Math 258, Section 31: Honors Algebra II
Winter Quarter 2009
John Boller
Homework 3
Due: Friday, January 23, 2009

1. (*) Read Dummit and Foote, Sections 7.5 and 8.1–8.3.

2. (*) Dummit and Foote, Section 7.5, #1, 2, and 3 (including going back to read 7.3 #26).

3. Adopt the notation of Theorem 15.

   (a) Show that if D is a subset of the group of units in R, then Q is isomorphic to R.

   (b) Show that the construction in Theorem 15 yields no "new" rings if R is finite.

4. Dummit and Foote, Section 7.5, # 4:

   Prove that any subfield of $\mathbb{R}$ contains $\mathbb{Q}$.

5. Dummit and Foote, Section 7.5, # 5:

   If F is a field, prove that the field of fractions of $F[[x]]$, the ring of formal power series in x with coefficients in F, is $F((x))$, the ring of formal Laurent series in x with coefficients in F.

6. Let R be the set of all $f \in \mathbb{Q}[x]$ such that $f(x) \in \mathbb{Z}$ for all $x \in \mathbb{Z}$.

   (a) Prove that R is a subring of $\mathbb{Q}[x]$.

   (b) Define, for a positive integer r:

   $$\binom{x}{r} = \frac{x(x-1)(x-2)\dots(x-r+1)}{r!}$$

   Prove that $\binom{x}{r} \in R$ for any positive integer r.

   (c) Prove that $\mathbb{Z}[x]$ is a *proper* subring of R.

   (d) Prove that the ideal (x) in R is *not* a prime ideal in R.

7. Suppose R is a commutative ring with 1. Let $S = R[x_1, x_2, \dots, x_n]$. For $a = (a_1, a_2, \dots, a_n) \in R^n$ define:

   $$\varphi_a : S \to S$$

   by:

   $$\varphi_a(f(x_1, x_2, \dots, x_n)) = f(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$$

   (a) Prove that φ_a is an automorphism of S for all $a \in R^n$.

   (b) Consider the map from R^n to $\mathrm{Aut}(S)$ given by:

   $$a \mapsto \varphi_a$$

   Prove that this map is a group homomorphism from the additive group of R^n to the multiplicative group $\mathrm{Aut}(S)$.

8. (*) Dummit and Foote, Section 8.1, #1, 2, and 5.

9. Dummit and Foote, Section 8.1, # 4:

   Let R be a Euclidean domain.

   (a) Prove that if $(a, b) = 1$ and a divides bc, then a divides c. More generally, show that if some nonzero a divides bc, then $\frac{a}{(a,b)}$ divides c.

   (b) Consider the Diophantine equation $ax + by = N$ where $a, b, N \in \mathbb{Z}$ and a and b are non-zero. Suppose (x_0, y_0) is a solution, that is, $ax_0 + by_0 = N$. Prove that the full set of solutions to this equation is given by:

   $$x = x_0 + m\frac{b}{(a,b)} \quad \text{and} \quad y = y_0 - m\frac{a}{(a,b)}$$

   as m ranges over $\mathbb{Z}$.

10. Dummit and Foote, Section 8.1, #8:

    For quadratic fields $\mathbb{Q}(\sqrt{D})$, it is known that $D = -1, -2, -3, -7, -11, -19, -43, -67$, and -163 are the only negative values of D for which every ideal in the quadratic integer ring $\mathcal{O}$ is principal. Recall that $\mathcal{O} = \mathbb{Z}[\sqrt{D}]$ if $D \equiv 2, 3 \pmod 4$ and $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ if $D \equiv 1 \pmod 4$ as developed in Section 7.1. Below, we determine which of these quadratic integer rings are Euclidean.

    (a) Suppose $D = -1, -2, -3, -7$, or -11.
    Show that $\mathcal{O}$ is Euclidean with respect to the norm N.

    (b) Suppose $D = -43, -67$, or -163.
    Show that $\mathcal{O}$ is not a Euclidean domain with respect to any norm.