$.

   Proof. We have $3^{105} = (3^3)^{35} = 27^{35} \equiv 1^{35} \equiv 1 \mod 13$ and $4^{105} = (4^3)^{35} = 64^{35} \equiv (-1)^{35} \equiv -1 \mod 13$. Adding both residues modulo 13 gives $1 + (-1) = 0$. □

4. Let a, b be integers. Show that if $(a, b) = 1$, then $(ab, a^2 + b^2) = 1$.

   Proof. Let $d = (ab, a^2 + b^2)$. Then d divides ab and $a^2 + b^2$. For a prime divisor p of d with p divides ab, we have that p divides a or p divides b. Suppose that p divides a. Then p divides a^2. But p divides $a^2 + b^2$ and so p divides b^2. Similarly, p divides b implies that p divides a^2. Hence, p divides $(a^2, b^2) = (a, b) = 1$. □

5. Prove that for any integer $n \geq 0$, $4(n^2 + 1)$ is not divisible by 11.

   Proof. Suppose the expression $4(n^2+1)$ would be divisible by 11. Then $n^2 + 1$ is divisible by 11, since 11 is a prime and so if 11 divides a product, it will divide a factor. Thus $n^2 + 1 \equiv 0 \mod 11$ or equivalently

$n^2 \equiv 10 \mod 11$ has a solution. One can check that this is not the case by working out $0^2, 1^2, \ldots, 10^2 \mod 11$.

Note that one only needs to check the squares $0^2, 1^2, \ldots, 5^2 \mod 11$, since $6^2, 7^2, \ldots, 10^2 \mod 11$ are the same as $5^2, 4^2, \ldots, 1^2 \mod 11$. To see this, note that for each modulus m there are at most $m/2 + 1$ different values for n^2 modulo m. This is because $n^2 \equiv (m-n)^2 \mod m$, and so the numbers modulo m (other than 0 and $m/2$) divide into pairs with the same square. □

6. Why is $[(p-2)!]^2 \equiv 1 \mod p$ for each prime p?

   Explanation. By Wilson's theorem, we have $(p-1)! \equiv -1 \mod p$. Squaring both sides gives $[(p-1)!]^2 \equiv 1 \mod p$. Thus $[(p-2)!]^2 \cdot (p-1)^2 \equiv 1 \mod p$. Since $p - 1 \equiv -1 \mod p$ and so $(p-1)^2 \equiv 1 \mod p$, we obtain $[(p-2)!]^2 \equiv 1 \mod p$. ♢

7. Show that if p is a positive integer such that both p and $p^2 + 2$ are prime, then $p = 3$.

   Proof. Any integer p is of the form $3k$, $3k+1$ or $3k+2$. But $(3k+1)^2 + 2 = 9k^2 + 6k + 3$ is divisible by 3 and so not prime. Moreover, $(3k+2)^2 + 2 = 9k^2 + 12k + 6$ is divisible by 3 and so not prime. Finally, $3k$ is prime only when $k = 1$. Hence, $p = 3$. □

8. Show that the Euler totient function satisfies $\phi(ab) \geq \phi(a)\phi(b)$ for any pair of positive integers a, b. And does equality hold if and only if $(a, b) = 1$?

   Proof. Write

$$a = \prod_i p_i^{a_i} \cdot \prod_j q_j^{\alpha_j} \quad \text{and} \quad b = \prod_i p_i^{b_i} \cdot \prod_k r_k^{\beta_k},$$

   where (p_i) is the list of primes dividing (a, b) and q_j, r_k are primes distinct from each other and different from the p_i. Then

$$\phi(ab) = \prod_i p_i^{a_i + b_i - 1}(p_i - 1) \cdot \phi\left(\prod_j q_j^{\alpha_j}\right) \cdot \phi\left(\prod_k r_k^{\beta_k}\right)$$

   and

$$\phi(a)\phi(b) = \prod_i p_i^{a_i + b_i - 2}(p_i - 1)^2 \cdot \phi\left(\prod_j q_j^{\alpha_j}\right) \cdot \phi\left(\prod_k r_k^{\beta_k}\right).$$

Thus

$$\frac{\phi(ab)}{\phi(a)\phi(b)} = \prod_i \frac{p_i}{p_i - 1}.$$

The desired inequality follows at once as well as the claim the equality holds if and only if $(a, b) = 1$.

As an example, consider $a = 12$ and $b = 16$. Since $(12, 16) = 4$, the only common prime is $p_1 = 2$. We have $\phi(12 \cdot 16) = \phi(192) = 64$ and $\phi(12)\phi(16) = 4 \cdot 8 = 32$. □

9. Prove that for an integer $n \geq 2$, n is prime if and only if the binomial coefficients $\binom{n}{1}, \ldots, \binom{n}{n-1}$ are divisible by n.

   Proof. Let p be prime and $1 \leq k \leq p - 1$. Then p divides $\binom{p}{k} = p(p-1)\cdots(p-k+1)/k!$, since $\binom{p}{k}$ is a natural number and p divides the numerator but not the denominator.

   Conversely, we look for a counter example. For this, let n be composite and p be the smallest prime factor of n. Put $k = n/p$. Then $1 \leq p \leq n-1$ and $\binom{n}{p} = n(n-1)\cdots(n-p+1)/p! = k(n-1)\cdots(n-p+1)/(p-1)!$ is not divisible by n. Otherwise, the numerator $k(n-1)\cdots(n-p+1)$ must be divisible by $n = kp$ and so $(n-1)\ldots(n-p+1)$ must be divisible by p. But n is divisible by p and so p does not divide any of the numbers $n-1, n-2, \ldots, n-p+1$. Since p is prime, it does not divide the product $(n-1)(n-2)\cdots(n-p+1)$.

   For instance, if $n = 12$, then $p = 2$ and $k = 6$. The binomial coefficient $\binom{12}{2} = 66$ is not divisible by 12. □

10. Show that for each integer a, $a^2 \equiv 0 \mod 4$ or $a^2 \equiv 1 \mod 4$.

    Proof. For each integer a, $a \equiv 0, 1, 2, 3 \mod 4$. Squaring gives $a \equiv 0, 1, 4, 9 \equiv 0, 1 \mod 4$. □

11. Solve the congruence $ax \equiv x \mod n$, where $a \in \mathbb{Z}$ and $n \geq 2$.

    Explanation. The congruence is equivalent to $ax - x = kn$ for some integer k. Thus $x = \frac{kn}{a-1}$ for $a \neq 1$. In case of $a = 1$, we have $x \equiv x \mod n$ which is true for all x. ♢

12. Given integers a, b, c, d with $d \not\equiv 0 \mod 5$ and m an integer with $am^3 + bm^2 + cm + d \equiv 0 \mod 5$. Show that there is an integer n for which $dn^3 + cn^2 + bn + a \equiv 0 \mod 5$.

Proof. Since $p = 5$ is a prime and d is nonzero modulo 5, the integer m cannot be zero modulo 5 and so has an inverse n with $mn \equiv 1 \mod 5$. Multiplying the congruence $am^3 + bm^2 + cm + d \equiv 0 \mod 5$ with n^3 gives the desired result. □

13. Show that for any two integers a and b, at least one of the expressions a^3, b^3, $a^3 + b^3$ or $a^3 - b^3$ is divisible by 7.

Proof. If a or b is a multiple of 7, then 7 divides a^3 or b^3. Otherwise, by Fermat's little theorem, $a^6 \equiv b^6 \equiv 1 \mod 7$. Thus

$$(a^3 + b^3)(a^3 - b^3) = a^6 - b^6 \equiv 0 \mod 7.$$

Since 7 is prime, it divides one of the factors $a^3 + b^3$ or $a^3 - b^3$. □

14. Show that 17 divides $15! - 1$.

Proof. Wilson's theorem states that $(n-1)! \equiv -1 \mod n$ for each prime number n. We have

$$\begin{aligned}
(17-1)! &\equiv -1 \mod 17,\\
16! &\equiv -1 \mod 17,\\
16 \cdot 15! &\equiv -1 \mod 17,\\
(-1) \cdot 15! &\equiv -1 \mod 17,\\
15! &\equiv 1 \mod 17,\\
15! - 1 &\equiv 0 \mod 17.
\end{aligned}$$

□

15. Calculate 8^{505} modulo 5.

Explanation. By Fermat's little theorem $a^{p-1} = 1$ for any $a \in \mathbb{Z}$ not divisible by p, where p is a prime. Equivalently, $a^{p-1} \equiv 1 \mod p$. Let n be a positive integer. Write $n = q \cdot (p-1) + r$, where $0 \leq r < p - 1$. Then $a^n = a^{q(p-1)+r} = (a^{(p-1)})^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \mod p$. We have $505 = 126 \cdot 4 + 1$ and so $8^{505} \equiv 8^1 \equiv 3 \mod 5$. ♢

16. Show that if p is prime, the only solutions of the congruence $x^2 \equiv x \mod p$ are the integers x with $x \equiv 0 \mod p$ or $x \equiv 1 \mod p$.

Proof. The congruence $x^2 \equiv x \mod p$ is equivalent to $p \mid x(x-1)$. Since p is prime, we have $p \mid x$ or $p \mid x - 1$. Thus $x \equiv 0 \mod p$ or $x \equiv 1 \mod p$. □

17. Find the last digit of $3^{29} + 11^{12} + 15$.

Explanation. Choose the modulus 10. Then $11^{12} \equiv 1^{12} \equiv 1 \mod 10$, $3^{29} = 3^{28} \cdot 3 = 81^7 \cdot 3 \equiv 3 \mod 10$, and $15 \equiv 5 \mod 10$. Adding modulo 10 gives the answer 9. ♢

18. Give a criterion for a natural number to be divisible by 7.

Explanation. Let $n = (a_k \dots a_1 a_0)_{10} = \sum_{j=0}^{k} a_j 10^j$. The expression

$$Q_3(n) = (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} \mp \dots$$

is called alternating sum of digits of third order of n. For instance, $Q_3(123456789) = 789 - 456 + 123 = 456$.

Claim that $7|n$ if and only if $7|Q_3(n)$. Indeed, we have $1001 = 143 \cdot 7$ and so $1000 \equiv -1 \mod 7$. Thus $1000^k \equiv (-1)^k \mod 7$ for each $k \geq 1$. Write $a'_0 = (a_2 a_1 a_0)_{10}$, $a'_1 = (a_5 a_4 a_3)_{10}$, and so on. Then $n = \sum_k a'_k 1000^k \equiv \sum_k (-1)^k a'_k \mod 7$. ♢

19. Do there exist integers x and y such the equation $735x + 847y = -28$ is satisfied?

Explanation. An equation of the form $ax + by = n$ with integers a, b, and n (a and b not both zero) has an integer solution if and only if (a, b) is a divisor of n. If so, there are infinitely many integer solutions; i.e., infinitely many pairs (x, y) fulfilling the equation.

We have $(735, 847) = 7$ and 7 divides -28. The extended Euclidean algorithm yields $735 \cdot (-53) + 847 \cdot 46 = 7$. Multiplying the equation by -4 gives $735 \cdot 212 + 847 \cdot (-184) = -28$.

In `Maple` use `igcdex(735,847,'x','y')`. ♢

20. Do we have $\phi(\phi(n)) < \log(n)$ for each natural number $n \geq 1$?

Explanation. No, we don't. We have $\phi(\phi(5)) = \phi(4) = 2 > 1.6094... = \log(5)$, but $\phi(\phi(10)) = \phi(4) = 2 < 2.4025... = \log(10)$. ♢

21. There is no rational number r with the property $r^2 = 3$.

Explanation. Write $r = \frac{a}{b}$ for integers a, b with $(a, b) = 1$. Then if $r^2 = 3$, then $a^2 = 3b^2$. Note that if a prime number divides a product, it will divide a factor. We have $3 \mid a^2$ and so $3 \mid a$, i.e., $a = 3s$ for some number s. Thus $a^2 = 3^2 s^2$ and so $b^2 = 3s^2$. Hence, $3 \mid b$ contradicting $(a, b) = 1$. ♢

22. Can a finite sum of square roots be an integer?

Explanation. It can happen just like $\sqrt{4}+\sqrt{9}=2+3=5$. Here the numbers are perfect squares; a *perfect square* is a natural number of the form a^2 for some integer a. Perfect squares are $0^2=0$, $1^2=1$, $2^2=4$, $3^2=9$ and so on.

There is an elementary way to see that if $\sqrt{a}+\sqrt{b}$ is an integer for some $a,b\in\mathbb{N}_0$, then a and b must be perfect squares. Indeed, suppose $\sqrt{a}+\sqrt{b}=c$ for some $c\in\mathbb{Z}$. If $a=0$, then b must be a perfect square; similarly for $b=0$. We may assume that $a,b\geq 1$. Squaring both sides gives $a+2\sqrt{ab}+b=c^2$ and therefore ab must be a perfect square. Assume that $ab=d^2$ for some $d\in\mathbb{Z}$. Then $a=\frac{d^2}{b}$ and so $\frac{d}{\sqrt{b}}+\sqrt{b}=c$. Multiplying both sides by $\sqrt{b}$ yields $d+b=c\sqrt{b}$. Thus $\sqrt{b}=\frac{b+d}{c}$ must be a perfect square and a must be as well. ♢

23. Show that $\sqrt[5]{17}$ is not a rational number.

Proof. Suppose $\sqrt[5]{17}$ is rational. Then $\sqrt[5]{17}=\frac{m}{n}$ for some natural numbers m,n. Thus $17n^5=m^5$ and so m is divisible by 17. Therefore, $m=17m_1$ for some natural number m_1. Thus $n^5=17^4m_1^5$ and so n is divisible by 17. Therefore, $n=17n_1$ for some natural number n_1. Thus $17n_1^5=m_1^5$, where $m>m_1$. Repeating this we get a descending sequence of natural numbers $m>m_1>m_2>\ldots$ which is impossible; the set of natural number is well-ordered. A contradiction. □

24. Is there a rational number between any two irrationals?

Explanation. Let a and b be distinct irrationals; we loose no generality to suppose $a<b$. Assume they have equal integers parts, since otherwise there is an integer between them and the question is trivial. They have infinite decimal expansions, $.a_1a_2a_3\ldots$ and $.b_1b_2b_3\ldots$. These cannot agree in every position since otherwise $a=b$. We may assume they agree up to the $n-1$th position and differ at the nth. Then $x=.b_1b_2b_3\ldots b_n000\ldots$ is a rational number strictly between a and b, since

$$a=.a_1a_2\ldots a_{n-1}a_n\ldots<.a_1a_2\ldots a_{n-1}b_n000\ldots=x$$

because $a_n<b_n$, and

$$x=.b_1b_2b_3\ldots b_n000\ldots<.b_1b_2b_3\ldots b_nb_{n+1}\ldots=b$$

because not all of b_{n+1},b_{n+2} can be zero.

For instance, there is a rational number between $\sqrt{2}=1.4141\ldots$ and $\sqrt{3}-\frac{1}{4}=1.482\ldots$; this method produces the rational number $1.48000\ldots=\frac{37}{25}$. ♢

25. For each integer $n \geq 2$, $\sqrt{n}$ is either an integer or an irrational number.

Proof. Take the prime factorization of $n \geq 2$ into prime powers $n = p_1^{n_1} \cdots p_k^{n_k}$, where $p_1, \ldots, p_k$ are distinct primes and $n_1, \ldots, n_k$ are positive integers. Then $\sqrt{n}$ has a rational square root if and only if the multiplicity of every prime factor of n is even. For instance, $2^4 3^6 11^2$ has a rational square root but $5^4 11^3$ does not. Moreover, if a natural number has a rational square root, that square root is always obtained by halving the multiplicity of each prime factor, and so the square root is also a natural number. The reader could make this argument more rigouros. □

26. Show that $x + r$ is irrational if x is irrational and r is rational.

Proof. Suppose $x + r$ is rational; that is, there are integers p, q with $x + r = \frac{p}{q}$. Then $x = \frac{p}{q} - r$. But $\frac{p}{q} - r$ is rational and so x is rational. A contradiction. □

27. Is $\sqrt{2} + \sqrt{3}$ rational or irrational?

Explanation. If $\sqrt{2} + \sqrt{3}$ is rational, then so is $\sqrt{3} - \sqrt{2}$, since $(\sqrt{2} + \sqrt{3})(\sqrt{3} - \sqrt{2}) = 1$. But then so is

$$\sqrt{2} = \frac{(\sqrt{2} + \sqrt{3}) - (\sqrt{3} - \sqrt{2})}{2}$$

and

$$\sqrt{3} = \frac{(\sqrt{2} + \sqrt{3}) + (\sqrt{3} - \sqrt{2})}{2}.$$

♢

28. Why are the Fibonacci numbers bad for the Euclidean algorithm and how to derive an upper bound on the number of steps needed in general?

Explanation. The computation of the greatest common divisor (gcd) of two successive Fibonacci numbers involves only Fibonacci numbers;

e.g.,

$$\begin{aligned} 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Claim that the smalleset positive integers $a > b$ for which the Euclidean algorithm requires n steps are f_{n+2} and f_{n+1}.

Proof. Let $n = 1$. Then the Euclidean algorithm ends after the first step. This means that a is divisible by b without remainder. The smallest positive integers for which this is true are $a = f_3 = 2$ and $b = f_2 = 1$.

Suppose the result holds for $n \geq 1$. Let $a > b$ be positive integers for which the Euclidean algorithm requires $n + 1$ steps to compute (a, b). The first step in the algorithm is $a = q_1 b + r_1$ with $r_1 < b$ and the second step is $b = q_2 r_1 + r_2$ with $r_2 < r_1$. Thus the algorithm requires n steps to compute (b, r_1). By induction, the smallest positive integers for which the Euclidean algorithm requires n steps are f_{n+2} and f_{n+1}. Therefore, $b \geq f_{n+2}$ and $r_1 \geq f_{n+1}$. Since $a = q_1 b + r_1$ and $q_1 \geq 1$, we obtain $a \geq b + r_1 \geq f_{n+2} + f_{n+1} = f_{n+3}$. This proves the result. □

Chapter 12

Polynomials

1. Show that if f and g are polynomials in $\mathbb{Z}[X]$, g is monic, and g divides f in $\mathbb{Q}[X]$, then g divides f in $\mathbb{Z}[X]$.

   Proof. Since g is monic, the leading coefficient of g is a unit and so the division algorithm in $\mathbb{Q}[X]$ is applicable. It yields the same result when applied over $\mathbb{Z}$. As an example, consider $f = 2X^3 - 4X^2 + 5X - 3$ and $g = X^2 + 2X + 1$. □

2. Let a and b be distinct integers and let $f \in \mathbb{Z}[X]$ be a monic polynomial. Show that $\frac{f(a)-f(b)}{a-b}$ is an integer.

   Proof. By division with remainder, we get $f(X) = p(X)(X-b) + f(b)$ for some polynomial $p \in \mathbb{Z}[X]$. If evaluated at $X = a$, we obtain $f(a) = p(a)(a-b) + f(b)$ which gives $\frac{f(a)-f(b)}{a-b} = p(a)$. This is an integer, since p has integer coefficients and a is an integer. □

3. Given a polynomial $f \in \mathbb{R}[X]$ of degree 9. Suppose for all $a \in \{1, 2, \ldots, 10\}$ we have $f(a) = a$. Find the value $f(100)$.

   Explanation. Define the polynomial $g(X) = f(X) - X$. Then g has still degree 10 and has zeros $1, 2, \ldots, 10$. Thus $g(X) = (X-1)(X-2)\cdots(X-10)$ and so $g(100) = (100-1)(100-2)\cdots(100-10) = 56534085859976524800$. Hence, $f(100) = g(100) - 10$. ♢

4. Given $f(X) = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$. Show that if ad is odd and bc is even, then not all roots are rational.

   Proof. Suppose the roots are rational numbers in lowest terms $\frac{p_i}{q_i}$, $1 \leq i \leq 3$. Then $f(X) = n(q_1X - p_1)(q_2X - p_2)(q_3X - p_3)$ for some integer n. Thus $f(x) = nq_1q_2q_3X^3 - n(q_1q_2p_3 + q_1p_2q_3 + p_1q_2q_3)X^2 + n(q_1p_2p_3 + p_1q_2p_3 + p_1p_2q_3)X - np_1p_2p_3$. Since ad is odd, all involved

numbers n, q_i, p_i, $1 \leq i \leq 3$, are odd. Moreover, b and c are both sums of three odd numbers and therefore are odd, too. Hence, bc is also odd. $\square$

5. Let $a, b, c \in \mathbb{R}$. Show that the solutions of the equation $(X-a)(X-b) = c^2$ are real numbers.

   Proof. The equation gives $X^2 - (a+b)X + (ab - c^2) = 0$. Then the discriminant is $D = (-(a+b))^2 - 4(ab-c^2) = (a-b)^2 + 4k^2 \geq 0$. $\square$

6. For what integer values of a does the polynomial $f = X^2 + aX + 6$ have two integer roots?

   Explanation. Let p and q be the integral roots. Then $f = (X-p)(X-q) = X^2 + (p+q)X + pq$. Thus $pq = 6$ and so (p, q) is one of the pairs $(1,6)$, $(6,1)$, $(-1,-6)$, $(-6,-1)$, $(2,3)$, $(3,2)$, $(-2,-3)$, $(-3,-2)$. Hence, $a = p + q \in \{\pm 7, \pm 5\}$. $\diamondsuit$

7. When the polynomial $f \in \mathbb{R}[X]$ is divided by $(X^2 + 3X + 2)$, the remainder is $(5X + 1)$. Find the remainder when f is divided by $X + 2)$.

   Explanation. Write $f(X) = q(X)(X^2 + 3X + 2) + 5X + 1$, where $q \in \mathbb{R}[X]$. But $X^2 + 3X + 2 = (X+1)(X+2)$ and so $f(X) = q(X)(X+1)(X+2) + 5X + 1$. Putting $X = -2$ gives $f(-2) = -9$. So the remainder when f is divied by $X + 2$ is -9. $\diamondsuit$

8. Find the roots of the polynomial $X^4 - 5X^2 + 6$ over $\mathbb{Q}$.

   Explanation. We have

   $$X^4 - 5X^2 + 6 = Y^2 - 5Y + 6 = (Y-3)(Y-2) = (X^2-3)(X^2-2).$$

   Thus the roots are $\pm\sqrt{3}$ and $\pm\sqrt{2}$. $\diamondsuit$

9. Let $f \in \mathbb{R}[X]$ with real-valued roots and the property that $f(a) = 0$ implies $f(a+1) = 1$. Prove that f has a repeated root.

   Proof. Suppose that f has distinct roots $\alpha_1, \ldots, \alpha_n$ such that $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ and $n \geq 2$. Then $f(X) - 1 = (X - \alpha_1 - 1) \cdots (X - \alpha_n - 1)$. In particular, the coefficient of X^{n-1} of f is $-\sum_i \alpha_i = -\sum_i (\alpha_i - 1)$ which is impossible. $\square$

10. Show that the exponential function e^x cannot be expressed as a quotient of two real-valued polynomials.

Proof. Suppose $e^x = \frac{p(x)}{q(x)}$ for two polynomials p and q. The limits

$$\lim_{x\to+\infty} \frac{p(x)}{q(x)} \quad \text{and} \quad \lim_{x\to-\infty} \frac{p(x)}{q(x)}$$

are identical in $\mathbb{R} \cup \{\pm\infty\}$. But

$$\lim_{x\to+\infty} e^x = +\infty \quad \text{and} \quad \lim_{x\to-\infty} e^x = 0.$$

□

11. Prove that $f = X^3 + X^2 + 1$ is irreducible over $\mathbb{Z}_2$?

Proof. Assume that it is reducible. Since it has degree 3, one of the factors would have to be linear, say $X - \alpha$. Therefore, α would be a root of this polynomial, since by division with remainder, $X - \alpha$ divides f iff $f(\alpha) = 0$. Check by plugging in directly, whether $\alpha \in \mathbb{Z}_2$ is a root. But $f(0) = 1$ and $f(1) = 1 + 1 + 1 = 1$ in $\mathbb{Z}_2$, and so the polynomial is irreducible. □

12. Find a monic quadratic polynomial $f \in \mathbb{Q}[x]$ such that if f is divided by $(X - 1)$, the remainder is 12 and if f is divided by $(X - 4)$, the remainder is 3.

Explanation. We have $f(X) = p(X)(X - 1) + 12$ and $f(X) = q(X)(X - 4) + 3$ for some polynomials p, q. Then $f(1) = 12$ and $f(4) = 3$. Since the polynomials in $\mathbb{Q}[X]$ have a unique factorization, $f(X) = a(X - 1)(X - 4)$ for some $a \in \mathbb{Q}$. But f is monic and hence $a = 1$. ♢

13. Given distinct integers a, b, and c and a polynomial $p \in \mathbb{Z}[X]$. Show that $p(a) = b$, $p(b) = c$, and $p(c) = a$ cannot hold simultaneously.

Proof. We have $a - b \mid p(a) - p(b)$. To prove this, write $p(X) = a_n X^n + \ldots + a_1 X + a_0$. Then $p(a) - p(b) = a_n(a^n - b^n) + \ldots + a_1(a - b)$. But

$$a^k - b^k = (a - b) \sum_{j=0}^{k-1} a^j b^{k-j-1}, \quad k \geq 1,$$

and so each summand of $p(a) - p(b)$ is divisible by $a - b$. This gives $a - b \mid p(a) - p(b) = b - c$, $b - c \mid p(b) - p(c) = c - a$, and $c - a = p(c) - p(a) = a - b$, i.e., we obtain the divisibility cycle $a - b \mid b - c \mid c - a \mid a - b$. In a divisibility cycle $k \mid m \mid n \mid k$, we have $m, n = \pm k$. But in the above case $k + m + n = 0$ and so $a = b$ contradicting the hypothesis. □

Chapter 13

Rings

1. What are empty sum and empty product in a ring R?

   Explanation. Consider the sum $\sum_{i=0}^{n} r_i$ of ring elements $r_i \in R$. The empty sum ($n < 0$) has as value the zero element of the ring. Likewise, the empty product has as value the unit element of the ring. ♢

2. Show that the residue class ring $R = \mathbb{Z}_3[X]/\langle X^2 + X + 1\rangle$ is not a field.

   Proof. R will be a field if the polynomial $f = X^2 + X + 1$ is irreducible over $\mathbb{Z}_3$. But $f = (X - 1)^2$ is not irreducible. □

3. In a ring R with unity 1, if there is an element $r \in R$ with $r \neq \pm 1$ and $r^2 = 1$, then $r - 1$ and $r + 1$ are zero divisors.

   Proof. If $r \neq \pm 1$ and $r^2 = 1$, then $(r - 1)(r + 1) = r^2 - 1 = 0$. Since $r - 1$ and $r + 1$ are different from 0, it follows that $r - 1$ and $r + 1$ are zero divisors.

   For instance, in the ring $\mathbb{Z}_8$, the element $r = 3$ satisfies $r^2 = 1$, and the elements 2 and 4 are zero divisors. □

4. What are the zero divisors of the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$?

   Explanation. The ring $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, which is a field and so has no zero divisors. In view of computations, let $0 \neq a + bi \in \mathbb{Z}[i]$. We want to solve $(a + bi)(x + yi) = 0$. Since $(a + bi)(x + yi) = (ax - by) + (bx + ay)i$, this is equivalent to $ax - by = 0$ and $bx + ay = 0$. The determinant of this matrix is

   $$\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 \neq 0.$$

   Thus the system has the only solution $x = y = 0$. ♢

5. Let R be a ring with $a \in R$. Show that if a^n is invertible for some $n \geq 1$, then a is invertible.

   Proof. Let a^n be invertible. Then there is $b \in R$ with $a^n b = 1 = ba^n$. Thus $a(a^{n-1}b) = 1$ and $(ba^{n-1})a = 1$. That is, a has right inverse $a^{n-1}b$ and left inverse ba^{n-1}. But if a ring element $b \in R$ has a left inverse $c \in R$ and a right inverse $d \in R$, then $c = c1 = c(bd) = (cb)d = 1d = d$. Thus one can infer that $a^{n-1}b = ba^{n-1}$. Hence, a is invertible. □

6. Every nonzero element in a finite commutative ring R is either a unit or a zero divisor.

   Proof. Let $a \in R$ be nonzero. Consider the left multiplication $R \to R : x \mapsto ax$. If this mapping is injective, then it is surjective, since R is finite. In this case, $1 = ax$ for some $x \in R$ and so a is a unit in R.

   If this mapping is not in injective, then there are $u, v \in R$ with $u \neq v$ such that $au = av$. But then $a(u - v) = 0$ and $u - v \neq 0$, and so a is a zero divisor. □

7. Is the quotient ring $\mathbb{Z}_7[X]/\langle 3X^3 + 4X^2 + 6X + 4\rangle$ an integral domain?

   Explanation. The quotient ring is an integral domain if the polynomial is irreducible. However, the polynomial $3X^3 + 4X^2 + 6X + 4 = 3X^3 - 3X^2 - X - 3$ has 2 as a root and so factors as follows, $3X^3 - 3X^2 - X - 3 = (X - 2)(3X^2 + 3X - 2)$. ♢

Chapter 14

Fields

1. Let p be a prime and n be a positive integer. Prove that $n!$ divides $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

   Proof. The quantity $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ is the number of regular $n \times n$ matrices over $\mathbb{Z}_p$. This is the number of ways of chosing n linearly independent vectors from $\mathbb{Z}_p^n$. The regular $n \times n$ matrices over $\mathbb{Z}_p$ form a group under multiplication called general linear group, written $\mathrm{GL}(n, p)$.

   The quantity $n!$ is the number of $n \times n$ permutation matrices over any field. The $n \times n$ permutation matrices over $\mathbb{Z}_p$ correspond one-to-one to the permutations of degree n and form a group under multiplication, which is isomorphic to the symmetric group S_n. This group is a subgroup of $\mathrm{GL}(n, p)$.

   By Lagrange's theorem, the group order of each finite group is divisible by the group order of any of its subgroups. □

2. Find the zeros of the polynomial $X^3 - 7$ over $\mathbb{Q}$.

   Explanation. The zeros of the polynomial $X^3 - 1$ are the third roots of unity: 1, $\frac{-1+i\sqrt{3}}{2}$, and $\frac{-1-i\sqrt{3}}{2}$. It follows that the zeros of the polynomial $X^3 - 7$ are $\sqrt[3]{7}$, $\sqrt[3]{7}\frac{-1+i\sqrt{3}}{2}$, and $\sqrt[3]{7}\frac{-1-i\sqrt{3}}{2}$. ♢

3. In a field we have an additive inverse for the multiplicative identity. Why is there no multiplicative inverse for the additive identity?

   Explanation. For the multiplicative identity 1 in a field, we have $1 + (-1) = 0$. The additive identity 0 in a field is absorbing; that is, $0r = (r + (-r))r = r^2 - r^2 = 0$ for each element r. Thus there cannot be an element r such that $0r = 1$. ♢

4. Show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

Proof. Suppose $\sqrt{3}$ would belong to $\mathbb{Q}(\sqrt{2})$. Then $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}^*$; the cases $a = 0$ or $b = 0$ can be similarly handled. Squaring both sides gives $3 = a^2 + 2ab\sqrt{2} + 2b^2$. Rearranging gives $\sqrt{2} = \frac{3-a^2-2b^2}{2ab}$ contradicting the fact that $\sqrt{2}$ is irrational. □

5. Can the field $\mathbb{F}_2[X]/\langle p(X)\rangle$ be constructed using p irreducible but not primitive?

   Explanation. For instance, the field $\mathrm{GF}(2^4)$ can be constructed by three irreducible polynomials over $\mathbb{F}_2$: $p_1 = X^4 + X + 1$, $p_2 = X^4+X^3+1$, and $p_3 = X^4+X^3+X^2+X+1$. The first two are primitive, but the latter is not. One needs only an irreducible polynomial to construct a Galois field. Selecting a primitive polynomial forces (the congruence class of) X to be a generator of the multiplicative group; this is the definition of "primitive". ♢

6. Let $f = aX^2 + bX + c$ with $a \neq 0$ in $\mathbb{R}[X]$. Write $D = b^2 - 4ac$. Prove that $\mathbb{R}[X]/\langle f\rangle$ is isomorphic to $\mathbb{C}$ if $D < 0$, and $\mathbb{R}[X]/\langle f\rangle$ is isomorphic to $\mathbb{R} \times \mathbb{R}$ if $D > 0$.

   Proof. If $D > 0$, then f has two real-valued roots α, β. If $D < 0$, then f has two complex-valued roots α, β, which are complex conjugates. In both cases, we can write $f = a(X - \alpha)(X - \beta)$.

   For simplicity, consider the polynomials $f = X^2 + 1$ and $g = X^2 - 1$ with roots $\pm i$ and ± 1, respectively. The mappings $\mathbb{R}[X] \to \mathbb{C} : p \mapsto p(i)$ and $\mathbb{R}[X] \to \mathbb{R} \times \mathbb{R} : p \mapsto (p(1), p(-1))$ are surjective homomorphisms with kernels $\langle f\rangle$ and $\langle g\rangle$, respectively.

   The homomorphism theorem tells that for each surjective homomorphism $\phi : R \to S$, the mapping $\psi : R/\ker(\phi) \to S$ with $r + \ker(\phi) \mapsto \phi(r)$ is an isomorphism. □

7. Are the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ isomorphic?

   Explanation. Note that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are both two-dimensional vector spaces over $\mathbb{Q}$ and hence are isomorphic as vector spaces. But they are not isomorphic as fields. To see this, we can find a property which holds inside one and not the other.

   In the field $\mathbb{Q}(\sqrt{2})$ there is an element which satisfies the field property $x^2 = 2$. However, there is no element in $\mathbb{Q}(\sqrt{3})$ which fulfills this. Suppose there is an isomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Then we have $\phi(x^2) = \phi(2)$. But $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2$ and so the element $y = \phi(x^2)$ of $\mathbb{Q}(\sqrt{3})$ satisfies $y^2 = 2$. Such an element does not exist. ♢

8. Mapping the additive group of a finite field of order 2^n to its multiplicative group.

   Explanation. In a finite field $\mathbb{F}$ of order 2^n, we know that its additive group is isomorphic to $\mathbb{Z}_2^n$ and $\mathbb{Z}_2^n$ can be thought of as the set of all n-digit binary strings with the operation of XOR. Thus we can label each element of the additive group of $\mathbb{F}$ as an n-digit binary string, or in other words as an integer $0, 1, \ldots, 2^n - 1$.

   We also know that the multiplicative group $\mathbb{F}^*$ of $\mathbb{F}$ is a cyclic group of order $2^n - 1$ (excluding the zero element). Thus we can label each element of $\mathbb{F}^*$ as an integer $0, 1, \ldots, 2^n - 2$.

   Consider the Galois field $\mathbb{F}_8$ given as the quotient $\mathbb{Z}_2[X]/\langle X^3 + X + 1\rangle$ by using the (primitive) irreducible polynomial $X^3 + X + 1 \in \mathbb{Z}_2[X]$. Let α be a zero of this polynomial, then $\mathbb{F}_8$ consists of the elements (residue classes) $0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1$. On the other hand, we have $\alpha^0 = 1$, $\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$, $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$, and $\alpha^7 = 1$. This gives a bijection between the multiplicative group $\mathbb{F}_8^*$ and the nonzero elements of the additive group of $\mathbb{F}_8$, called *Zech logarithm.* $\diamondsuit$

Chapter 15

Complex Numbers

1. What is $\sqrt{i}$?

   Explanation. Write $\sqrt{i} = a + ib$ for some $a, b \in \mathbb{R}$. Then $i = (a + ib)^2 = (a^2 - b^2) + 2abi$. Thus $a^2 - b^2 = 0$ and $2ab = 1$. By inserting $a = \frac{1}{2b}$ into $a^2 - b^2 = 0$, we get $a = b = \pm\frac{1}{\sqrt{2}}$. ♢

2. Find all solutions of $z^2 + \bar{z}^2 = 0$.

   Explanation. Write $z = a + ib$ for some $a, b \in \mathbb{R}$. Then the above equation becomes $0 = (a + ib)^2 + (a - ib)^2 = 2a^2 - 2b^2$. Hence, we obtain $b = \pm a$. ♢

3. For every complex number z we have $e^z \neq 0$.

   Proof. Write $z = x + iy$ for some $x, y \in \mathbb{R}$. Then $e^z = e^{x+iy} = e^x(\cos y + i \sin y)$. Thus $0 = e^z = e^x(\cos y + i \sin y)$ implies $\cos y = -i \sin y$, which cannot hold. □

4. How to write 2^i in polar form?

   Explanation. We have $2^i = e^{i \ln 2} = \cos(\ln 2) + i \sin(\ln 2)$. ♢

5. Solve $iz + (1 + i)\bar{z} + 4i = 0$ over the complex numbers.

   Explanation. The conjugate of a complex number $z = a + bi$ with $a, b \in \mathbb{R}$ is $\bar{z} = a - bi$. This gives $0 = i(a + bi) + (1 + i)(a - bi) + 4i = a + (2a - b + 4)i$. Equivalently, $a = 0$ and $2a - b + 4 = 0$; that is, $a = 0$ and $b = 4$. ♢

6. Find $z \in \mathbb{C}$ such that $|z| = 2i(\bar{z} + 1)$.

   Explanation. Let $z = a + bi$, where $a, b \in \mathbb{R}$. Then the above equation becomes $\sqrt{a^2 + b^2} = 2i(a - bi + 1) = 2b + 2(a + 1)i$. This

gives $2(a+1) = 0$ and $\sqrt{a^2+b^2} = 2b$. Thus $a = -1$ and $\sqrt{b^2-1} = 2b$. Hence, since $b > 0$, the solution is $z = -1 + \frac{1}{\sqrt{3}}i$. ♢

7. Why is the mapping $\phi : \mathbb{C} \to \mathbb{R}$ with $\phi(z) = |z|$ not an additive homomorphism?

   Explanation. An additive homomorphism between two groups satisfies $\phi(a+b) = \phi(a) + \phi(b)$. Thus for two complex numbers z and w, we must have $|z+w| = |z| + |w|$. This is not the case. To see this, let $z = a + bi$ and $w = c + di$. Then $|z+w| = |(a+c) + (b+d)i| = \sqrt{(a+c)^2 + (b+d)^2}$ and $|z| + |w| = \sqrt{a^2+b^2} + \sqrt{c^2+d^2}$. For instance, if $z = i$ and $w = 1$, then $|i+1| = \sqrt{1^2+1^2} = \sqrt{2}$ and $|i| + |1| = 1 + 1 = 2$. ♢

8. If $1/(a+b) = 1/a + 1/b$, what is the solution for $z = a/b$?

   Explanation. We have

$$\begin{aligned} \frac{1}{a+b} &= \frac{1}{a} + \frac{1}{b}, \\ 1 &= \frac{a+b}{a} + \frac{a+b}{b}, \\ 1 &= 2 + \frac{b}{a} + \frac{a}{b}, \\ 0 &= 1 + \frac{1}{z} + z, \\ 0 &= z^2 + z + 1, \\ 0 &= \left(z + \frac{1}{2}\right)^2 + \frac{3}{4}. \end{aligned}$$

   Hence, $z = -\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$. ♢

9. Square the Euler formula $e^{\pi i} = -1$.

   Explanation. By squarring, we obtain $e^{2\pi i} = 1 = e^0$ but cannot infer that $2\pi i = 0$. Indeed, in the complex setting, $e^{z_1} = e^{z_2}$ does not imply $z_1 = z_2$, since the complex-valued function $z \mapsto e^z$ is not injective. We have $e^{z+2k\pi i} = e^z$ for each $k \in \mathbb{Z}$. ♢

10. Calculate $i^{9999999999}$.

    Explanation. We have $i^2 = -1$, $i^3 = -i$, and $i^4 = 1$. Thus by integral division we obtain $9999999999 = 4 \cdot 2499999999 + 3$ and so

$$\begin{aligned} i^{9999999999} &= i^{4\cdot 2499999999+3} = (i^4)^{2499999999} \cdot i^3 \\ &= 1^{2499999999} \cdot (-i) = -i. \end{aligned}$$

    ♢

11. Find the square root of $3 + i\sqrt{3}$.

Explanation. Write $\sqrt{3 + i\sqrt{3}} = \pm(a+ib)$. Then $3+i\sqrt{3} = (a+ib)^2 = (a^2-b^2)+2abi$. Thus $a^2 - b^2 = 3$ and $2ab = \sqrt{3}$. Now find a and b. ♢

12. Solve the complex equation $z^4 = -4$.

Explanation. We have $z^4 + 4 = (z^2 + 2i)(z^2 - 2i)$. Note that $i = e^{i\pi/2} = \left(e^{i\pi/4}\right)^2$. Thus $z^2 - 2i = (z + \sqrt{2}e^{i\pi/4})(z - \sqrt{2}e^{i\pi/4})$ and $z^2 + 2i = (z + \sqrt{2}ie^{i\pi/4})(z - \sqrt{2}ie^{i\pi/4})$. This gives the four roots. ♢

13. Find the algebraic solutions of the complex equation $z^4 = -16i$.

Explanation. Consider the principle root $z_0 = \sqrt[4]{16i} = (16i)^{1/4}$. Using $i = e^{-i\pi/2}$, we obtain $x_0 = 2\left(e^{-i\pi/2}\right)^{1/4} = 2e^{-i\pi/8}$. The other solutions are given by multiplying with the 4-th roots of unity: $2e^{-i\pi/8}$, $2ie^{-i\pi/8}$, $-2e^{-i\pi/8}$, and $-2ie^{-i\pi/8}$. ♢

14. Find the complex number obtained by rotating the complex number $3 + i$ by the angle of $\frac{\pi}{4}$.

Explanation. Rotating by $\frac{\pi}{4}$ is the same thing as multiplying the complex number $z = 3 + i$ by $z' = \cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4}) = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$. So the answer is $zz' = \sqrt{2} + 2\sqrt{2}i$. ♢

15. Find the square root of a complex number.

Explanation. Let $z = a + bi \in \mathbb{C}$. Find $\sqrt{z} = c + di$. We have $z = (c + di)^2 = (c^2 - d^2) + 2cdi$. Equating both representations gives $a = c^2 - d^2$ and $b = 2cd$. Then $c = b/2d$ and so $a = b^2/4d^2 - d^2$. Thus $d^4 + ad^2 - b^2/4 = 0$. By the `Maple` routine `solve` we obtain four solutions for d: $\pm\frac{1}{2}\sqrt{-2a \pm 2\sqrt{a^2+b^2}}$. ♢

16. Summing the n n-th roots of any complex number gives 0.

Proof. Let $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ be a polynomial over some field and let its roots (perhaps with repetitions) in some extension field be $\alpha_1, \ldots, \alpha_n$. Then $f = (X - \alpha_1)\cdots(X - \alpha_n)$ and comparing coefficients gives $\alpha_1 + \ldots + \alpha_n = a_{n-1}/(-1)^{n-1}$.

The n n-th roots of a complex number w are the roots of $z^n - w$. It follows that the sum of these roots must be 0. Note that the roots are $|\sqrt[n]{w}|e^{2\pi ik/n}$ for $0 \le k \le n-1$. □

17. The complex numbers can be ordered. But they cannot be made into an ordered field with the usual addition and multiplication.

    Explanation. A total (lexicographic) ordering $\preceq$ on $\mathbb{C}$ can be defined as $(a+bi) \preceq (c+di)$ if $a < c$ or $a = c$ and $b \leq d$.

    Another total ordering can be defined by noting that $\mathbb{C}$ and $\mathbb{R}$ have the same cardinality and therefore there is a bijection $f : \mathbb{C} \to \mathbb{R}$. Then define $z_1 \leq_f z_2$ in $\mathbb{C}$ if $f(z_1) \leq f(z_2)$ in $\mathbb{R}$.

    But all these orderings are incompatible with the field operations. That is, $\mathbb{C}$ cannot be made into an *ordered field* in which $a < b$ implies $a + c < b + c$ for all c, and $a < b$ and $c > 0$ imply $ac < bc$ for all c. Indeed, if there is such an ordering $\prec$ on $\mathbb{C}$, then either $i \prec 0$ or $0 \prec i$. First, suppose that $0 \prec i$. Then $0i \prec i^2$ and so $0 \prec -1$. Since $0 \prec -1$, we have $0 \prec (-1)^2 = 1$. Moreover, $0 \prec -1$ implies $0 + 1 \prec -1 + 1 = 0$ and hence $1 \prec 0 \prec 1$. A contradiction. The case that $i \prec 0$ is similar noting that $i \prec 0$ implies $0 \prec -i$. ♢

18. What is the value of 1^i?

    Explanation. In general, if $z, \alpha \in \mathbb{C}$, define $z^\alpha = \exp(\alpha \log z)$, where exp is defined in some independent manner such as by a power series. Thus $1^i = \exp(i \log 1)$. The complex logarithm is defined as $\log z = \log|z| + i \arg(z)$, where $\log|z|$ and $\arg(z)$ are real numbers. Thus $\log 1 = \log 1 + i \arg(1)$. For the argument, we have the principle value $\arg(1) = 0$, but there are infinitely many values $\arg(1) = 0 + 2k\pi$ with $k \in \mathbb{Z}$. In view of the principle value or principle branch of the logarithm, we obtain $1^i = e^0 = 1$. Other valid solutions are $1^i = \exp(i \cdot 2k\pi i) = e^{-2k\pi}$ for $k \in \mathbb{Z}$.

    Complex exponentiation is not the same function as real exponentiation. They only agree for appropriate branches of the logarithm. Complex exponentiation is only ever well-defined relative to the choice of the branch of the logarithm. ♢

19. Show that i^i is a real number.

    Proof. In general, if $z, \alpha \in \mathbb{C}$, define $z^\alpha = \exp(\alpha \log z)$, where exp is defined in some independent manner such as by a power series. The complex logarithm is defined as $\log z = \log|z| + i \arg(z)$, where $\log|z|$ and $\arg(z)$ are real numbers. Here $z = i$ and so $\log i = i \arg(i)$. Thus $i^i = \exp(i \cdot i \arg(i)) = \exp(-\arg(i))$ and hence no matter what we choose for the range of argument, we always have $i^i \in \mathbb{R}$. Fun stuff eh? □