Math 100b Winter 2010 Homework 5

Due 2/19/09 in class, or by 5pm in HW box on 6th floor of AP&M

Reading

All references will be to Beachy and Blair, 3rd edition.

Read 9.1-9.3.

Assigned Problems

Write up neat solutions to these problems.

Section 5.4: 2, 4.

Section 9.1: 1, 13, 14.

Additional Problems

Before the problems, we discuss some setup. Let d be an integer with $d \neq 0, d \neq 1$ and such that d is squarefree (not divisible by the square of a prime integer.)

Define $R = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}\} \subseteq \mathbb{C}$. You should verify for yourself that R is a subring of $\mathbb{C}$. Note that if d is positive, then R is contained in $\mathbb{R}$, but if d is negative then the elements of R are generally complex. The rings R have many applications in number theory.

Fix d, and consider the ring $R = \mathbb{Z}[\sqrt{d}]$. If $r = a + b\sqrt{d} \in R$, we define the *norm function* $\delta(r) = a^2 - db^2$; note that $\delta(r)$ is always an integer. If d is negative, $\delta(r)$ is the square of the complex norm of r; but there is no such description if d is positive.

1. Let $R = \mathbb{Z}[\sqrt{d}]$ as above.

(a). Prove that the norm function δ is multiplicative: for all $s, t \in R$, $\delta(st) = \delta(s)\delta(t)$.

(b). Prove that $s \in R$ is a unit in R if and only if $\delta(s) = \pm 1$. (Hint: for the direction $\delta(s) = \pm 1$ implies s is a unit, if $s = a + b\sqrt{d}$ consider $t = a - b\sqrt{d}$.) Using this, prove that if $d \leq -2$, then the only units of $\mathbb{Z}[\sqrt{d}]$ are ± 1.

(c). Prove that if $s \in R$ and $\delta(s)$ is a prime number in $\mathbb{Z}$, then s is an irreducible element of R.

Remark. The rings $R[\sqrt{d}]$ with $d \geq 2$ have infinitely many units, in contrast to the result of part (b) for negative d. You saw an example of this in exercises 9.1 13, 14 above.

2. Take $d = -2$, so that $R = \mathbb{Z}[\sqrt{-2}]$. Prove that R is a Euclidean domain with respect to the norm function $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$ defined above.

(Hint: follow carefully the proof we gave (or the book gives) that the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain.)

Remark: you now know that $\mathbb{Z}[\sqrt{d}]$ is a Euclidean domain with respect to the norm function δ defined above, for $d = -1, -2$. Actually the rings $\mathbb{Z}[\sqrt{d}]$ are only Euclidean domains for a relatively few small values of d.

3. Prove that $R = \mathbb{Z}[\sqrt{-6}]$ is not a UFD. (Hint: See Example 9.2.1 in the text for a similar example. Consider the two factorizations $-6 = (-2)(3) = \sqrt{-6}\sqrt{-6}$, and prove that these are two essentially different factorizations into irreducibles, violating the definition of a UFD. To understand what elements are associates of each other in this ring, remember problem 1(b).)

4. Consider $R = \mathbb{Z}[\sqrt{2}]$. Show that the field of fractions $Q(R)$ is isomorphic to $\mathbb{Q}[\sqrt{2}] = \{p + q\sqrt{2} | p, q \in \mathbb{Q}\}$.

(Hint. Define a homomorphism $\phi : Q(R) \to \mathbb{Q}[\sqrt{2}]$ by the formula $[x, y] \mapsto xy^{-1}$, where $[x, y]$ is an arbitrary element of $Q(R)$ (so $x, y \in R$ and $y \neq 0$) in the bracket notation we used for elements of $Q(R)$. You must show that ϕ is well-defined! So you need to explain why xy^{-1} is independent of the choice of representative $[x, y]$ of the equivalence class; also, why is xy^{-1} an element of $\mathbb{Q}[\sqrt{2}]$? Once you have shown that ϕ is well-defined, show that ϕ is a homomorphism of rings, and a bijection.)