Assignment - 5 (submission deadline: 9th April, 2021)

Note: Unless otherwise stated, notation used is as defined in the class.

1. Let G be a group, then prove that G is abelian when $a^2 = a \ \ \forall a \in G$ holds.

2. Which of the following algebraic structures $(R, +, \cdot)$ form a ring?

   (a) Let X be any set and $R = P(X)$, the power set of X. Define $A + B = A \bigtriangleup B$ and $A \cdot B = A \cap B$ for all $A, B \in R$ (where $A \bigtriangleup B = (A - B) \cup (B - A)$)

   (b) In the above set R, define $A + B = A \cup B$ and $A \cdot B = A \cap B$ for all $A, B \in R$.

   (c) Let R be the set of all real-valued continuous functions defined on $\mathbb{R}$. Define $(f+g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(g(x))$ for all $f, g \in R$ and for all $x \in \mathbb{R}$.

   (d) Let R be the set of all twice differentiable real-valued functions having second derivative zero at $x = 0$. Define $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)g(x)$ for all $f, g \in R$ and for all $x \in \mathbb{R}$.

3. Let R be a commutative ring with characteristic p, where p is a prime number. Prove that $(a + b)^p = a^p + b^p$.

4. Show that

   (a) $\mathbb{Z}$ is not a field,

   (b) $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \ \mid \ a, b \in \mathbb{Z}\}$ is not a field.

5. Find all c such that $\mathbb{Z}_3[x]/\langle x^3 + cx^2 + 1\rangle$ is a field.

6. (a) Determine the Galois field $\mathsf{GF}(3^3)$ generated by $x^3 + 2x + 1 = 0$ and list down the polynomial equivalents for each ternary 3-tuple in this field.

   (b) Find the inverse and square root of 121 in $\mathsf{GF}(3^3)$ generated by $x^3 + 2x + 1 = 0$.

   (c) Find all the quadratic residues (or squares) in the field $\mathsf{GF}(3^3)$ (half of the nonzero elements of this field are quadratic residues and half are quadratic non-residues).

7. The field $\mathsf{GF}(2^5)$ can be constructed as $\mathbb{Z}_2[x]/(x^5 + x^2 + 1)$.

   (a) Compute $(x^4 + x^2) \times (x^3 + x + 1)$.

   (b) Using the **Extended Euclidean algorithm**, compute $(x^3 + x^2)^{-1}$.

8. Let E be the modular elliptic curve defined by $y^2 = x^3 + 3x \pmod{17}$.

   (a) Find all points of E (including the point at infinity).

   (b) Find $2(8, 14)$.

   (c) Determine $\mathsf{ord}_E((8, 14))$.

——-END———