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 $I = 4\mathbb{Z}$.)

   Proof. By the Fourth (or "Lattice") Isomorphism Theorem (see Dummit and Foote Theorem 7.8(3)), the canonical map $J \to J/I$ from the set of ideals in R containing I to the set of ideals of R/I is a 1-1 correspondence. Since R is PID, let $J = (a)$. We check that $\bar{a} \in R/I$ generates J/I. Suppose $\bar{r}$ is an element in J/I. Choose a representative $r \in J$ for $\bar{r}$. Then $r = ba$ for some $b \in R$. But then we have $\overline{b}\overline{a} = (b + I)(a + I) = ba + I = r + I = \overline{r}$ in R/I, so $J/I = (\overline{a})$. $\square$

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)*

   Proof. Suppose I_2 is principal i.e. $I_2 = (r)$. This means that $2 = u_1 r$ and $1+\sqrt{-5} = u_2 r$. From Problem 6b of Homework 1, 2 and $1+\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. This implies that u_1 and u_2 are units (because if r is a unit, then $I_2 = R$, and it can be directly checked that $1 \notin I_2$ – see below). But then $1 + \sqrt{-5} = u_2 u_1^{-1} 2$, and by Problem 6b of Homework 1 this cannot be so (using the fact from Problem 6a of Homework 1 that the set of units in R is $\{1, -1\}$).
   To check that $1 \notin I_2$, consider the ring $\mathbb{Z}[\sqrt{-5}]/(2) = (\mathbb{Z}/2\mathbb{Z})[\sqrt{-5}] = \{0, 1, \sqrt{-5}, 1+\sqrt{-5}\}$ is an integral domain. In $\mathbb{Z}[\sqrt{-5}]/(2)$, $(1+\sqrt{-5})^2 = 0$, so $1 \notin (1+\sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]/(2)$, so $1 \notin (2, 1 + \sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]$.
   Identical arguments show that I_3 and I_3' are non-principal. $\square$

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

Proof. The ideal I_2^2 is generated by $\{r_1, r_2, r_3\} = \{4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\}$. First observe that $2 = r_2 - r_1 - r_3$, so the ideal (2) sits inside I_2^2. Also, $4 = 2 \cdot 2, 2+2\sqrt{-5} = 2 \cdot (1+\sqrt{-5}), -4+2\sqrt{-5} = 2 \cdot (-2+\sqrt{-5})$, and so the opposite inclusion is also true. So $I_2^2 = (2)$. □

(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: $(6) = I_2^2 I_3 I_3'$.

Proof. By entirely similar argument as part (b), we can show that $I_2 I_3 = (1-\sqrt{-5})$ and $I_2 I_3' = (1+\sqrt{-5})$. Since $6 = (1-\sqrt{-5})(1+\sqrt{-5})$, the conclusion that $(6) = I_2^2 I_3 I_3'$ follows directly. □

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 $x, y \in R$.

Proof. First assume R is a Bezout domain, and let $a, b \in R$. Let $(d) = (a, b)$; the two directions of containment mean that d divides a and b, so it is a common divisor, and d can be written in the form $d = ax = by, x, y \in R$. Finally if $d'|a$ and $d'|b$, then $d'|(ax+by) = d$, so d is a gcd.

For the other direction, suppose that 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 $x, y \in R$. Then if $a, b \in R$, let d be a gcd of a and b, and let $d = ax + by$ be the promised R-linear combination. Since d is a gcd, we have $a, b \in (d)$, and since d is a linear combination, $d \in (a, b)$; thus $(a, b) = (d)$ is principal. □

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

Proof. Let $I = (a_1, \ldots, a_n)$ be a finitely-generated ideal with $n \geq 2$. Let d be a gcd of a_{n-1} and a_n such that $d = a_{n-1}x + a_n y, x, y \in R$, and let $J = (a_1, \ldots, a_{n-2}, d)$. Then $I \subseteq J$ since $a_{n-1}, a_n \in (d) \subseteq J$. On the other hand, $J \subseteq I$ since $d = a_{n-1}x + a_n y \in (a_{n-1}, a_n) \subseteq I$. Thus, I has one fewer generator than in the original presentation, so by induction I 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).

Proof. Let $a/b \in F$, and let d be a gcd of a and b i.e. $a = du, b = dv$. Then $v \neq 0$ since $b \neq 0$ (so d also $\neq 0$) and $u/v = a/b$ since $bu = duv = av$.

Let e be a common divisor of u and v i.e $u = ex, v = ey$. Then $a = dex, b = dey$, so de is a common divisor of a and b. Since d is a gcd, this means that $de|d$, so e is a unit (this follows from the "cancellation property" for integral domains. In more detail, $d = dez$, so $0 = d - dez = d(1 - ez)$, and so $1 - ez = 0$). Since every common divisor of u and v is a unit, they divide 1, which is itself a common divisor of u and v, so 1 is a gcd of u and v. □

4. Dummit and Foote #8.3.6:

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

Proof. $\mathbb{Z}[i]$ is a Euclidean domain, hence a PID. Simple norm arguments show that $1 + i$ is irreducible, and in a PID this means that $1 + i$ is prime. Therefore, $(1 + i)$ is a prime ideal, and again since $\mathbb{Z}[i]$ is a PID, this means it is maximal; thus, $\mathbb{Z}[i]/(1 + i)$ is a field. Now, in $\mathbb{Z}[i]/(1 + i)$ we have $2 = (1 + i)(1 - i) = 0$ and $i = 1 + i - 1 = -1 = 1$, so 0 and 1 are the only elements of $\mathbb{Z}[i]/(1 + i)$ (and since $1 + i$ is not a unit is $\mathbb{Z}[i]$, the quotient can't be just $\{0\}$). □

(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.

Proof. Since q is prime in $\mathbb{Z}$ and $\equiv 3 \mod 4$, by Fermat's sum-of-squares theorem and our lemma from class, q is prime in $\mathbb{Z}[i]$. Therefore, (q) is a prime ideal in $\mathbb{Z}[i]$, so since $\mathbb{Z}[i]$ is a PID (q) is maximal and $\mathbb{Z}[i]/(q)$ is a field. The following is a complete set of coset representatives:

$$\{a + bi | 0 \leq a < q, 0 \leq b < q\},$$

and this has size q^2. □

(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.

Proof. Since p is prime in $\mathbb{Z}$, π and $\overline{\pi}$ are non-real, and therefore distinct. They are irreducibles since their norms are prime, so by the argument in part (a), $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are fields.

Since the units in $\mathbb{Z}[i]$ are just $\{1, -1, i, -i\}$, we also see that π and $\overline{\pi}$ are not associates. Since their norms are prime, this means that their gcd equals 1. Since

$\mathbb{Z}[i]$ is a PID, this means that 1 is a $\mathbb{Z}[i]$-linear combination of π and $\overline{\pi}$ i.e. (π) and $(\overline{\pi})$ are comaximal.

By the Chinese Remainder Theorem, $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$. As in part b,

$$\{a + bi | 0 \leq a < p, 0 \leq b < p\}$$

is a complete set of coset representatives for $\mathbb{Z}[i]/(p)$, of size p^2. Since neither $\mathbb{Z}[i]/(\pi)$ nor $\mathbb{Z}[i]/(\overline{\pi})$ is the zero ring, they must both have order p since this is the only nontrivial factorization of p^2 in $\mathbb{Z}$. □

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.

   Proof. In the forward direction suppose R is a P.I.D. Then, by definition, it is also a Bezout Domain and we have proved in class that it is also a U.F.D.

   Conversely, suppose I is an ideal. Let a be a non-zero element of I with the minimal number of irreducible factors. We will show that $I = (a)$. So suppose there is a non-zero element $b \in I$ such that $b \notin (a)$. Consider the ideal (a, b). Because R is a Bezout domain $(a, b) = (c)$ for some non-zero element c. This implies that $a = rc$ for some element r. If r is a unit, then $b \in (a)$, a contradiction. But then, since R is a U.F.D, this implies that the element c has a smaller number of irreducible factors, again a contradiction. □

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.

   Proof. Suppose R is a UFD. By Gauss' Lemma, there exists $r \in F$ such that $ra(x), r^{-1}b(x) \in R[x]$. Since a and b are monic, $r, r^{-1} \in R$, but this means that $a(x) = r^{-1}ra(x) \in R[x]$ and $b(x) = rr^{-1}b(x) \in R[x]$, a contradiction.

   In $\mathbb{Z}[2\sqrt{2}][x]$, let $p(x) = x^2 + 2\sqrt{2}x + 8 = (x + \sqrt{2})(x - \sqrt{2})$. Both factors are monic, of smaller degree, and since $\sqrt{2} \notin \mathbb{Z}[2\sqrt{2}]$, the factors are not contained in $\mathbb{Z}[2\sqrt{2}][x]$. Therefore, $\mathbb{Z}[2\sqrt{2}$ is not a UFD. (In particular, $8 = 2^3 = (2\sqrt{2})^2$ is an element with distinct factorizations into irreducibles). □