Problem Set 12

Due Thursday, December 4

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Consider the ring $R = \mathbb{Z}[x]$ and the ideal $I = (3, x^3 + x + 1)$.

(a) Show that $R/I \cong (\mathbb{Z}/3)[x]/(x^3 + x + 1)$.

(b) Find, with proof, all the ideals of R that contain I.

Problem 2. Let $R = \mathbb{Z}[\sqrt{-5}]$ where $\sqrt{-5} = \sqrt{5} \cdot i \in \mathbb{C}$ and $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

(a) Prove that $R \cong \mathbb{Z}[x]/(x^2 + 5)$ and, for integers $p \geq 2$, $R/(p) \cong (\mathbb{Z}/p)[x]/(x^2 + [5]_p)$.

(b) Let p be a prime integer. Show that p is a prime element in R if and only if the polynomial $x^2 + [5]_p \in (\mathbb{Z}/p)[x]$ does not have a root in $\mathbb{Z}/p$.

(c) Show that the integer 7 is irreducible[1] in R, but is not a prime element in R.

Problem 3. Let $R = \mathbb{Z}[\sqrt{-2}]$ where $\sqrt{-2} = \sqrt{2} \cdot i \in \mathbb{C}$ and $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$.

(a) Show that R is a Euclidean domain.

(b) Show that $R/(5)$ is a field.

(c) Show that for any nonzero ideal $I \subseteq R$, the quotient ring R/I is finite.

[1] Hint: Consider the complex norm $N : \mathbb{C} \to \mathbb{R}$ given by $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. You can use without proof that $N(\alpha\beta) = N(\alpha)N(\beta)$.