**Math 404 – Spring 2025 – Harry Tamvakis**
**PROBLEM SET 3 – Due February 20, 2025**

Reading for this week: Review of basic ring theory (Chapter 2), and 3.1 - 3.7 from Chapter 3.

## Problems

**1)** (a) Given two ideals $I, J$ of a commutative ring $R$, the sum $I + J$ is the ideal consisting of all sums $i + j$ where $i \in I$ and $j \in J$, while the product $IJ$ is defined to be the ideal consisting of all finite sums of products $ij$ with $i \in I$ and $j \in J$. Assume that $I + J = R$ and prove that $IJ = I \cap J$. [Hint: To prove that $I \cap J \subset IJ$, use the fact that there exist $a \in I$ and $b \in J$ such that $a + b = 1$.]

(b) Prove the *Chinese remainder theorem*: if $I + J = R$ then

$$R/(IJ) \cong R/I \times R/J.$$

[Hint: Define a homomorphism $\phi : R \to R/I \times R/J$ and show that (i) $\phi$ is surjective; (ii) $\mathrm{Ker}(\phi) = IJ$.]

(c) Show that if $m$, $n$ are relatively prime positive integers and $a$, $b$ are arbitrary integers then there exists an integer $x$ that satisfies

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.$$

[Hint: One way to do this uses part (b).]

**2)** Let $f$ and $g$ be polynomials of degree $n$ with coefficients in a field $F$. Suppose that there exists $n + 1$ distinct elements $a_1, \ldots, a_{n+1}$ in $F$ such that $f(a_i) = g(a_i)$ for $i = 1, 2, \ldots, n + 1$. Prove that $f = g$.

**3)** Find all integers $a$ such that the polynomial $p(x) = x^3 + ax + 1$ is not irreducible over $\mathbb{Q}$. For each such value of $a$, exhibit a non-trivial factorization of $p$ over $\mathbb{Q}$.

**4)** In this and the following problems, we let $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(a) Prove that the ring $\mathbb{F}_5[x]/(x^2 + x + 1)$ is a field.

(b) Prove that the ring $\mathbb{F}_3[x]/(x^3 + x + 1)$ is not a field.

**5)** In each case, factor the given polynomial as a product of irreducible polynomials:

(a) $x^4 - 12$ in $\mathbb{Q}[x]$; (b) $x^4 + 64$ in $\mathbb{Q}[x]$; (c) $x^4 + 2$ in $\mathbb{F}_3[x]$.

**6)** List all irreducible polynomials of degrees 1 to 5 over the field $\mathbb{F}_2$ with two elements.

**7)** (a) Show that if a polynomial $f(x) \in \mathbb{R}[x]$ has a complex root $z$, then the conjugate $\overline{z}$ is also a root of $f(x)$.

(b) Show that any polynomial $f(x) \in \mathbb{R}[x]$ of degree at least one is a product of irreducible polynomials of degrees 1 or 2.

**8)** (a) Let $F \subset F' \subset K$ be field extensions. Prove that if $[K : F]$ is finite and equal to $[K : F']$, then $F = F'$.

(b) Give an example which shows that this need not be the case if $F, F' \subset K$ but $F$ is not contained in $F'$. Justify your answer!

## <u>Extra Credit Problems.</u>

**EC1)** Let $d$ be a non-zero integer which is not divisible by a perfect square other than one (in other words, $d$ is *square free*). Note that $d$ might be negative. Consider one of the two square roots of $d$, call it $\sqrt{d} \in \mathbb{C}$. Write $\mathbb{Z}[\sqrt{d}]$ for the set

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$$

(this is a subset of $\mathbb{C}$). Check that under the ordinary operations in $\mathbb{C}$, $\mathbb{Z}[\sqrt{d}]$ is a domain (you do not have to write down a proof of this).

(a) Prove that $x + y\sqrt{d}$ is a *unit* in $\mathbb{Z}[\sqrt{d}]$ if and only if $x^2 - dy^2 = \pm 1$.

(b) If $d < 0$, show the number of units in $\mathbb{Z}[\sqrt{d}]$ is always finite and that the group of units $\mathbb{Z}[\sqrt{d}]^\times$ is a finite *cyclic* group. Find this group explicitly if $d < 0$ for each $d$.

(c) Now consider the case $d = 2$. Then $u = 1 + \sqrt{2}$ is a unit of $\mathbb{Z}[\sqrt{2}]$. Show that the group of units contains the cyclic group generated by $u$, which is an infinite cyclic group. (With more work one can show that the group of units is always infinite when $d \geq 2$.)

**EC2)** Suppose that $a, b, c$ are rational numbers such that $a + b + c$, $ab + bc + ca$, and $abc$ are integers. Prove that $a$, $b$, and $c$ must all be integers.