Math 258, Section 31: Honors Algebra II
Winter Quarter 2009
John Boller
Homework 4
Due: Friday, February 6, 2009

1. (*) Read Dummit and Foote, Sections 8.3–9.3.

2. (*) Dummit and Foote, Section 8.2, #2–4.

3. Dummit and Foote, Section 8.2, #5:
   Let $R = \mathbb{Z}[\sqrt{-5}]$. Define the ideals $I_2 = (2, 1 + \sqrt{-5})$, $I_3 = (3, 2 + \sqrt{-5})$, and $I_3' = (3, 2 - \sqrt{-5})$.

   (a) Prove that I_2, I_3, and I_3' are not principal ideals.

   (b) Prove that the product of two non-principal ideals may be a principal ideal by showing that $I_2^2 = (2)$.

   (c) Prove that $I_2 I_3 = (1 - \sqrt{-5})$ and $I_2 I_3' = (1 + \sqrt{-5})$ are principal. Conclude that $I_2^2 I_3 I_3' = (6)$.

4. Dummit and Foote, Section 8.2, #6:

   Let R be an integral domain, and suppose that every prime ideal in R is principal. This exercise shows that R must be a P.I.D.

   (a) Assume that the set of ideals of R that are not principal is non-empty, and prove that this set has a maximal element under inclusion.

   (b) Let I be an ideal which is maximal with respect to being non-principal, and let $a, b \in R$ with $ab \in I$ but with $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ be the ideal generated by I and a, let $I_b = (I, b)$ be the ideal generated by I and b, and define $J = \{r \in R \mid rI_a \subset I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R with $I \subset_{\neq} I_b \subset J$ and $I_a J = (\alpha\beta) \subset I$.

   (c) If $x \in I$, show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_a J$ is principal, a contradiction.

5. Suppose R is an integral domain with Euclidean norm N satisfying the following two conditions:

   - For any natural number n, the set $\{0\} \cup \{a \in R \mid N(a) < n\}$ is a subgroup of the additive group of R.
   - For $ab \neq 0$, $N(ab) \geq \max\{N(a), N(b)\}$.

   Then, prove that Euclidean division is unique with respect to N: in other words, prove that for any pair (a, b) with $b \neq 0$, there exists a unique pair (q, r) subject to the conditions $a = bq + r$ and $r = 0$ or $N(r) < N(b)$.

6. Let k be a field. Let R the formal power series ring $k[[x]]$. Define N on $R \setminus \{0\}$ as follows: $N(f)$ is the smallest n for which the coefficient of x^n in f is nonzero.

   (a) Prove that R is a Euclidean domain with Euclidean norm N.

   (b) For $a, b, a + b$ nonzero elements of R, prove that $N(a + b)$ cannot be bounded as a function of $N(a)$ and $N(b)$.

   (c) Prove that if a and b are two power series such that b does not divide a (and $b \neq 0$), there are infinitely many pairs (q, r) for which $a = bq + r$ and $N(r) < N(b)$.

7. Let R be a ring with 1. For a a unit in R, consider the map:

$$\varphi_a : x \mapsto axa^{-1}$$

(a) Prove that φ_a is an automorphism of R.

(b) Prove that the map $a \mapsto \varphi_a$ is a homomorphism from the multiplicative group of units in R to the automorphism group of R.

(c) Suppose the additive group of R is generated by all the multiplicative units. Prove that if L is a left ideal of R with the property that $\alpha(L) \subseteq L$ for all automorphisms α of R, then L is a two-sided ideal of R.

8. (a) Suppose R is an integral domain that is a Noetherian ring (i.e., every ideal in R is finitely generated). Prove that if r is a nonzero non-unit of R, we can write $r = up_1^{k_1} \ldots p_n^{k_n}$ where u is a unit and p_i are irreducible. (Hint: Imitate the proof for principal ideal domains).

   (b) Suppose R is an integral domain. Prove that if a nonzero non-unit $r \in R$ can be written as $up_1^{k_1} \ldots p_n^{k_n}$ where all the p_i are prime and u is a unit, then any two factorizations of r into irreducibles are equal up to ordering and associates.

   (c) Use parts (a) and (b) along with the fact that in a Bezout domain, every irreducible element is prime, to show that every principal ideal domain is a unique factorization domain.

9. Suppose $\mathcal{O}$ is a quadratic integer ring, with N the algebraic norm. Prove that if a is a prime element of $\mathcal{O}$, then $|N(a)|$ is either prime (as a natural number) or the square of a prime. Give examples where $|N(a)|$ is prime and examples where $|N(a)|$ is the square of a prime.

10. Dummit and Foote, Section 8.3, #5:

    Let $R = \mathbb{Z}[\sqrt{-n}]$, where n is a square-free integer greater than 3.

    (a) Prove that 2, $\sqrt{-n}$, and $1 + \sqrt{-n}$ are irreducibles.

    (b) Prove that R is not a U.F.D. Conclude that the quadratic integer ring $\mathcal{O}$ is not a U.F.D. when $D \equiv 2, 3 \pmod 4$ and $D < -3$.

    (c) Give an explicit ideal in R that is not principal.

11. (*) Dummit and Foote, Section 9.1, #1–7, 9, and 16.

12. Dummit and Foote, Section 9.1, #10:

    Prove that the ring $\mathbb{Z}[x_1, x_2, x_3, \ldots]/(x_1x_2,\ x_3x_4,\ x_5x_6,\ \ldots)$ contains infinitely many minimal prime ideals.

13. (*) Dummit and Foote, Section 9.2, #1–3, 6–10.

14. A combination of Dummit and Foote, Section 9.2, #10, 11:

    Let $f(x), g(x) \in \mathbb{Q}[x]$ be two non-zero polynomials, and let $d(x)$ be their gcd.

    (a) Given $h(x) \in \mathbb{Q}[x]$, show that there are polynomials $a(x), b(x) \in \mathbb{Q}[x]$ such that $a(x)f(x) + b(x)g(x) = h(x)$ if and only if $d(x)$ divides $h(x)$.

    (b) If $a_0(x)$ and $b_0(x)$ are particular solutions to the equation in part (a), show that the full set of solutions is given by:

    $$a(x) = a_0(x) + m(x)\frac{g(x)}{d(x)}$$

    $$b(x) = b_0(x) - m(x)\frac{f(x)}{d(x)}$$

    as $m(x)$ ranges over all polynomials in $\mathbb{Q}[x]$.

    (c) When $f(x) = x^3 + 4x^2 + x - 6$ and $g(x) = x^5 - 6x + 5$, find $d(x)$ and at least one pair of solutions for $a_0(x)$ and $b_0(x)$ when $h(x) = d(x)$.