Math 200a (Fall 2016) - Homework 8

Professor D. Rogalski

Posted November 23–Due **Fri. December 2** at 3pm

1 Reading

Read Sections 9.1-9.5.

2 Exercises to submit on Fri. December 2 by 3pm

Exercise 1. Let n be a squarefree integer with $n > 3$ and let $R = \mathbb{Z}[\sqrt{-n}] = \{a+b\sqrt{-n} | a, b \in \mathbb{Z}\}$. (Note this is different from the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ when $n \equiv 1 \mod 4$).

(a). Prove that 2, $\sqrt{-n}$, $1 + \sqrt{-n}$, and $1 - \sqrt{-n}$ are all irreducible in R.

(b). Show that R is not a UFD.

(c). Find an element in R which is irreducible and not prime.

Exercise 2. Let $R = \mathbb{Z} + x\mathbb{Q}[x]$ be the subring of $\mathbb{Q}[x]$ consisting of polynomials with rational coefficients whose constant terms are integers.

(a). Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and those polynomials $f \in R$ which are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1.

(b). Show that $x \in R$ cannot be written as a product of finitely many irreducibles in R. Thus R is not a UFD.

(c). We proved in class that if a commutative ring is noetherian, then every element is a finite product of irreducibles. Thus R must be non-noetherian. Find an explicit infinitely ascending chain of ideals $I_1 \subsetneq I_2 \subsetneq \dots$ of R.

Exercise 3. Suppose that R is a UFD with field of fractions F. A polynomial f is *monic* if it has leading coefficient 1; in other words $f(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1} + x^n$.

(a). Suppose that $f \in R[x]$ factors as $f = gh$ with $g, h \in F[x]$. Show that the product of any coefficient of g with any coefficient of h is in R.

(b). Suppose that f, g, and h are as in part (a) and that moreover g and h are monic. Show that $g \in R[x]$ and $h \in R[x]$.

(c). Show that the ring $S = \mathbb{Z}[2\sqrt{2}] = \{a + b2\sqrt{2} | a, b \in \mathbb{Z}\}$ is not a UFD by finding $f \in S[x], g, h \in F[x]$, where F is the field of fractions of S, which violate the results above.

Exercise 4. Consider the ring $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$, in other words the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$. You may assume the basic properties of the norm function $N(a + b\sqrt{-5}) = a^2 + 5b^2$, as described on p. 229-230 of the text.

(a). Consider the ideals $I_2 = (2, 1 + \sqrt{-5})$, $I_3 = (3, 2 + \sqrt{-5})$, $I_3' = (3, 2 - \sqrt{-5})$. Show that $R/I_2 \cong \mathbb{Z}_2$, and $R/I_3 \cong R/I_3' \cong \mathbb{Z}_3$. Conclude that all three ideals are maximal ideals.

(b). Show that $R/(3) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ as rings. (Hint: Chinese Remainder theorem).

(c). Is $R/(2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$?

Exercise 5. This problem continues the investigations of the ring R in problem 7, so keep the notation introduced there.

(a). Prove that I_2, I_3, I_3' are all not principal ideals of R.

(b). Prove that $I_2^2 = (2)$, $I_2 I_3 = (1 - \sqrt{-5})$, $I_2 I_3' = (1 + \sqrt{-5})$, and $I_3 I_3' = (3)$. In particular, this gives multiple examples showing that a product of nonprincipal ideals can be principal.

Remark. The ring R is an example of a Dedekind domain. *Although unique factorization fails in the sense that R is not a UFD, there is a different kind of unique factorization: every nonzero ideal is a product of maximal ideals in a unique way up to the order of the factors. This is demonstrated by part (b): even though the element* 6 *factors in two essentially different ways (hence R is not a UFD), in the two equal products of principal ideals* $(2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$, *factoring each principal ideal as a product of maximal ideals, one gets the same answer $I_2^2 I_3 I_3'$ on both sides up to rearrangement of the ideals. Dedekind domains are important in algebraic geometry and number theory and may be studied in more detail in Math 200c.*

3 Additional problems on topics covered late in the quarter (not to be handed in)

Exercise 6. Recall that the *characteristic* of a ring R is the order of the element 1 in the additive group of R, when this is a finite number; otherwise we say that R has characteristic 0. Using the Eisenstein criterion, prove that the following elements are irreducible in the indicated ring.

(a). The element $x^n - p \in (\mathbb{Z}[i])[x]$, where p is an odd prime in $\mathbb{Z}$ and $n \geq 1$.

(b). The element $x^2 + y^2 - 1 \in F[x, y]$, where F is any field of characteristic not 2.

Exercise 7. Let R be the ring $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} | a, b \in \mathbb{Z}\}$. By using similar arguments as we used to study the Gaussian integers $\mathbb{Z}[i]$, show that the following are equivalent for an odd prime number $p \in \mathbb{Z}$:

(i) p is not irreducible in R.

(ii) $p = a^2 + 2b^2$ for some $a, b \in \mathbb{Z}$.

(iii) $\overline{-2}$ is a square in $\mathbb{Z}_p$.

(By the way, it is also known that -2 is a square mod p as in condition (iii) if and only if p is congruent to either 1 or 3 modulo 8.)