17. *Binomial theorem.* The binomial coefficient $\binom{n}{k}$ is the number of subsets of k elements in a set of n elements. We can interpret it as how many ways we can select k elements from n elements so that every element can be selected at most once and the order of the selection is irrelevant. Prove:

(a) $\binom{n}{k} = \dfrac{n!}{k!(n-k)!} = \dfrac{n(n-1)\dots(n-k+1)}{k!}$;

(b) $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n} = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$.

18. Prove: (a) $\binom{n}{k} = \binom{n}{n-k}$; (b) $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$;

(c) $\binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{n}{k} = \binom{n+1}{k+1}$; (d) $\sum_{k=0}^{n}\binom{n}{k} = 2^n$.

19. Give an explicit formula for the sums: (a) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots$;

(b) $\binom{n}{0} - 2\binom{n}{1} + 4\binom{n}{2} - 8\binom{n}{3} + \ldots$; *(c) $\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \ldots$.

20. Let S be a set of n elements.
(a) How many (binary) operations can be defined on S?
(b) How many of them are commutative?
(c) How many of them have an identity?

21. Prove the following propositions:
(a) An operation can have at most one identity.
(b) If an associative operation has an identity, then every element can have at most one inverse.
(c) If an associative operation on S has an identity and every element has an inverse, then the equations $ax = b$ and $ya = b$ have unique solutions x and y in S for every $a, b \in S$.
(d) If an operation on S is associative and the equations $ax = b$ and $ya = b$ have solutions x and y in S for every $a, b \in S$, then there is an identity and every element has an inverse.

Remark: From (c) and (d) we infer that subtraction can be performed iff there is a zero element and every element has a negative, and division can be performed iff there is an identity (for multiplication) and every element has a reciprocal.

22. Let X be any (finite or infinite) set and S the set of all $X \to X$ functions with the composition as an operation. Show that this operation is associative and has an identity. Which functions have a left inverse and which have a right inverse?

23. Consider an associative operation with identity. True or false:
(a) If each of two elements has an inverse, then also their product has an inverse.
(b) If the product of two elements has an inverse, then also each of the factors has an inverse.

24. Which of the following sets are rings under the given addition and multiplication? Are the rings commutative, do they have an identity, which elements have a left or right inverse, and which are left or right zero divisors? Which rings are fields?
(a) The set $\mathbf{Z}_n$ of the remainders under division by n under the natural addition and multiplication. (E.g. if $n = 8$, then $3 + 7 = 2$ and $3 \cdot 7 = 5$.)
(b) The even remainders under division by (b1) 10; (b2) 12; (b3) 15 under the natural addition and multiplication.
(c) The following sets of 2×2 real matrices under the usual matrix addition and multiplication:

(c1) diagonal matrices $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$;

(c2) upper-triangular matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$;

(c3) symmetric matrices $\begin{pmatrix} a & b \\ b & d \end{pmatrix}$, i.e. $A^T = A$;

(c4) skew-symmetric matrices $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$, i.e. $A^T = -A$;

(c5) $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$; (c6) $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$; (c7) $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$; (c8) $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$; (c9) $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

(d) The real numbers under addition $\oplus$ and multiplication $\odot$ defined below:
(d1) $\oplus$ is the usual addition and $a \odot b = 2ab$;
(d2) $a \oplus b = 2(a+b)$ and $\odot$ is the usual multiplication;
(d3) $a \oplus b = a+b+2$ and $\odot$ is the usual multiplication;
(d4) $a \oplus b = \sqrt[3]{a^3+b^3}$ and $\odot$ is the usual multiplication;
(d5) $a \oplus b = a+b+2$ and $a \odot b = ab+2a+2b+2$.

(e) The set of all subsets of a set X where addition is the symmetric difference and multiplication is the intersection, i.e. $A+B = A \triangle B = (A \cup B) \setminus (A \cap B)$ and $AB = A \cap B$.

(f) The following sets of polynomials f with real coefficients under the usual polynomial addition and multiplication:
(f1) $\deg f$ is even or $f = 0$;
(f2) every term in f has an even degree;
(f3) $\deg f \le 10$ or $f = 0$;
(f4) $\deg f \ge 10$ or $f = 0$;
(f5) 2021 is a root of f;
(f6) the sum of coefficients of f is 0;
(f7) the constant term of f is an integer.

(g) The following sets of real numbers where $a, b, c \in \mathbf{Q}$ with the usual addition and multiplication:
(g1) $\{a + b\sqrt{5}\}$; (g2) $\{a + b\sqrt[3]{5}\}$; (g3) $\{a + b\sqrt[3]{5} + c\sqrt[3]{25}\}$.

(h) All $f : \mathbf{R} \to \mathbf{R}$ functions with the usual addition and (h1) with the usual multiplication $(fg)(x) = f(x)g(x)$; (h2) with composition $(f \circ g)(x) = f(g(x))$ as multiplication.

25. Prove the following propositions for rings:
(a) The left cancelation law ($ab = ac \Rightarrow b = c$) holds iff $a \ne 0$ and a is not a left zero divisor.
(b) If an element c has a left inverse, then c is not 0 and is not a left zero divisor, but the converse is false.
(c) If a finite commutative ring has no zero divisors, then it is a field.

Remark: It can be proved that (c) holds even without assuming the ring to be commutative.

26. Prove that if $a^2 = a$ holds for every element a in a ring, then the ring is commutative and every element is its own negative. Exhibit examples for such rings.

27. Show that the commutative law for addition does not follow from the other ring axioms, but it follows for rings with identity.

***28.** Prove that if $1 - ab$ has an inverse in a ring (with identity 1), then so does also $1 - ba$.

29. Can we turn the set $\mathbf{Z}$ of integers into a field, if
(a) multiplication is as usual and we can define an addition $\oplus$ arbitrarily;
(b) addition is as usual and we can define a multiplication $\odot$ arbitrarily;
(c) we can define both an addition $\oplus$ and a multiplication $\odot$ arbitrarily?