.1 UFDs, PIDs, Euclidean domains

Problem .1.1. Prove Lemma 2.1.

Lemma 2.1. *Let R be a UFD, and let a, b, c be nonzero elements of R. Then*

- $(a) \subseteq (b) \iff$ *the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a;*
- *a and b are associates (that is, $(a) = (b)$) $\iff$ the two multisets coincide;*
- *the irreducible factors of a product bc are the collection of all irreducible factors of b and c.*

Solution. Let M_a denote the multiset containing the irreducible factors of a.

- $(a) \subseteq (b) \iff a = bc \iff a = (q_1^{\alpha_1} \cdots q_r^{\alpha_r})c \iff M_b \subseteq M_a$.
- $(a) = (b) \iff (a) \subseteq (b)$ and $(b) \subseteq (a) \iff M_a \subseteq M_b$ and $M_b \subseteq M_a$. That is, the multisets coincide.
- It is clear from point 1 that the irreducible factors of b and c are contained in the irreducible factors of bc. Now suppose q is an irreducible factor of bc. If q is a factor of b then we are done so suppose not. Then we may factor $bc = bqr$ where r is some collection of units and irreducible factors. Since R is a UFD and in particular an integral domain, we cancel b on both sides and obtain $c = qr$. That is, q is a factor of c. Thus, the irreducible factors of bc are the collection of irreducible factors of b and c.

□

Problem .1.2. Let R be a UFD, and let a, b, c be elements of R such that $a \mid bc$ and $\gcd(a, b) = 1$. Prove that a divides c.

Solution. Since $a \mid bc$, there exists $r \in R$ such that $ar = bc$. By uniqueness, both sides of this equation share the same multiset of irreducible factors. Since $\gcd(a, b) = 1$, a and b share no irreducible factors. Thus, the irreducible factors of a are contained in those of c and we have $a \mid c$. □

Problem .1.3. Let n be a positive integer. Prove that there is a one-to-one correspondence preserving multiplicities between the irreducible factors of n (as an integer) and the composition factors of $\mathbb{Z}/n\mathbb{Z}$ (as a group). (In fact, the Jordan-Hölder theorem may be used to prove that $\mathbb{Z}$ is a UFD.)

Solution. Let d be the largest proper divisor of n and let $G_1 = \mathbb{Z}/d\mathbb{Z}$. Then G/G_1 is simple of cyclic, hence it has prime order. Repeating this process (a finite number of times since n is finite), we obtain a composition series of G,

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1,$$

where G_i/G_{i+1} has prime order. Then

$$n = |G| = |G/G_1||G_1/G_2| \cdots |G_{m-1}/G_{m-2}| = p_1 p_2 \cdots p_{m-1}.$$

Thus, this process produces a composition series whose factors are in bijection with the prime (and irreducible, since we are in $\mathbb{Z}$) factors of n. $\square$

Problem .1.4. Consider the elements x, y in $\mathbb{Z}[x, y]$. Prove that 1 is a gcd of x and y, and yet 1 is *not* a linear combination of x and y. (Cf. Exercise II.2.13.)

Solution. Certainly $(x, y) \subseteq (1) = R$. Now consider d such that $(x, y) \subseteq (d)$. Then $d \mid x$ and $d \mid y$. However, both x and y are irreducible and $(x) \subsetneq (d)$ so the two are not associate. Thus, d is a unit in $\mathbb{Z}[x, y]$ such as 1. However, 1 cannot be written as a linear combination of x and y by comparing degrees. $\square$

Problem .1.5. Let R be the subring of $\mathbb{Z}[t]$ consisting of polynomials with no term of degree 1: $a_0 + a_2 t^2 + \cdots + a_d t^d$.

- Prove that R is indeed a subring of $\mathbb{Z}[t]$, and conclude that R is an integral domain.
- List all common divisors of t^5 and t^6 in R.
- Prove that t^5 and t^6 have no gcd in R.

Solution. Certainly if $f, g \in R$, then $f - g \in R$ since adding polynomials cannot introduce terms of a new degree. We also have

$$fg = (a_0 + a_2 t^2 + \cdots)(b_0 + b_2 t^2 + \cdots) = a_0 b_0 + (a_0 b_2 + a_2 b_0) t^2 + \cdots \in R$$

Thus, R is a subring of $\mathbb{Z}[t]$. A subring of an integral domain is also an integral domain (or else non-zero elements x, y such that $xy = 0$ would also be in the ring). Thus, R is an integral domain.

The common divisors of t^5 and t^6 in R are 1, t^2, and t^3. However, note that $t^6 = t^5 \cdot t$ and $t \notin R$. Suppose $d = \gcd(t^5, t^6)$. Then $t^6 \in (d)$. That is, there is an element a such that $t^6 = t^5 \cdot t = ad$. We may cancel since R is an integral domain to find that $t = bd$ and thus $t \in (d)$, a contradiction. Therefore, t^5 and t^6 have no greatest common divisor. $\square$

Problem .1.6. Let R be a domain with the property that the intersection of any family of principal ideals in R is necessarily a principal ideal.

- Show that greatest common divisors exist in R.
- Show that UFDs satisfy this property.

Solution. Since the intersection is associative, we may consider only two elements $a, b \in R$. Consider their intersection $(a) \cap (b) = (m)$. Then we have $ab = dm$ for some $d \in R$. We claim that $d = \gcd(a, b)$. Indeed, we have $(m) \subseteq (a)$ so $m = a \cdot r$ for some r. Then $ab = dm = dar \Longrightarrow b = dr \Longrightarrow d \mid b$. Similarly, $d \mid a$ so it is a common divisor of both. Now let $c \mid a$ and $c \mid b$. That is, $a = cr_1$ and $b = cr_2$. Then $c \mid ab$, or $ab = cx$ for some x. Rewriting, we have $cr_1 b = cx \Longrightarrow (x) \subseteq (b)$. Similarly, $(x) \subseteq (a)$. Then $(x) \subseteq (a) \cap (b) = (m)$ so $x = ms$ for some s. Finally, we have $dm = ab = cx = c(ms) \Longrightarrow d = cs \Longrightarrow c \mid d$. Thus, d is indeed a gcd for a and b.

Let R be a UFD and consider a family of principal ideals $\{(a_i)\}$. Let $I \bigcap_i (a_i)$ and pick any $r_0 \in I$. If $(r_0) = I$, we are done so suppose not. Then pick $s \in I - (r_0)$. We may then set $r_1 = \gcd(r_0, s)$. The ideal (r_1) is the smallest principal ideal containing (r_0, s), which is a subset of each (a_i) since both generators are chosen from the intersection of these ideals. Thus $(r_1) \subseteq I$ and we have the chain

$$(r_0) \subsetneq (r_0, s) \subseteq (r_1) \subseteq I.$$

This process can be repeated as long as $(r_n) \subsetneq I$. Thus, we form an ascending chain of principal ideals and since R is a UFD, it must stabilize. This occurs when $(r_n) = I$. □

Problem .1.7. Let R be a Noetherian domain, and assume that for all nonzero a, b in R, the greatest common divisors of a and b are linear combinations of a and b. Prove that R is a PID.

Solution. Suppose that R is not a PID and let I be a non-principal ideal. Choose $0 \neq a_0 \in I$. Then $(a_0) \subsetneq I$ so we may choose $b_0 \in I - (a_0)$. We may consider $a_1 = \gcd(a_0, b_0)$. Then we find

$$(a_0) \subsetneq (a_0, b_0) = (a_1) \subsetneq I$$

Repeating this indefinitely yields an ascending chain of ideals which does not stabilize, a contradiction to the assumption that R is Noetherian. Thus, R must be a PID. □

Problem .1.8. Let R be a UFD, and let $I \neq (0)$ be an ideal of R. Prove that every descending chain of principal ideals containing I must stabilize.

Solution. Consider a descending chain of principal ideals containing I

$$(a_1) \supsetneq (a_2) \supsetneq \cdots$$

There is a corresponding ascending chain of multisets of irreducible factors. Let $0 \neq b \in I$. Then $(b) \subseteq (a_i)$ for all (a_i) in the ascending chain. Letting M_b denote the multiset of irreducible factors of b, we have that each multiset in the corresponding ascending chain is contained in M_b. If the chain does not stabilize, then eventually the multiset of irreducible factors for say a_n will have greater size than M_b, a contradiction. Therefore the descending chain of principal ideals must stabilize. □

Problem .1.9. The *height* of a prime ideal P in a ring R is (if finite) the maximum length h of a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_h = P$ in R. (Thus, the Krull dimension of R, if finite, is the maximum height of a prime ideal in R.) Prove that if R is a UFD, then every prime ideal of height 1 in R is principal.

Solution. First note that (0) is prime in R since R is an integral domain. Thus, the chain of ideals looks like

$$(0) \subsetneq P.$$

Since P is non-empty, there is some non-zero element $a \in P$. Consider the factorization of a into irreducibles. Since P is prime, one of these elements belongs to P, say p. Since R is a UFD, irreducible elements are prime so (p) is a prime ideal. But then we have

$$(0) \subsetneq (p) \subseteq P.$$

Since P has height one, it must be the case that $(p) = P$, so P is principal. □

Problem .1.10. It is a consequence of a theorem known as *Krull's Hauptidealsatz* that every nonzero, nonunit element in a Noetherian domain is contained in a prime ideal of height 1. Assuming this, prove a converse to Exercise 2.9, and conclude that a Noetherian domain R is a UFD if and only if every prime ideal of height 1 in R is principal.

Solution. Suppose R is a Noetherian domain such that every prime ideal of height 1 is principal. Since R is Noetherian, the a.c.c. holds for all ideals, and principal ideals in particular. Therefore, we only need to show that irreducible elements are prime. Let q be an irreducible element of R. By Krull's Hauptidealsatz, q is contained in some prime ideal of height 1, say (p). Then we have $q = pa$ for some unit a. Thus, $(p) = (q)$ and (q) is prime, implying that q is a prime element. Since every irreducible element is prime, R is a UFD. □

Problem .1.11. Let R be a PID, and let I be a nonzero ideal of R. Show that R/I is an artinian ring (cf. Exercise 1.10), by proving explicitly that the d.c.c. holds in R/I.

Solution. Since R is a PID, let $I = (a)$. Consider a descending chain of ideals in R/I

$$\frac{I_0}{I} \supsetneq \frac{I_1}{I} \supsetneq \frac{I_2}{I} \supsetneq \cdots$$

This corresponds to a descending chain of ideals containing I in R. Since R is a PID, it is also a UFD and by Exercise 2.8, a descending chain of principal ideals containing a non-zero ideal must stabilize. Thus, this descending chain in R stabilizes and so does the one in R/I. $\square$

Problem .1.12. Prove that if $R[x]$ is a PID, then R is a field.

Solution. Consider the ideal (x). By Exercise 2.11, the quotient $R[x]/(x)$ is artinian. Furthermore, R is an integral domain (since $R[x]$ is) and by Exercise 1.10, an artinian integral domain is a field. $\square$

Problem .1.13. For a, b, c positive integers with $c > 1$, prove that $c^a - 1$ divides $c^b - 1$ if and only if $a \mid b$. Prove that $x^a - 1$ divides $x^b - 1$ in $\mathbb{Z}[x]$ if and only if $a \mid b$. (Hint: For the interesting implications, write $b = ad + r$ with $0 \le r < a$, and take 'size' into account.)

Solution. Since $\mathbb{Z}$ is a Euclidean domain, we may write $b = ad + r$ with $0 \le r < a$. Then we have

$$x^b - 1 = x^b - x^r + x^r - 1 = x^r \left(x^{ad} - 1\right) + x^r - 1$$

Furthermore, note that

$$x^{ad} - 1 = (x^a - 1)\left(x^{a(d-1)} + x^{a(d-2)} + \cdots + 1\right)$$

Then $x^a - 1$ divides the right side of the first equation if and only if $r = 0$, if and only if a divides b. The first statement is a direct implication by setting $x = c$. $\square$

Problem .1.14. Prove that if k is a field, then $k[[x]]$ is a Euclidean domain.

Solution. Define a valuation on $k[[x]] \setminus \{0\}$, setting $v(f)$ to be the degree of the smallest term of f with non-zero coefficient. Indeed, given power series f, g, we write

$$f = qg + r.$$

This is possible since k is a field. If $v(g) > v(f)$ then let $q = 0$ and set $r = f$ so that $v(r) < v(g)$. If $v(g) = v(f)$, then define q such that the first non-zero term of qg equals that of f. Then define r such that the remaining terms are equivalent and we have $v(r) < v(g)$. Similarly, if $v(g) < v(f)$, define q such that the first $v(f) - v(g)$ terms of qg are equal to those of f (possible since k is a field). Then $v(r) < v(g)$. Thus, this is indeed a Euclidean valuation. $\square$

Problem .1.15. Prove that if R is a Euclidean domain, then R admits a Euclidean valuation $\bar{v}$ such that $\bar{v}(ab) \geq \bar{v}(b)$ for all nonzero $a, b \in R$. (Hint: Since R is a Euclidean domain, it admits a valuation v as in Definition 2.7. For $a \neq 0$, let $\bar{v}(a)$ be the minimum of all $v(ab)$ as $b \in R, b \neq 0$. To see that R is a Euclidean domain with respect to $\bar{v}$ as well, let a, b be nonzero in R, with $b \nmid a$; choose q, r so that $a = bq + r$, with $v(r)$ minimal; assume that $\bar{v}(r) \geq \bar{v}(b)$, and get a contradiction.)

Solution. Define $\bar{v}$ as above; that is, set $\bar{v}(a) = \min\{v(ab) \mid b \in R, b \neq 0\}$. Clearly, $\bar{v}$ satisfies the property that $\bar{v}(ab) \geq \bar{v}(b)$. Let $a, b \in R$ be non-zero and $b \nmid a$. Write $a = bq + r$ with minimal $v(r)$. Suppose that $\bar{v}(r) \geq \bar{v}(b)$. That is, there exists $c \in R$ such that for all $x \in R$, $v(rx) \geq v(bc)$. In particular, for $x = c$, we have $v(rc) \geq v(bc)$. However, multiplying the initial equation by c yields $ac = bcq + rc$ where $v(rc) < v(bc)$, a contradiction. Thus, $\bar{v}$ is a Euclidean valuation. $\square$

Problem .1.16. Let R be a Euclidean domain with Euclidean valuation v; assume that $v(ab) \geq v(b)$ for all nonzero $a, b \in R$ (cf. Exercise 2.15). Prove that associate elements have the same valuation and that units have minimum valuation.

Solution. Let a and b be associates. That is, we can write $a = ub$ for some unit u. Then we have $v(a) = v(ub) \geq v(b)$. Furthermore, we have $b = u^{-1}a$ so $v(b) = v(u^{-1}a) \geq v(a)$. Thus, $v(a) = v(b)$.

Now consider a unit u. For all $r \in R$, we have $r = ru^{-1}u$. This implies that $v(u) \leq v(r)$ so units have minimum valuation. $\square$

Problem .1.17. Let R be a Euclidean domain that is not a field. Prove that there exists a nonzero, nonunit element c in R such that $\forall a \in R, \exists q, r \in R$ with $a = qc + r$ and either $r = 0$ or r a unit.

Solution. The existence of a nonzero, nonunit element c is guaranteed since R is not a field. Choose such a c with minimal valuation. Let $a \in R$ and choose q, r such that $a = qc + r$. If $r = 0$ then we are done so suppose not. We have $v(r) < v(c)$. If r is not a unit, then a contradiction arises as we chose c to have minimal valuation. Thus r must be a unit. $\square$

Problem .1.18. For an integer d, denote by $\mathbb{Q}(\sqrt{d})$ the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\sqrt{d}$, with norm N defined as in Exercise III.4.10. See Exercise 1.17 for the case $d = -5$; in this problem, you will take $d = -19$.

Let $\delta = (1 + i\sqrt{19})/2$, and consider the following subring of $\mathbb{Q}(\sqrt{-19})$:

$$\mathbb{Z}[\delta] := \left\{ a + b\frac{1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\}.$$

- Prove that the smallest values of $N(z)$ for $z = a + b\delta \in \mathbb{Z}[\delta]$ are 0, 1, 4, 5. Prove that $N(a + b\delta) \geq 5$ if $b \neq 0$.
- Prove that the units in $\mathbb{Z}[\delta]$ are ± 1.
- If $c \in \mathbb{Z}[\delta]$ satisfies the condition specified in Exercise 2.17, prove that c must divide 2 or 3 in $\mathbb{Z}[\delta]$, and conclude that $c = \pm 2$ or $c = \pm 3$.
- Now show that $\nexists q \in \mathbb{Z}[\delta]$ such that $\delta = qc + r$ with $c = \pm 2, \pm 3$ and $r = 0, \pm 1$.

Conclude that $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is not a Euclidean domain.

Solution. Certainly $N(z)$ takes on those values for values $(0, 0)$, $(\pm 1, 0)$, $(\pm 2, 0)$, and $(0, \pm 1)$. To prove these are minimal, let $|a| > 2$. Then

$$N(a + b\delta) \geq N(a) = a^2 > 4 = N(\pm 2).$$

Furthermore, if $b \neq 0$ then

$$N(a + b\delta) \geq N(b\delta) = \frac{b^2}{4} + 19 \cdot \frac{b^2}{4} = 5b^2 \geq 5$$

Clearly two units in $\mathbb{Z}[\delta]$ are ± 1. Now let u be a unit. Then $N(u) = 1$. By Point 1, we have $u = \pm 1$.

If $c \in \mathbb{Z}[\delta]$ satisfies the condition from the previous problem then we have $2 = q_1 c + r_1$ and $3 = q_2 c + r_2$. If $r_1 = 0$ then $c \mid 2$. If $r_1 \neq 0$ then $r_1 = \pm 1$. If $r_1 = 1$ then $2 = q_1 c + 1 \implies q_1 c = 1$, contradicting that c is not a unit. If $r_1 = -1$, then we have

$$q_2 c + r_2 = 3 = 2 + 1 = q_1 c - 1 + 1 = q_1 c$$

so $c \mid 3$. Given the condition and point 1, it must be the case that $c = \pm 2$ or $c = \pm 3$.

Now suppose there exists $q = a + b\delta \in \mathbb{Z}[\delta]$ such that $\delta = qc + r$ with $c = \pm 2, \pm 3$ and $r = 0, \pm 1$. If $r = 0$, then we have $N(q)N(c) = N(qc) = N(\delta) = 5$. Since 5 is prime and $N(c) = 4$ or 9 respectively, q cannot exist. Similarly, if $r = 1$, then we have $N(q)N(c) = N(qc) = N(\delta - 1) = 5$ and the same contradiction arises. If $r = -1$, then $N(qc) = 7$, another contradiction. Thus, there can be no such q and $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is not a Euclidean domain. $\square$

Problem .1.19. A *discrete valuation* on a field k is a surjective homomorphism of abelian groups $v : (k^*, \cdot) \to (\mathbb{Z}, +)$ such that $v(a+b) \geq \min(v(a), v(b))$ for all $a, b \in k^*$ such that $a + b \in k^*$.

- Prove that the set $R := \{a \in k^* \mid v(a) \geq 0\} \cup \{0\}$ is a subring of k.
- Prove that R is a Euclidean domain.

Rings arising in this fashion are called *discrete valuation rings*, abbreviated DVR. They arise naturally in number theory and algebraic geometry. Note that the Krull dimension of a DVR is 1 (Example III.4.14); in algebraic geometry, DVRs correspond to particularly nice points on a 'curve'.

- Prove that the ring of rational numbers a/b with b *not* divisible by a fixed prime integer p is a DVR.

Solution. To show that R is a subring, first note that it is a subgroup under addition. Indeed, for nonzero $a, b \in R$ we have

$$v(a-b) \geq \min(v(a), v(-b)).$$

Note that $v(-b) = v(-1 \cdot b) = v(-1) + v(b)$ where -1 is the additive inverse of 1. Furthermore,

$$v(-1) + v(-1) = v(-1 \cdot -1) = v(1) = 0$$

implies that $v(-1) = 0$. Thus, we have $v(-b) = v(b)$ so $v(a-b) \geq \min(v(a), v(-b)) \geq 0$, meaning $a - b \in R$.

To show that R is closed under multiplication, see that $v(ab) = v(a) + v(b)$. Since both $v(a)$ and $v(b)$ are non-negative, so is their sum. Therefore, $ab \in R$ and R is a ring.

To prove that R is a Euclidean domain, we must show that v is a Euclidean valuation which we do by cases. Let $a, b \in R$ be nonzero. If $v(a) \geq v(b)$, then we have $v(a/b) = v(a) - v(b) \geq 0$ so $a/b \in R$. Therefore we can write $a = (a/b)b + 0$. If $v(a) < v(b)$, then we have $a = 0b + a$. Thus, in any case we can choose $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $v(r) < v(b)$.

Consider the ring R of rational numbers a/b with b not divisible by a fixed prime integer p. We should define a discrete valuation, that is a group homomorphism to $\mathbb{Z}$, on the field $\mathbb{Q}$ so that the resulting ring arises in the manner defined above. Given a rational number a/b such that a fixed prime $p \nmid b$, we can use the unique factorization of $\mathbb{Z}$ to write

$$\frac{a}{b} = \frac{p^k z}{b}$$

for integers k, z such that $p \nmid z$. Then define $v(a/b) = k$. To verify that v is a discrete valuation, we first show that it is a homomorphism of groups. Indeed, if $x, y \in \mathbb{Q}^*$, then

$$v(xy) = v\left(\frac{a_1 a_2}{b_1 b_2}\right) = v\left(\frac{p^{k_1} z_1 p^{k_2} z_2}{b_1 b_2}\right) = v\left(\frac{p^{k_1+k_2} z_1 z_2}{b_1 b_2}\right) = k_1 + k_2 = v(x) + v(y)$$

Thus, v is a group homomorphism. Furthermore, we find that

$$v(x+y) = v\left(\frac{a_1b_2 + a_2b_1}{b_1b_2}\right) = v\left(\frac{p^{k_1}z_1b_2 + p^{k_2}z_2b_1}{b_1b_2}\right)$$

WLOG, we may assume $k_1 \leq k_2$. Then

$$v\left(\frac{p^{k_1}z_1b_2 + p^{k_2}z_2b_1}{b_1b_2}\right) = v\left(p^{k_1}\frac{z_1b_2 + p^{k_2-k_1}z_2b_1}{b_1b_2}\right) = k_1 \geq \min(v(x), v(y))$$

Therefore, v is a discrete valuation and the resulting ring is in fact the one defined above. I did not formulate this valuation myself and I don't see how it's at all a natural definition but it works out. □

Problem .1.20. As seen in Exercise 2.19, DVRs are Euclidean domains. In particular, they must be PIDs. Check this directly, as follows. Let R be a DVR, and let $t \in R$ be an element such that $v(t) = 1$. Prove that if $I \subseteq R$ is any nonzero ideal, then $I = (t^k)$ for some $k \geq 1$. (The element t is called a 'local parameter' of R.)

Solution. Let $a \in I$ be a nonzero element with minimal valuation $v(a) = n$. Then for all nonzero $b \in I$, we have

$$v(b/a) = v(b) - v(a) \geq 0 \implies b/a \in R \implies b \in (a).$$

Although this is sufficient, we can go on to show that if $v(a) = v(b)$ then $(a) = (b)$. Indeed, we find

$$v(a/b) = v(b/a) = 0 \implies b \mid a \text{ and } a \mid b \implies (a) = (b)$$

For a local parameter t, we have $v(t^k) = k$ so for an element $a \in I$ with minimal valuation n, we have $I = (t^n)$. □

Problem .1.21. Prove that an integral domain is a PID if and only if it admits a Dedekind-Hasse valuation. (Hint: For the $\Longleftarrow$ implication, adapt the argument in Proposition 2.8; for $\Longrightarrow$, let $v(a)$ be the size of the multiset of irreducible factors of a.)

Solution. First suppose that R is an integral domain admitting a Dedekind-Hasse valuation. Let I be an ideal of R. If I is zero then it is clearly principal so suppose not. Then choose $0 \neq b \in I$ to have minimal valuation. For all $a \in I$, we either have $(a, b) \in (b)$ or there exists $q, r, s \in R$ such that $as = bq + r$ with $v(r) < v(b)$. In the first case, $a \in (b)$. In the latter case, $r = as - bq \in I$. By choice of b, we cannot have $v(r) < v(b)$. Thus, $r = 0$ and $a \in (b)$. Therefore, $I = (b)$ so R is a PID.

Now suppose that R is a PID. We must show that it admits a Dedekind-Hasse valuation. Define $v : R \to \mathbb{Z}^{\geq 0}$ to send $v(a)$ to the size of the multiset of irreducible factors of a (recall that a PID is a UFD). To verify that this is a Dedekind-Hasse valuation, let $a, b \in R$. We have $(a, b) = (d)$ for some $d \in R$. In particular, $d \mid b$ so $v(d) \leq v(b)$. If $v(d) = v(b)$, then $(b) = (d)$ by considering the size of multisets of irreducible factors so we have $(a, b) = (b)$ and $b \mid a$. If $v(d) < v(b)$, we can write

$$-d = as + bq \Longrightarrow as = bq + d$$

for $q, s \in R$. Thus, v is indeed a Dedekind-Hasse valuation. □

Problem .1.22. Suppose $R \subseteq S$ is an inclusion of integral domains, and assume that R is a PID. Let $a, b \in R$ and let $d \in R$ be a gcd for a and b in R. Prove that d is also a gcd for a and b in S.

Solution. Since R is a PID, we have $(a, b) = (d)$. That is, there exist $x, y \in R$ such that $ax + by = d$. Now let $c \in S$ such that $c \mid a$ and $c \mid b$. Then $c \mid ax + by = d$. Thus, d is a gcd for a and b in S as well. □

Problem .1.23. Compute $d = \gcd(5504227617645696, 2922476045110123)$. Further, find a, b such that $d = 5504227617645696a + 2922476045110123b$.

Solution. A brief application of the extended Euclidean algorithm shows that $d = 234982394879$. Furthermore, we have $a = 1055$ and $b = -1987$. □

Problem .1.24. Prove that there are infinitely many prime integers. (Hint: Assume by contradiction that $p_1, \ldots, p_N$ is a complete list of all positive prime integers. What can you say about $p_1 \cdot \cdots \cdot p_N + 1$? This argument was already known to Euclid, more than 2,000 years ago.)

Solution. Let $P = p_1 \cdot \cdots \cdot p_N + 1$. By assumption, P is not prime so it is divisible by some prime in our list, say p_i. But then we have $p \mid P - p_1 \cdot \cdots \cdot p_N = 1$, a contradiction. Therefore the list of primes is not complete. □

Problem .1.25. Variation on the theme of Euclid from Exercise 2.24: Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial such that $f(0) = 1$. Prove that infinitely many primes divide the numbers $f(n)$, as n ranges in $\mathbb{Z}$. (If $p_1, \ldots, p_n$ were a complete list of primes dividing the numbers $f(n)$, what could you say about $f(p_1 \cdots p_N x)$?)

Once you are happy with this, show that the hypothesis $f(0) = 1$ is unnecessary. (If $f(0) = a \neq 0$, consider $f(p_1 \cdots p_N a x)$. Finally note that there is nothing special about 0.)

Solution. First note that the requirement $f(0) = 1$ implies that the constant term of the polynomial is 1. Suppose there were a complete list of primes dividing the values of $f(n)$. Let $P = p_1 \cdots p_N$ and consider $f(Px)$. We find

$$f(Px) = 1 + a_1(Px) + a_2(Px)^2 + \cdots + a_n(Px)^n$$

In particular, for $x = 1$, we have p_i divides the left side. But p_i also divides P and so it divides the difference

$$p_i \mid f(Px) - (a_1Px + a_2(Px)^2 + \cdots + a_n(Px)^n) = 1,$$

a contradiction.

An entirely analogous proof works for $f(0) = a \neq 0$ and considering the product $f(Pax)$. The case $f(0) = 0$ is trivial since all primes p divide $f(p)$. $\square$