HOMEWORK

In general, we always assume that a ring R is commutative with an unit 1 without special mention.

1. Let G be a set with an operation $\cdot$ such that

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

for any $a, b, c \in G$. Then if G satisfies that
(1) there exists $e \in G$, such that $a \cdot e = a$ for any $a \in G$;
(2) for any $a \in G$, there exists $b \in G$ such that $a \cdot b = e$.
Then $(G, \cdot, e)$ is a group.

2. Let $G := \{(a_{ij})_{n\times n} \mid a_{ij} \in \mathbb{Z} \,\text{and}\, |(a_{ij})_{n\times n}| = 1 \,\text{or}\, -1\}$. Prove that G is a group respect to the matrix multiplication.

3. Let J be a fixed $n \times n$ matrix over $\mathbb{R}$ with $|J| \neq 0$. Prove that

$$G := \{A \mid A \in \mathbb{R}^{n\times n},\ AJA^T = J\}$$

is a group respect to the matrix multiplication.

4. Let M be an arbitrary set, and $P(M)$ be the set consisting of all the subsets of M. Prove that $P(M)$ is a group respect to the operation

$$A \cdot B = (A - B) \cup (B - A)$$

5. Let G be a group with operation $\cdot$, and S be a nonempty set. Let $M(S, G)$ be the set consisting of all the map $f : S \to G$ with the operation

$$\begin{aligned} f * g :& S \to G, \\ & s \mapsto f(s) \cdot g(s) \end{aligned}$$

Prove that $M(S, G)$ is a group respect to above operation $*$.

6. Prove that: for any abelian group G, we have

$$\circ(ab) \leq \circ(a) \circ (b)$$

for any $a, b \in G$. On the same time, point out there exists non-abelian group such that above equality is not valid.

7. Prove that the group $(\mathbb{Q}, 0, +)$ is not isomorphic to $(\mathbb{Q}^* := \mathbb{Q} - \{0\}, 1, \times)$.

8. Prove that there exists no simple group G of order $|G| = 56$.

9. Prove that any group G of order $|G| = 35$ is cyclic, namely $G = (a)$ for some $a \in G$.

10. Let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, and $U(\mathbb{Z}_n)$ be the group of all units (invertible elements in $\mathbb{Z}_n$). Prove that

$$\bar{m} \in U(\mathbb{Z}_n) \Leftrightarrow (m, n) = 1.$$

11. Let $G = (a)$ be a cyclic group of order n. Prove that its group of isomorphisms $Aut(G) \cong U(\mathbb{Z}_n)$. In particular, when $n = p$ is a prime number, $Aut(G)$ is also cyclic.

12. Let R be a (noncommutative) ring, and $1 - ab$ is invertible. Prove that $1 - ba$ is also invertible.

13. Let R be a ring, then a non-zero element x is called by a nilpotent element if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove:
(1) If x is nilpotent, then $1 - x$ is invertible.
(2) The ring $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ has a nilpotent element if and only if m can be divisible by p^2 for some $p \in \mathbb{Z}^+$.

14. Let $m, n \in \mathbb{Z}$ be positive. Prove that the great common divisor $(m, n) \in \mathbb{Z}$ equals to $(m, n) \in \mathbb{Z}[i]$.

15. Let R be a ring. Prove that $f(x) \in R[x]$ is a zero divisor if and only if $r \cdot f(x) = 0$ for some $r \neq 0 \in R$.

16. Prove that $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ is an Euclidean ring.

17. Prove that $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ is not an UFD.

18. Prove that $\mathbb{C}[x, y]/(x^2 - y^3)$ is not an UFD.

19. Prove that $R[x]$ is an UFD, provided R is so.

20. Let $F \subset E$ and $E \subset K$ be two finite algebraic extensions. Prove that $F \subset K$ is a finite algebraic extension.

21. Prove that the isomorphisms of $\mathbb{Q}$ and $\mathbb{R}$ are both trivial (only identities).

22. Let $\mathbb{R} \subset K$ be a finite algebraic extension with $[K : \mathbb{R}] = 2$. Prove that K is isomorphic to $\mathbb{C}$.

23. Let $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{5}] \subset \mathbb{R}$ be subfields. Prove that $\mathbb{Q}[\sqrt{2}]$ is not isomorphic to $\mathbb{Q}[\sqrt{5}]$.

24. Let F be a finite field, and $F^* := F - \{0\}$. Prove that $(F^*, \times, 1)$ is a cyclic group.

25. Construct a non-separable polynomial.

26. Prove that one can construct regular 17-gons using straight-edge and compass.

27. Prove that one can not construct regular 7-gons using straight-edge and compass.

28. Let $K \subset L$ be a Galois extension, and $K \subset E \subset L$. Prove that E/K is Galois if and only if $Gal(L/E) \subset Gal(L/K)$ is a normal subgroup.

29. Prove that $f(x) = x^n - 1 \in \mathbb{Q}[x]$ can be solved by radicals.

30. Construct a polynomial $f(x) \in \mathbb{Q}[x]$, which cannot be solved by radicals.

31. Prove (by a direct computation) that $\mathbb{Q} = (\mathbb{Q}[\sqrt{2}, \sqrt{11}])^G$ where $G = Gal(\mathbb{Q}[\sqrt{2}, \sqrt{11}]/\mathbb{Q})$ is the Galois group.