Problem Set 1
Abstract Algebra II

Bennett Rennier
barennier@gmail.com

January 15, 2018

Section 8.1

Ex ? Let a and b be two relatively prime positive integers. Prove that every sufficiently large positive integer N can be written as an integer combination $ax + by$ of a and b where x and y are non-negative. Prove in fact that the integer $ab - a - b$ cannot be written as a positive integer combination of a and b, but that every integer greater than $ab - a - b$ can be.

Proof. Suppose there exists $x, y \in \mathbb{N}$ such that $xa + yb = ab - a - b$. Rearranging we get that $(x + 1 - b)a + (y + 1)b = 0$. Since y, a, and b are positive, this means that $x + 1 - b < 0$, which means that $x \leq b$. If we look at the original equation mod b, we get that $xa = -a \pmod{b}$. This means that $x = -1 \pmod{b}$. Since $x \leq b$, this means that $x = b - 1$. By similar argument, we see that $y = a - 1$. Plugging this in we get that $ab-a-b = xa+yb = (b-1)a+(a-1)b = ab-a+ab-b$, which means that $ab = ab+ab = 2ab$, this would mean that $ab = 0$, which is a contradiction as $a, b > 0$. This proves that $ab-a-b$ cannot be expressed.

Lemma: We can choose $x, y \in \mathbb{Z}$ such that $t = xa + yb$ where $0 \leq x < b$ for any t. Proof: Since $\gcd(a, b) = 1$ we know that there exist $x, y \in \mathbb{Z}$ such that $xa + yb = 1$. This means that $t = txa + tyb$. This shows that $t = txa + typ + mab - mab = (tx + mb)a + (y - ma)b$ for all $m \in \mathbb{Z}$. Choose m so that $0 \leq tx + mb < b$. This proves the lemma.

Let $n > 0$. By our lemma, choose x and y such that $xa + yb = ab - a - b + n$ where $0 \leq x < b$. Then $yb = ab - a - b + n - xa = (b - x - 1)a + n - b$. If we divide by b, we get that $y = \frac{(b-x-1)a}{b} + \frac{n}{b} - 1$. This means that $y + 1 = \frac{(b-(x+1))a}{b} + \frac{n}{b}$. Since $0 \leq x < b$, then $0 < x + 1 \leq b$, which means that $b - (x + 1) \geq 0$. Since $b - (x + 1)$, a, b, and n are all positive, this means that $y + 1 > 0$, which shows that $y \geq 0$. Since $x, y \geq 0$, this proves that all integers greater than $ab - a - b$ can be written as a nonnegative integer combination of a and b. $\square$

Ex 9 Prove that the ring of integers $\mathcal{O}$ in the quadratic integer ring $\mathbb{Q}(\sqrt{2})$ is a Euclidean Domain with respect to the norm given by $N(a + b\sqrt{2}) = |a^2 - 2b^2|$. $\mathbb{Z}(\sqrt{2})$?

Proof. Let $a = a_1 + a_2\sqrt{2}$ and $b = b_1 + b_2\sqrt{2}$ be arbitrary elements of $\mathbb{Z}[\sqrt{2}]$, where $b \neq 0$. Since $\mathbb{Q}(\sqrt{2})$ is a field, we know that there exists a $x = x_1 + x_2 \in \mathbb{Q}(\sqrt{2})$ such that $x = \frac{a}{b}$. Let c_1 and c_2 be the closest integers to x_1 and x_2 respectively. Let $c = c_1 + c_2\sqrt{2}$, which is in $\mathbb{Z}[\sqrt{2}]$. Let $y = \frac{a}{b} - c = (x_1 - c_1) + (x_2 - c_2)\sqrt{2}$. This means that $yb = a - cb$, which turns into $a = cb + yb$. We see that $yb = (\frac{a}{b} - c)b = a - cb$ which is clearly in $\mathbb{Z}[\sqrt{2}]$.

Now we need to check that $N(yb) < N(b)$ or $N(yb) = 0$. Since c_1 and c_2 were defined as the closest integers to x_1 and x_2 respectively, we see that that $N(y) = |(x_1 - c_1)^2 - 2(x_2 - c_2)^2| \leq |(x_1 - c_1)^2| + |-2(x_2 - c_2)^2| = (x_1 - c_1)^2 + 2(x_2 - c_2)^2 \leq \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{3}{4}$. This means that $N(yb) = \frac{3}{4}N(b)$. Thus $N(yb) < N(b)$ unless $N(b) = 0$, which shows that $N(yb) = 0$. This proves the statement. $\square$

Ex 10 Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$. [Use the fact that $I = (\alpha)$ for some nonzero α and then use the Division Algorithm in this Euclidean Domain to see that every coset of I is represented by an element of norm less than $N(\alpha)$.]

Proof. Let $I \subseteq \mathbb{Z}[i]$ be a nonzero ideal. Since $\mathbb{Z}[i]$ is an Euclidean domain with norm $N(a + bi) = a^2 + b^2$, this means that $\mathbb{Z}[i]$ is also a PID. Thus, $I = (\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. Let $x + I$ be an arbitrary coset of I. By the Euclidean Algorithm, there exists $q, r \in R$ such that $x = q\alpha + r$ where $N(r) < N(\alpha)$. Rearranging the equation, we get that $r = x - q\alpha = x + (-q)\alpha \in x + I$. Thus, $x + I = r + I$, which means that every coset of I can be represented by an element with a norm less that $N(\alpha)$. But we can see that under this norm, there are only finitely many elements with norm n for each $n \in \mathbb{N}$ (Visually, this norm is a circle in the complex plane and can only intersect finitely many integer coordinates). Thus, there are only finitely many elements in $\mathbb{Z}[i]$ with norm less than α. This proves that there are only finitely many cosets for I, and thus $\mathbb{Z}[i]/I$ is finite. $\square$

Ex 11 Let R be a commutative ring with 1 and let a and b be nonzero elements of R. A least common multiple of a and b is an element $e \in R$, such that

i) $a \mid e$ and $b \mid e$, and

ii) if $a \mid e'$ and $b \mid e'$, then $e \mid e'$.

a) Prove that a least common multiple of a and b (if such exists) is a generator for the unique largest principal ideal contained in $(a) \cap (b)$.

b) Deduce that any two nonzero elements in a Euclidean Domain have a least common multiple which is unique up to multiplication by a unit.

c) Prove that in a Euclidean Domain the least common multiple of a and b is $\frac{ab}{\gcd(a,b)}$.

Proof. a) Let e be a least common multiple of a and b. Since $a \mid e$ and $b \mid e$, we see that $(e) \subseteq (a)$ and that $(e) \subseteq (b)$. Thus, we get that $(e) \subseteq (a) \cap (b)$. Now, let I be an ideal contained in $(a) \cap (b)$. This means that $I \subseteq (a)$ and that $I \subseteq (b)$. Let i be an element of I. Since $I \subseteq (a)$, this means that $i = ax$ for some $x \in R$. Similarly, $i = by$ for some $y \in R$. This means that $a \mid i$ and $b \mid i$. Since e is a least common multiple, this means that $e \mid i$. Thus $(i) \subseteq (e)$. This means that $i \in (e)$. Since i was an arbitrary member of I, this proves that $I \subseteq (e)$. Thus e is the greatest ideal contained in $(a) \cap (b)$. [Is principal necessary?]

b) Since all Euclidean Domains are PIDs, this means that $(a) \cap (b) = (e)$ for some $e \in R$. Thus, since (e) is the largest principal ideal contained in $(a) \cap (b)$, this means that e is the least common multiple. Assume that f is also a least common multiple. Then (f) is also the unique principal ideal contained in $(a) \cap (b)$. Thus, $(f) = (e)$. Since all Euclidean Domains are Integral Domains, by Proposition 3, this means that $f = ue$ for some unit $r \in R$. This proves that e is unique up to multiplication by a unit.

c) Let d be the greatest common divisor of a and b. Since $d \mid a$ and $d \mid b$, we know that $d \mid ab$. Thus $ed = ab$ for some $e \in R$. Claim: e is the least common multiple of a and b.

   1) Since $d \mid ab$, we can let $e = \frac{ab}{d}$. Since $d \mid b$, we see that $e = a \cdot \frac{b}{d}$. Thus, $e \in (a)$, which means that $(e) \subseteq (a)$. Similarly, $(e) \subseteq (b)$. This means that $(e) \subseteq (a) \cap (b)$.

   2) Suppose there exists an $f \in R$ such that $(e) \subseteq (f) \subseteq (a) \cap (b)$. We see that since $a \mid f$ that $f = ax$ for some $a \in R$. Multiplying by b, we get that $bf = abx$. Since $ed = ab$, this means that $bf = abx = edx$. Since $(e) \in (b)$, this means $b \mid e$, which means we get that $f = \frac{edx}{b} = e \cdot \frac{dx}{b}$. This shows that $f \in (e)$, which means that $(e) = (f)$. This proves that e is the least common multiple of a and b.

□

Section 8.2

Ex 1 Prove that in a Principal Ideal Domain two ideals (a) and (b) are comaximal if and only if a greatest common divisor of a and b is 1.

Proof. Suppose that 1 is a greatest common divisor of a and b. This means that $1 = sa + tb$ for some $s, t \in R$. Thus, $1 \in (a, b)$. This proves that $(a, b) = (a) + (b) = R$.

Now suppose (a) and (b) are comaximal, that is $(a) + (b) = R$. Since $1 \in R$, this means that $sa + tb = 1$ for some $s, t \in R$. Thus, $1 \in (a, b)$. This means that $(a, b) = R = (1)$. By proposition 2, this proves that 1 is a greatest common divisor of a and b. □

Ex 3 Prove that a quotient of a PID by a prime ideal is again a PID.

Proof. Let R be a PID, and I be a prime ideal in R. Since R is a PID, this means that I is maximal (Proposition 7). Thus, R/I is a field. Let J be a nonzero ideal of R/I, and let $a \in J$ be nonzero. Since R/I is a field, this means that a^{-1} exists. Thus, $1 = a^{-1}a \in J$. This means that $J = (1)$, which is principal. Thus, all the ideals of R/I are principal. □

Ex 6 Let R be an integral domain and suppose that every prime ideal in R is principal.

a) Assume that the set of ideals of R that are not principal is nonempty and prove that this set has a maximal element under inclusion.

b) Let I be an ideal which is maximal with respect to being nonprincipal, and let $a, b \in R$ with $ab \in I$, but $a \notin I$ 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 $J = \{r \in R \mid rI_a \subseteq I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principals ideals in R with $I \subsetneq I_b \subseteq J$ and $I_aJ = (\alpha\beta) \subseteq I$.

c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_aJ$ is principal, a contradiction, and conclude that R is a PID.

Proof. a) Since the set of ideals of R that are not principal is nonempty, we can put a partial ordering on this set using set inclusion. Suppose $I_1 \subseteq I_2 \subseteq \ldots$ is a chain of ideals. Claim: $\cup_{i\in\mathbb{N}} I_i$ is an ideal. Let $a, b \in \cup_{i\in\mathbb{N}} I_i$. This means that $a \in I_j$ and $b \in I_k$ for some $i, j \in \mathbb{N}$. Assume without loss of generality that $j \leq k$. This means that $a, b \in I_k$. This proves that $a + b \in I_k$ and that $ra \in I_k$ for all $r \in R$. Thus, $a + b, ra \in \cup_{i\in\mathbb{N}} I_i$. This proves that $\cup_{i\in\mathbb{N}} I_i$ is an ideal. We also clearly see that $I_j \subseteq \cup_{i\in\mathbb{N}} I_i$ for every $j \in \mathbb{N}$. Thus proves that every chain has an upper bound. By Zorn's Lemma, this means that this set has a maximal element.

b) Suppose that I_a is not a principal ideal. Since $a \notin I$, we see that $I \subsetneq I_a = (I, a)$. However, I is the maximal nonprincipal ideal. This proves that I_a is a principal ideal.

Let $x_1i_1 + y_1a$ and $x_2i_2 + y_2b$ be arbitrary elements in I_a and I_b respectively. We see that $(x_1i_1 + y_1a)(x_2i_2 + y_2b) = x_1x_2i_1i_2 + x_1i_1y_2b + y_1x_2i_2a + y_1y_2ab$. Since i_1, i_2, and ab are all in I, this proves that this product is in I. Thus, $I_b \subseteq J$. By a similar argument as the one used in the last paragraph $I \subsetneq I_b$. This means that $I \subsetneq I_b \subseteq J$. Since I is the maximal nonprinciple ideal, this means that J must be principle.

Let $I_a = (\alpha)$ and $J = (\beta)$ since they are both principle. We see that $\alpha\beta \in I_aJ$. Letting $x\alpha y\beta$ be an arbitrary element of I_aJ, we see that $x\alpha y\beta = xy\alpha\beta \in (\alpha\beta)$. This proves that $I_aJ = (\alpha\beta)$. It follows from the definition of J that $I_aJ \subseteq I$. This shows that $I_aJ \subseteq I \subseteq I_b$.

c) Let $x \in I$. Since $I \subseteq I_a = (\alpha)$, we see that $x = s\alpha$ for some $s \in R$. Since $sI_a = s(\alpha) = (s\alpha) = (x) \subseteq I$, we see that $s \in J$. This means that $I \subseteq I_aJ$ and thus that $I = I_aJ$. Since $I_aJ = (\alpha\beta)$, we see that I is principal. This is a contradiction against the definition of I. Thus, either Zorn's Lemma is false or the set of all nonprincipal ideals of R is empty. Since we assume Zorn's Lemma, it must be that R contains no nonprincipal ideals, which makes R a PID.

□

Section 8.3

Ex 2 Let a and b be nonzero elements of the Unique Factorization Domain R. Prove that a and b have a least common multiple and describe it in terms of the prime factorizations of a and b in the same fashion that Proposition 13 describes in their greatest common divisor.

Proof. Let a and b be two nonzero elements of a UFD R. Let $a = p_1^{e_1}p_2^{e_2}\ldots p_n^{e_n}$ and $b = p_1^{f_1}p_2^{f_2}\ldots p_n^{f_n}$ be the unique prime factorizations for a and b, where $p_1 \ldots p_n$ are distinct primes, $e_i \geq 0$, and $f_i \geq 0$. Claim: $\ell = p_1^{\max(e_1,f_1)}p_2^{\max(e_2,f_2)}\ldots p_n^{\max(e_2,f_2)}$ is the least common multiple of a and b. Since the exponents of the primes in ℓ are larger than the exponents on the corresponding primes of both a and b, we see that a and b divide ℓ. Let k be a common multiple of a and b. Since $k \in R$, it has a unique factorization. Let this factorization be

$c = q_1^{g_1} q_2^{g_2} \dots q_m^{g_m}$. Since p_i divides a and a divides c, we see that p_i divides c. This means that p_i must divide one of the q_j's. This means that $\{p_i, \dots, p_n\} \subseteq \{q_i, \dots q_m\}$, and also that the exponents of the primes in common must be greater in c than in a. By similar argument, the exponents of the primes in common must be greater in c than in b as well. This means that $c = p_1^{h_1} p_2^{h_2} \dots p_n^{h_n} q_1^{h_{n+1}} \dots q_m^{h_m}$, where $h_i \geq \max(e_i, f_i)$ for $i \leq n$. This shows that ℓ divides c. Thus, $\operatorname{lcm}(a, b) = \ell$, which proves that any $a, b \in R \setminus \{0\}$ have a least common multiple in R. $\square$

Ex 3 Determine all the representations of the integer $2130797 = 17^2 \cdot 73 \cdot 101$ as a sum of two squares.

Proof. By Corollary 19, we see that since $17 = 73 = 101 = 3 \pmod 4$, that 2130979 can be written as the sum of two squares. Also by that Corollary, we see that there are $4 \cdot 3 \cdot 2 \cdot 2 = 48$ ways to do so. Let $2130797 = A^2 + B^2$. Since $17^2 = (4+i)^2(4-i)^2$, $73 = (8+3i)(8-3i)$, and $101 = (10+i)(10-i)$, the factorization of $A + Bi$ into units are

$$\begin{aligned}
(4+i)(4+i)(8+3i)(10+i) &= 851 + 1186i \\
(4+i)(4+i)(8-3i)(10+i) &= 1421 + 334i \\
(4+i)(4+i)(8+3i)(10-i) &= 1069 + 994i \\
(4+i)(4+i)(8-3i)(10-i) &= 1459 + 46i \\
(4+i)(4-i)(8+3i)(10+i) &= 1309 + 646i \\
(4+i)(4-i)(8-3i)(10+i) &= 1411 - 374i \\
(4+i)(4-i)(8+3i)(10-i) &= 1411 + 374i \\
(4+i)(4-i)(8-3i)(10-i) &= 1309 - 646i \\
(4-i)(4-i)(8+3i)(10+i) &= 1459 - 46i \\
(4-i)(4-i)(8-3i)(10+i) &= 1069 - 994i \\
(4-i)(4-i)(8+3i)(10-i) &= 1421 - 334i \\
(4-i)(4-i)(8-3i)(10-i) &= 851 - 1186i
\end{aligned}$$

From this we see that $2130797 = 851^2 + 1186^2 = 1421^2 + 334^2 = 1069^2 + 994^2 = 1459^2 + 46^2 1309^2 + 646^2 = 1411^2 + 374^2$ are 6 different ways to write 2130797 as the sum of two squares. When we consider that there are 2 choices for ordering and 4 choices for different signs, this gives us the full $2 \cdot 4 \cdot 6 = 48$ possible ways. $\square$

Ex 6 a) Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

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

Proof. a) [I tried to do this problem before I read the chapter, so there is much more work than necessary.] We know that $\mathbb{Z}[i]$ is a ED under the norm $N(a+bi) = a^2 + b^2$. We also see that $N((a+bi)(x+yi)) = N((ax-by)+(bx+ay)i) = (ax-by)^2 + (bx+ay)^2 = (ax)^2 + (by)^2 + (bx)^2 + (ay)^2 - axby + bxay = x^2(a^2+b^2) + y^2(a^2+b^2) = (x^2+y^2)(a^2+b^2) =$

$N(a+bi) \cdot N(x+yi)$. Thus, $N(ab) = N(a)N(b)$ for all $a, b \in \mathbb{Z}[i]$. Let $1+i = ab$ for some $a, b \in \mathbb{Z}[i]$. We see that

$$2 = 1^2 + 1^2 = N(1+i) = N(ab) = N(a)N(b)$$

which means that $N(a) = 1$ and $N(b) = 2$ or vice-versa. Without loss of generality assume that $N(a) = 1$. Let $a = x + iy$. This means that $N(a) = x^2 + y^2 = 1$. Rearranging, we get that $x^2 \leq 1 - y^2 \leq 1$, which shows that $x = 0$ or $x = 1$. Similarly, $y = 0$ or $y = 1$. However, if $x = y = 1$, then $N(a) = 1^2 + 1^2 = 2$, a contradiction. Similarly, it's a contradiction if $x = y = 0$. Thus, either $x = 1$ and $y = 0$ or $y = 1$ and $x = 0$. This means that $a = 1$ or $a = i$. However, both 1 and i are units ($i \cdot i^3 = 1$). This proves that $1 + i$ is irreducible. Since $\mathbb{Z}[i]$ is a ED, and thus a PID, this means that $1 + i$ is prime, which means that $(1 + i)$ is a prime ideal. Since $\mathbb{Z}[i]$ is a PID, this means that $(1 + i)$ is a maximal ideal. Finally, this implies that $\mathbb{Z}[i]/(1 + i)$ is a field. By Section 8.1 Ex 10, we know that $\mathbb{Z}[i]/(1 + i)$ is finite.

Let $a+bi \in \mathbb{Z}[i]/(1+i)$. We see that $(1+i)(1+i) = 1+i+i-1 = 2i \in \mathbb{Z}[i]/(1+i)$ and that $(1-i)(1+i) = 1+i-i+1 = 2 \in \mathbb{Z}[i]/(1+i)$. Thus, $a, b \in \{0, 1\}$. Let $I = (i + 1)$ so that we can use parenthesis in the next equation. We see that

$$-1 + I = -1 + 2 + I = 1 + I = 1 - (i + 1) + I = -i + I = -i + 2i + I = i + I$$

Since $\mathbb{Z}[i]/(1 + i)$ is a field, this means that $1 + (1 + i) \neq (1 + i)$, so the only elements of $\mathbb{Z}[i]/(1 + i)$ are $1 + (1 + i)$ and $(1 + i)$. This proves that $\mathbb{Z}[i]/(1 + i)$ is a field of order 2.

b) Since $q = 3 \pmod 4$, q is irreducible by Proposition 18. Since $\mathbb{Z}[i]$ is a PID, (q) is prime. This means that (q) is a prime ideal. Since $\mathbb{Z}[i]$ is a PID, this means (q) is maximal, and thus that $\mathbb{Z}[i]/(q)$ is a field.

Let $x + yi + (q) \in \mathbb{Z}[i]/(q)$, where $x, y \in \mathbb{Z}$. Since $\mathbb{Z}$ is a Euclidean Domain, we see that $x = pq + r$ for some $0 \leq r < q$. Similarly, $y = sq + t$ where $0 \leq t < q$. This means that $x + yi + (q) = pq + r + (sq + t)i + (q) = r + ti + (q)$. Thus, all the cosets of $\mathbb{Z}[i]/(q)$ are of the form $x + yi + (q)$ where $0 \leq x, y < q$. Suppose $a + bi + (q) = x + yi + (q)$ are two such cosets. Then $(a - x) + (b - y)i \in (q)$. This means that $(a - x) + (b - y)i$ is divisble by q. Thus $a - x$ and $b - y$ are both divisible by q. However, since $0 \leq a, b, x, y < q$, it's impossible for $a - x$ and $b - y$ to be divisible by q. Thus, the cosets of this form are distinct. There are clearly q^2 cosets of this form, which proves that the order of the field $\mathbb{Z}[i]/(q)$ is p^2.

□

Ex 8 Let R be the quadratic integer ring $\mathbb{Z}\left[\sqrt{-5}\right]$ and define the ideals $I_2 = (2, 1 + \sqrt{-5})$, $I_3 = (3, 2 + \sqrt{-5})$, and $I_3' = (3, 2 - \sqrt{-5})$. Prove that $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{5}$ are irreducibles in R, no two of which are associate in R, and that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{5})$ are two distinct factorizations of 6 into irreducibles in R.

Proof. [Incomplete. The Frobenius Coin Problem took a long time.] □

Additional Problems

Ex A At the end of Section 8.3 is a summary which gives examples of rings which shows that there are strict inclusions among each type of ring we considered this week. Please write up a verification that each example actually proves the corresponding inclusion is strict.

Proof. Section 8.3 Ex 8 proves that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. It is an integral domain as $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$ which is a field.

$\mathbb{Z}[x]$ is not a PID as $(2, x)$ is an ideal which is not principal. $\mathbb{Z}[x]$ is a UFD as $\mathbb{Z}$ is a UFD. [The proof of this fact is later on in the book.]

The proofs that $\mathbb{Z}[(1 + \sqrt{-19})/2$ is a PID but not a ED are unfortunately omitted due to time constraints, but I will make sure to know them.

$\mathbb{Z}$ is a Euclidean domain with $N(n) = |n|$ (in fact, it's the prime example of one). It's not a field as 2 has no inverse. $\square$