Tutorial 4
Discrete Mathematics

Algebraic Structures

1. Let G be the set of all points on the hyperbola $xy = 1$ along with the point $(0, \infty)$ at infinity. Define $(a, \frac{1}{a}) + (b, \frac{1}{b}) = (a + b, \frac{1}{a+b})$. Prove that, G is an abelian group under this operation.

2. Define an operation $\circ$ on $G = \mathbb{R}^* \times \mathbb{R}$ as $(a, b) \circ (c, d) = (ac, bc + d)$. Prove that, $(G, \circ)$ is a non-abelian group.

3. Let G be a non-abelian group, and $a, b \in G$. Prove that, $\texttt{ord}(ab) = \texttt{ord}(ba)$.

4. Let G be a (multiplicative) group, and H, K are subgroups of G. Prove that,
   (a) $H \cap K$ is a subgroup of G.
   (b) $H \cup G$ need not be a subgroup of G.
   (c) $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.
   (d) Define $HK = \{hk \mid h \in H, k \in K\}$. Define KH analogously.
   Prove that, HK is a subgroup of G if and only if $HK = KH$.

5. Let G be a finite group, and $h = \texttt{ord}(a)$ for some $a \in G$.
   Prove that $\texttt{ord}(a^k) = \frac{h}{\texttt{gcd}(h,k)}$ for all $k \in \mathbb{Z}$.

6. Let $R = \mathbb{Z} \times \mathbb{Z}$, and r, s be constant integers. Define two operations, on R as follows:
   $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) * (c, d) = (ad + bc + rac, bd + sac)$.
   (a) Prove that, R is a ring under these operations, $+$ and $*$.
   (b) Prove that R is an integral domain *if and only if* $(r^2 + 4s)$ is not a perfect square.

7. Let $R_1, R_2, \ldots, R_n$ be rings. Prove that, the Cartesian product $(R_1 \times R_2 \times \cdots \times R_n)$ is a ring under component-wise addition and multiplication. Show that, if each R_i is a ring with identity, then so also is the product.

8. Let R be a commutative ring with identity. Prove that, the set $R[x]$ of all univariate polynomials with coefficients from R is again a commutative ring with identity (under polynomial addition and multiplication).

9. Let us define the following sets:
$$\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \quad \text{and} \quad \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$
$$\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \quad \text{and} \quad \mathbb{Q}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\}$$
   Answer the following.
   (a) Prove that $\mathbb{Z}[\sqrt{5}]$ is an integral domain. Argue that $\mathbb{Z}[\sqrt{5}]$ contains infinitely many units.
   (b) Prove that $\mathbb{Z}[\sqrt{-5}]$ is an integral domain. Find all the units of this ring.
   (c) Prove that $\mathbb{Q}[\sqrt{5}]$ is a field.
   (d) Prove that $\mathbb{Q}[\sqrt{-5}]$ is a field.

10. Let $(S, \circ)$ and $(T, \star)$ be two algebraic systems. A function $f : S \longrightarrow T$ is called a *homomorphism* if for any $s_1, s_2 \in S$, we have $f(s_1 \circ s_2) = f(s_1) \star f(s_2)$.

    f is called – (i) an *epimorphism* if it is onto (surjective); (ii) a *monomorphism* if it is one-to-one (injective); and (iii) an *isomorphism* if it is a bijection.

    Answer the following.

    (a) Define a homomorphism from $(\mathbb{N}, +)$ to $(\mathbb{Z}_4, +)$. Determine whether the map you define is an epimorphism, monomorphism or both.

    (b) Consider the algebraic system $(T = \{1, \omega, \omega^2\}, \bullet)$ (here, $\bullet$ is multiplication and $\omega^3 = 1$). Show that $(T, \bullet)$ is a group. Is it abelian too?

    (c) Show that $(T, \bullet)$ is isomorphic to $(\mathbb{Z}_3, +)$.

11. Show that the following systems are semi-groups. Are any of them monoids?

    (a) $(2^X, \cup)$ where X is a finite set.

    (b) $(2^X, \cap)$ where X is a finite set.

    (c) $(\mathbb{Z}^+, \max)$ where for $x, y \in \mathbb{Z}^+$, $\max(x, y)$ is the maximum of x and y.

    (d) $(\mathbb{N}, \max)$.
