Exercises from Chapter 8

Wesley Basener

May 7, 2025

Problem 1.3. Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.

Proof. Let x be the element of R with minimal norm m. By definition of a Euclidean Domain, there must be some elements q, r in R such that $1 = qx + r$, where $N(r) < N(x)$ or $r = 0$ and 1 is unity. Since x has minimal norm, $r = 0$. Hence, $1 = qx$ and x is a unit. Since the minimal possible norm is always 0, any nonzero element of norm 0 will hence be a unit. □

Problem 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, prove that if a divides bc with nonzero a, b then $\frac{a}{(a,b)}$ divides c.

(b) Consider the Diophantine equation $ax + by = N$ where a, b and N are integers and a, b are nonzero. Suppose x_0, y_0 is a solution: $ax_0 + by_0 = N$. Prove that the full set of solutions to this equation is given by $x = x_0 + m\frac{b}{(a,b)}$, $y = y_0 - m\frac{a}{(a,b)}$ as m ranges over the integers. [If x, y is a solution to $ax + by = N$, show that $a(x - x_0) = b(y_0 - y)$ and use (a).]

Proof. For part a, since $a|bc$, we must have some $q \in R$ such that $qa = bc$. By theorem 4, we have that $xa + yb = 1$ for some $x, y \in R$. Multiplying both sides by c, we get $xac + ybc = xac + yqa = c$. Factoring a from the left, we can see that a divides c $a(xc + yq) = c$.
For part b, if x, y are any solution, then $xa + yb = N = x_0a + y_0b$. Which can be factored as $a(x - x_0) = b(y_0 - y)$. By part a, $\frac{a}{((a,b))}|(y_0 - y)$, meaning there is some m such that $m\frac{a}{((a,b))} = y_0 - y$ which of course means $y = y_0 - m\frac{a}{(a,b)}$. Substituting for y, we find $a(x - x_0) = b(y_0 - y_0 + m\frac{a}{(a,b)}) = \frac{mba}{(a,b)}$ Solving for x, we have $x = x_0 + m\frac{b}{(a,b)}$. Therefore, every solution to the Diophantine equation is of the form $x = x_0 + m\frac{b}{(a,b)}$, $y = y_0 - m\frac{a}{(a,b)}$. □

Problem 2.1. Prove that in a Principle Ideal Domain two ideals (a) and (b) are comaximal if and only if a greatest common divisor of a and b is 1.

Proof. Since we are in a PID, there must be some e in R such that $(e) = (a) + (b)$. Suppose d be the gcd of a and b. Any element of $(a) + (b)$ is also in (d) meaning d generates $(a) + (b)$. Since d is the gcd of a and b, it follows that (d) is the smallest ideal containing $(a) + (b)$. (d) cannot be larger than (e) for this reason. (d) also cannot be smaller than (e), otherwise (e) would contain elements outside of $(a) + (b)$. Therefore, $(d) = (e)$. It is now obvious that $(a) + (b) = R$ if and only if $(d) = 1$. □

Problem 2.2. Prove than any two nonzero elements of a PID have a least common multiple.

Proof. For any a and b in R, having an lcm is equivalent to there being a single element L generating the largest possible ideal contained in both (a) and (b). The intersection of (a) and (b) is the largest possible ideal contained in both (a) and (b). This intersection must have a single generator (L). Therefore, L is the lcm of a and b. □

Problem 2.3. Prove that the quotient of a PID by a prime ideal is again a PID.

Proof. Let R be the PID and P be a prime ideal in R. Let I be an ideal in R/P then $I' = \{r : r + P \in I\}$ is an ideal in R. I' must have a single generator i, in R. Therefore, $I = (i) + P$ and I is a principle ideal. □

Problem 2.4. Let R be an integral domain. Prove that if the following two conditions hold, then R is a PID. (i) any two nonzero elements a and b of R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and (ii) if $a_1, a_2, a_3, ...$ are nonzero elements of R such that $a_{i+2}|a_i$ for all i, then there is a positive integer N such that a_n is a unit for all $n \geq N$.

Proof. Let I be any ideal in R. Let a_1 be any element of I. If a_1 generates I, then I is principle. Otherwise, there must be some b_1 in I, which does not divide a_1. Let a_2 be the gcd of a_1 and b_1. If a_2 generates I, then I is, again, principle. Otherwise, we continue the process to find a sequence of elements $a_1, a_2, a_3, ...$ If this sequence terminates with a generator, I is ideal. Otherwise, since we have $a_{i+2}|a_i$ for all i, there must be some N such that $a_{n \geq N}$ are all units. This would mean that (1) is a generator of I and I is principle. Therefore, must be I principle. □

Problem 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 nonprinciple ideals in R.

(b) Prove that the product of two nonprinciple ideals can be principle 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 principle. Conclude that the principle ideal (6) is the product of four ideals $I_2^2 I_3 I_3'$.

Proof. For (a), the ideals all have relatively prime generators. So, their single element generator would need to be 1. But 1 itself is not contained in any of the ideals. Therefore, none of them are principle.
For (b) The generators for I_1^2 are 4, $2+2\sqrt{-5}$, and $4-2\sqrt{-5}$. These give the term $2(2+2\sqrt{-5})+(4-4\sqrt{-5}) = 2$. So 2 is in I_2^2. Since 2 can generate all the generators, $(2) = I_2^2$.
For c, ... □

Problem 2.6. Let R be an integral domain and suppose that every prime ideal in R is principle. This exercise proves that every ideal of R is principle i.e. R is a PID.

(a) Assume that the set of ideals of R that are not principle is nonempty and prove that this set has a maximal element under inclusion (which by hypothesis is not prime). [Use Zorn's Lemma.]

(b) Let I be an ideal which is maximal with respect to being nonprinciple, 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 $J = \{r \in R | rI_a \subseteq I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principle ideals in R with $I \subsetneqq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$.

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

Proof. Let Σ be the set of all ideals in R that are not principle, and assume for the sake of contradiction that it is nonempty. We can define a binary relation on Σ where for any elements I_a, I_b in Σ, $I_a \leq I_b$ if $I_a \subseteq I_b$. It is clear that this relation is reflexive, anti-symmetric, and transitive. It is therefore a partial order. For any possibly infinite chain $I_0, I_1, ...$ in Σ, the union of every element in the chain $\bigcup_{n=0}^{\infty} I_n$ is also an ideal. This can be seen by letting x be any element of this union and letting r be any element of R. rx is an element of every ideal that x is in, thus it is also an element of $\bigcup_{n=0}^{\infty} I_n$. Note also that if x generates the union, then x generates whatever ideal(s) it is in, which contradicts the ideals being nonprinciple. So, there is no x which generates the union and the union is therefore in Σ. By our partial order, the union is the upper bound of the chain and is in Σ. By Zorn's lemma, Σ has a maximal element on inclusion.

Since I is a subset of I_a and I is the maximal nonprinciple ideal, I_a must be principle and is hence generated

by some α (Note to self, never write a question where a and α represent different variables)
Any element i of I, is in both I and R. So, i^2 is in rI. Hence, i is in J. Since J contains I, J must be principle as well. So, J is also generated by a single element β.
I is obviously a subset of I_b, with $b \notin I$. So, I is a proper subset of I_b.
ba is in I with $b \in R$ and $a \in I_a$. So, b is in J. Since I is also in J, I_b is a subset of J.
Since J is by definition the set of elements that when multiplied by I_a is in I, I_aJ is a subset of I.

Let x be in I, then x is in I_a, and $x = s\alpha$ for some s in R. Since $s\alpha$ is in I, then $sr\alpha = sI_a$ is in I for all r in R. Thus, s is in J. So, $I = I_aJ$ is principle, which contradicts our hypothesis and. Therefore, the set of nonprinciple ideal in R is empty. □

Problem 2.7. An integral domain where every ideal generated by two elements is principle 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 gcd d in R that can be written as an R-linear combination of a and b (ie. $d = xa + yb$ for some x and y in R).

(b) Prove that every finitely generated ideal of a Bezout domain is principle.

(c) Let F be the fraction field of the Bezout domain R. Prove that every element of F can be written in the form a/b where $a, b \in R$ and a and b relatively prime.

Proof. For part a, R is Bezout if and only if for any a and b in R, there exists a d in R such that $(a, b) = (d)$. This implies that d divides both a and b. If there is another element c of R, which divides a and b, then (c) is a subset of (a, b) and is hence a subset of (d) meaning $cx = d$ for some x in R. So d is the gcd of a and b. Since $(d) = (a, b)$, it is obvious that there is some x and y in R such that $ax + by = d$.

For part b, let I be finitely generated. Then $I = (a_1, a_2, ..., a_n)$. We can rewrite this as $(a_1, a_2) \cup (a_3, ..., a_n) = (a_{1,2}) \cup (a_3, ..., a_n) = (a_{1,2}, a_3, ..., a_n)$. By induction, we can continue rewriting the ideal until we have $I = (a_{1,2,...,n})$

For part c, let a and b be in R. From part a, we know a and b have a gcd, d. Now, let $a = a'd$ and $b = b'd$. Then, a/b can be written as a'/b'. If d is one, then a and b are relatively prime, and there is no need to factor the fraction. □

Problem 2.8. Prove that if R is a PID and D is a multiplicatively closed subset of R, then $D^{-1}R$ is a also a PID.

Proof. Let I be an ideal in $D^{-1}R$. Then any element of I will have the form r/d for r in R and d in D. Since d is also in R, $rd/d = r$ is also in I. Hence, I is some ideal in R multiplied by D^{-1} and is thus principle. □

Theorem 14. *Every PID is a UFD. In particular, every Euclidean Domain is a UFD.*

Proof. (I basically copied this proof from DF. I wanted to reword what they wrote because it was a bit confusing the first time through.)

Since every ED is a PID, we only need to prove the first case. Let R be a PID and r be a nonzero element of R, which is not a unit. We wish to show that r is a unique product of elements. If r is irreducible, we are done. Otherwise, r is the product of some r_1r_2. If either factor were a unit, we could divide it out. So we can assume WLG that neither are units. If r_1 is irreducible, we leave it, otherwise we again reduce it to r_11r_22. We can continue reducing r until all factors are irreducible. But we now need to show that this process terminates.

Suppose it does not, then, with some relabeling of terms, and the axiom of choice, we would have $r = r_1x_1...$, $r_1 = r_2x_2$, $r_2 = r_3x_3$, ... on and on, where r_i and x_i are not units for any i. We now have the following chain of ideals, $(r) \subset (r_1) \subset (r_2) \subset ... \subset R$. Where all subsets are proper since r_i and x_i are not units. Consider the union of all ideals in this chain, $I = \cup_{i=1}^{\infty}(r_i)$. As we are in a PID, I must have a single element generator α. But α is in I, meaning it must be in at least one of the (r_i). Therefore, for some N,

$(r_N) = (\alpha) = I$ and for every $n > N$, $r_n = r_N$ contradicting the earlier statement about proper inclusions. Thus, the factorization must terminate.

Now, it remains to show that the factorization is unique. Suppose we have two prime factorizations of r.

$$r = q_1 q_2 ... q_n = p_1 p_2 ... p_m$$

Then q_1 divides the product on the right. By proposition 11, q_1

□

Problem 3.1. Let $G = \mathbb{Q}^x$ be the multaplicative group of rational numbers. If $a = p/q$ with p and q relatively prime, let $\phi : G \to G$ be the function that replaces 2 and 3 in the factorization of a.

(a) Prove that ϕ is a isomorphism.

(b) Prove that there are infinitely many isomorphisms of the group G to itself.

(c) Prove that none of the isomorphisms above can be extended to an isomorphism from the ring $\mathbb{Q}$ to itself. In fact, prove that the identity map is the only isomorphism from $\mathbb{Q}$ to itself.

Proof. For part a, let a and b any elements of G. a and b can be written $a = 2^n 3^m p/q$ and $b = 2^i 3^j l/k$ where p, q, l, and k are not divisible by 2 or 3 and m, n, l, and k are integers.

$$\phi(a)\phi(b) = \phi(2^n 3^m p/q) \cdot \phi(2^i 3^j l/k) = 3^n 2^m p/q \cdot 3^i 2^j l/k = 3^{n+i} 2^{m+k} \frac{pl}{qk} = \phi(2^{n+i} 3^{m+k} \frac{pl}{qk}) = \phi(ab) \quad (1)$$

For part b, instead of swapping 2 and 3, we can create a ϕ_2^p that swaps 2 and any other prime p. Since there are an infinite number of primes, there will be an infinite number of isomorphisms.

For part c, let ϕ_q^p be a function that swaps two primes in the factorization of elements on the ring. If either q or p is 1, the ϕ_q^p is not a ring isomorphism. Otherwise, we have

$$\phi(q) - \phi(1) = p - 1 \neq q - 1 = \phi(q - 1) \quad (2)$$

ϕ is not closed on addition, so it cannot be a ring isomorphism.

For any non identity function $\phi : \mathbb{Q} \to \mathbb{Q}$, if ϕ ... □

Problem 3.2. Let a and b be nonzero elements of the UFD R. Prove that a and b have least common multiple and describe it in terms of their prime factors.

Proof. We can write a and b as $a = u p_1^{n_1} p_2^{n_2} ...$ and $b = v p_1^{m_1} p_2^{m_2} ...$, where $\gcd(u, v) = 1$. Consider $e = uv p_1^{\max(n_1, m_1)} p_2^{\max(n_2, m_2)} ....$ $avq_1 q_2 ... = e$ where $q_i = p_i^{\max(m_i - n_i, 0)}$. So, a divides e. It can be similarly shown that b divides e. Consider some $e' \neq e$ which is also divisible by a and b. We need to show that e' is divisible by e. Suppose e' has less factors than e. Then, there are three cases. e' is not divisible by u, in which case it is not divisible by a, e' is not divisible by v in which case it is not divisible by b, or e' is not divisible by some $p_i^{\max(m_i, n_i)}$ in which case it is not divisible by at lest one of a or b. Thus, any such e' must have more factors than e and is divisible by e. Therefore, e is the lcm of a and b. □

Problem 3.3. Determine all the representations of the integer $2130797 = 17^2 \cdot 73 \cdot 101$ as the sum of two squares.

Proof. pass □