Math 418, Spring 2024 – Homework 2

Due: Wednesday, January 31st, at 9:00am via Gradescope.

Instructions: Students should complete and submit all problems. Textbook problems are from Dummit and Foote, *Abstract Algebra, 3rd Edition.* All assertions require proof, unless otherwise stated. Typesetting your homework using LaTeX is recommended, and will gain you 2 bonus points per assignment.

1. Let R be a Principal Ideal Domain, and I an ideal of R. Prove that every ideal of $S := R/I$ is principal. (S may fail to be an integral domain, and hence is not always a P.I.D itself; for example, $R = \mathbb{Z}$ and $I = 4\mathbb{Z}$.)

2. Dummit and Foote #8.2.5: Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. 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 nonprincipal ideals in R. *(Hint: use Homework 1 Problem 6)*

   (b) Prove that the product of two nonprincipal ideals can be principal by showing that $I_2^2 = (2)$.

   (c) Prove similarly that $I_2 I_3 = (1-\sqrt{-5})$ and $I_2 I_3' = (1+\sqrt{-5})$ are principal. Conclude that the principal ideal (6) is the product of 4 ideals: $(6) = I_2^2 I_3 I_3'$.

3. Dummit and Foote #8.2.7: An integral domain R in which every ideal generated by two elements is principal (i.e., for every $a, b \in R, (a, b) = (d)$ for some $d \in R$) is called a Bezout Domain.

   (a) Prove that the integral domain R is a Bezout Domain if and only if every pair of elements a, b of R has a g.c.d. d in R that can be written as an R-linear combination of a and b, i.e., $d = ax + by$ for some $x, y \in R$.

   (b) Prove that every finitely generated ideal of a Bezout Domain is principal.

   (c) Let F be the fraction field of the Bezout Domain R *(since R is an integral domain, this has the form $F = \{a/b | a \in R, b \in R \setminus \{0\}\}$, with $a/b = c/d$ if and only if $ad = bc$.)*. Prove that every element of F can be written in the form a/b with $a, b \in R$ and a and b relatively prime (1 is a gcd of a and b).

4. Dummit and Foote #8.3.6:

(a) Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

(b) Let $q \in \mathbb{Z}, q > 0$ be a prime with $q \equiv 3 \mod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

(c) Let $p \in \mathbb{Z}, p > 0$ be a prime with $p \equiv 1 \mod 4$ and write $p = \pi\overline{\pi}$ as in Proposition 18 ($\overline{\pi}$ is the complex conjugate of π). Show that the hypotheses for the Chinese Remainder Theorem (Theorem 17 in Section 7 .6) are satisfied and that $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$ as rings. Show that the quotient ring $\mathbb{Z}[i]/(p)$ has order p^2 and conclude that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are both fields of order p.

5. Dummit and Foote #8.3.11: Prove that R is a P.I.D. if and only if R is a U.F.D. that is also a Bezout Domain.

6. Dummit and Foote #9.3.1: Let R be an integral domain with quotient field F and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$. Prove that if $a(x) \notin R[x]$ then R is not a Unique Factorization Domain. Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a U.F.D.