Algebra 3 (2003-04) – Assignment 10

Instructor: Dr. Eyal Goren

Submit by Monday, November 24, 12:00 by mail-box on 10^{th} floor. For full marks solve 6 sub-questions (question 3 is considered as a sub-question). Solving more gives you bonus.

1. Let D be a square free integer (i.e., ± 1 times a product of distinct primes).

(1) Let
$$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}, \qquad \mathbb{Q}[\sqrt{D}] := \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}.$$
Prove that $\mathbb{Q}[\sqrt{D}]$ is a subring of $\mathbb{C}$ and that $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{Q}[\sqrt{D}]$. Furthermore, prove that
$$\mathbb{Z}[\sqrt{D}] \cong \mathbb{Z}[x]/(x^2 - D), \qquad \mathbb{Q}[\sqrt{D}] \cong \mathbb{Q}[x]/(x^2 - D)$$
and that $\mathbb{Q}[\sqrt{D}]$ is a field. (Do NOT use theorems we did not cover in class).

(2) Find the units of $\mathbb{Z}[\sqrt{-1}]$. Show that $\mathbb{Z}[\sqrt{3}]$ has infinitely many units.

(3) Show that $\mathbb{Z}[i]/(1 + 2i)$ is a finite field. Calculate the number of elements of this field. (Suggestion: do the last bit first.)

(4) If $L \supset \mathbb{Q}$ is a field one calls an element $\ell \in L$ an *algebraic integer* if ℓ is a solution of some monic polynomial with integer coefficients $f(x) \in \mathbb{Z}[x]$. It is a general theorem that the set of algebraic integers is a ring. Show that every element of $\mathbb{Z}[\sqrt{D}]$ is an algebraic integer.

Let $\omega = \frac{-1+\sqrt{-3}}{2}$. Prove that
$$\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$$
is a subring of $\mathbb{Q}[\sqrt{-3}]$ that properly contains $\mathbb{Z}[\sqrt{-3}]$. Prove that every element of $\mathbb{Z}[\omega]$ is an algebraic integer. [1]

(5) Prove that $\mathbb{Z}[\omega]$ is a Euclidean domain.

2.

(1) Prove that $\mathbb{Q}[x, y]$ (the ring of polynomials with rational coefficients in two variables) is not a PID.

(2) Prove that $\mathbb{Z}[\sqrt{-6}]$ is not a PID by showing that the ideal $(2, \sqrt{-6})$ is not a principal ideal.

(3) Prove that if R is a PID and $I \lhd R$ is a prime ideal then R/I is a PID.

(4) Prove that $\mathbb{Z}[x]$ is not a PID.

3. Let R be a commutative ring. Assuming that there is an algorithm providing for two co-prime ideals I, J elements $i \in I, j \in J$ such that $1 = i + j$, provide an algorithm to write the inverse isomorphism in the Chinese Remainder Theorem:
$$R/A_1 \times R/A_2 \times \cdots \times R/A_k \longrightarrow R/A_1A_2 \cdots A_k.$$
Apply your method to find an integer x that satisfies the congruences
$$x \equiv 1 \pmod 5, x \equiv 12 \pmod{18}, x \equiv 1 \pmod{19}.$$

[1] In fact, if D is square free and $D \equiv 2, 3 \pmod 4$ then the ring of algebraic integers of $\mathbb{Q}[\sqrt{D}]$ is $\mathbb{Z}[\sqrt{D}]$, while if $D \equiv 1 \pmod 4$ then the ring of algebraic integers of $\mathbb{Q}[\sqrt{D}]$ is $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.