Chapter I

Irreducibility and factorization in integral domains

I.1 Chain conditions and existence of factorizations

Problem I.1.1. Let R be a Noetherian ring, and let I be an ideal of R. Prove that R/I is a Noetherian ring.

Solution. There is a surjective homomorphism $\varphi : R \to R/I$. By Exercise III.4.2, R/I is also Noetherian. In particular, we have an exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

and by Proposition III.6.7, R is Noetherian if and only if both I and R/I are Noetherian. □

Problem I.1.2. Prove that if $R[x]$ is Noetherian, so is R. (This is a 'converse' to Hilbert's basis theorem.)

Solution. Consider the ideal $I = (x)$. By Exercise 1, $R[x]/(x) \cong R$ is also Noetherian. One may also consider an arbitrary ideal I in R and realize that $I[x]$ is an ideal in $R[x]$. Since $I[x]$ is finitely generated, the coefficients in I are also finitely generated; hence, I is finitely generated and R is Noetherian. □

Problem I.1.3. Let k be a field, and let $f \in k[x], f \notin k$. For every subring R of $k[x]$ containing k and f, define a homomorphism $\varphi : k[t] \to R$ by extending the identity on k and mapping t to f. This makes every such R a $k[t]$-algebra. (Example III.5.6).

- Prove that $k[x]$ is finitely generated as a $k[t]$-module.
- Prove that every subring R as above is finitely generated as a $k[t]$-module.
- Prove that every subring of $k[x]$ containing k is a Noetherian ring.

Solution. If $\deg(f) = n$, then $k[x]$ is generated as a $k[t]$-module by the set $\{1, x, x^2, \dots, x^{n-1}\}$. Clearly any element $g(x) \in k[x]$ with degree $< n$ is generated by the set of generators given. If $\deg(g) = n$, then it is generated by 1 since it can have coefficient f. Thus, we can consider the case where $\deg(g) > n$. Using the division theorem, we can write $g(x) = p(x) \cdot f(x) + r(x)$ where $\deg(r) < n$. Thus, r is generated by the set. Since $\deg(f) > 0$, it must be the case that $\deg(p) < deg(g)$. If $\deg(p) \leq n$, it is finitely generated. Otherwise, we may repeat use of the division algorithm until it is. Thus, every element of $k[x]$ can be written as a linear combination of elements in the generating set. Therefore, $k[x]$ is a finitely generated $k[t]$-module.

Recall that if k is a field then $k[t]$ is a PID; that is, every ideal can be generated by a single element. Since $k[x]$ is finitely generated as a $k[t]$-module, $k[x]$ is also Noetherian. Any subring R containing k and f is a submodule of $k[x]$. Then R is finitely generated.

Certainly any subring R is Noetherian as a $k[t]$-module. Therefore, it is also a finite type $k[t]$-algebra and hence isomorphic to a quotient of $k[t]$. Since $k[t]$ is a Noetherian ring, by Hilbert's Basis Theorem so is any quotient of $k[t]$. That is, R is a Noetherian ring. $\square$

Problem I.1.4. Let R be the ring of real-valued continuous functions on the interval $[0, 1]$. Prove that R is not Noetherian.

Solution. Consider the ideal $I_{[a,b]} = \{f \in R \mid f([a, b]) = 0\}$. This is indeed an ideal because for $f, g \in I_{[a,b]}$, we have $(f + g)([a, b]) = f([a, b]) + g([a, b]) = 0$, so $f + g \in I_{[a,b]}$. Furthermore, if $h \in R$, then $(h \cdot f)([a, b]) = h([a, b]) \cdot f([a, b]) = h \cdot 0 = 0$ so $h \cdot f \in I_{[a,b]}$, proving that $I_{[a,b]}$ is an ideal.

Now notice that if $[c, d] \subset [a, b]$, then $I_{[c,d]} \subset I_{[a,b]}$. Since there are uncountably many inclusive subsets, there is an associated chain of ideals that never stabilizes. Thus, R is not Noetherian. $\square$

Problem I.1.5. Determine for which sets S the power set ring $\mathscr{P}(S)$ is Noetherian. (Cf. Exercise III.3.16.)

Solution. Recall that the power set ring is defined with the following operations:

$$A + B = (A \cup B) \setminus (A \cap B), \quad A \cdot B = A \cap B.$$

By Exercise III.3.16, if $T \subset S$, then the subsets of T form an ideal of $\mathscr{P}(S)$ and for finite S, every ideal is of this form. These ideals are finitely generated. Simply take the one element subsets of T and add them to form the other subsets (this works because the set difference is empty). Thus, $\mathscr{P}(S)$ is Noetherian for finite S. I believe for any infinite set S, the ring is not Noetherian since we can construct an ideal whose elements are all finite subsets of S. Such an ideal doesn't have any clear finite basis. □

Problem I.1.6. Let I be an ideal of $R[x]$, and let $A \subseteq R$ be the set defined in the proof of Theorem 1.2. Prove that A is an ideal of R.

Solution. The set is defined as follows:

$$A = \{0\} \cup \{a \in R \mid a \text{ is a leading coefficient of an element of } I\}$$

Certainly the set is nonempty. To see it is a subgroup, let $a, b \in A$. That is, there are polynomials f, g whose leading terms are ax^m and bx^n respectively. WLOG assume that $m < n$. Then consider $h = x^{n-m} \cdot f \in I$. The leading term of this polynomial is ax^n. Then $g - h$ has leading term $(a - b)x^n$ so $a - b \in A$ and A is an additive subgroup.

Given $r \in R$, the polynomial $r \cdot f \in I$ and it has leading term rax^m. Thus, $ra \in A$ so A is an ideal of R. □

Problem I.1.7. Prove that if R is a Noetherian ring, then the ring of power series $R[[x]]$ (cf. §III.1.3) is also Noetherian. (Hint: The order of a power series $\sum_{i=0}^{\infty} a_i x^i$ is the smallest i for which $a_i \neq 0$; the *dominant coefficient* is then a_i. Let $A_i \subseteq R$ be the set of dominant coefficients of series of order i in I, together with 0. Prove that A_i is an ideal of R and $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$. This sequence stabilizes since R is Noetherian, and each A_i is finitely generated for the same reason. Now adapt the proof of Lemma 1.3)

Solution. Let I be an ideal of $R[[x]]$. Define the ideal A_i of R as follows:

$$A_i = \{0\} \cup \{a_i \mid a_i \text{ is a dominant coefficient of an order 0 power series in } I\}$$

We can verify that A_i is an ideal since the power series corresponding to elements $a, b \in A_i$ can be subtracted to yield another power series in I whose dominant coefficient is $a - b$. Similarly, multiplying a power series by some element of R yields another power series in I whose leading term is ra, hence $ra \in A_i$.

Note that $A_i \subseteq A_{i+1}$. Indeed, if $a_i \in A_i$, then there is a power series $f(x) = \sum_{k=i}^{\infty} a_k x^k$. Then the power series $f(x) \cdot x = \sum_{k=i}^{\infty} a_k x^{k+1}$ has order $i + 1$ and dominant coefficient a_i, so $a_i \in A_{i+1}$. Furthermore, each A_i is finitely generated since R is Noetherian and the ascending chain $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$ stabilizes for some n.

Now consider the sets S_i which are finite sets of power series of order i whose dominant coefficients generate A_i. Certainly there are only finitely many such sets since the ascending chain stabilizes as shown above. We claim that the union $S = \bigcup S_i$ generates I. Indeed, given a power series f, the terms of degree $\leq n$ are killed off by elements in S. Terms of degree $> n$ require an infinite series of the form $\sum_{k=n+1}^{\infty} r_k x^{k-n}$ to be killed off. However, this is not an issue as the series is in the ring $R[[x]]$. Thus, the ideal I is finitely generated by S. $\square$

Problem I.1.8. Prove that every ideal in a Noetherian ring R contains a finite product of prime ideals. (Hint: Let $\mathscr{F}$ be the family of ideals that do not contain finite products of prime ideals. If $\mathscr{F}$ is nonempty, it has a maximal element M since R is Noetherian. Since $M \in \mathscr{F}$, M is not itself prime, so $\exists a, b \in R$ s.t. $a \notin M, b \notin M$, yet $ab \in M$. What's wrong with this?)

Solution. Consider such a family $\mathscr{F}$ and a maximal element M. The ideals $M + (a)$ and $M + (b)$ are both strictly larger than M. Since M does not contain a finite product of prime ideals, neither does $M + (a)$. Thus, $M + (a) \in \mathscr{F}$, contradicting the maximality of M. $\square$

Problem I.1.9. Let R be a commutative ring, and let $I \subseteq R$ be a proper ideal. The reader will prove in Exercise 3.12 that the set of prime ideals containing I has minimal elements (the *minimal primes* of I). Prove that if R is Noetherian, then the set of minimal primes of I is finite. (Hint: Let $\mathscr{F}$ be the family of ideals that do *not* have finitely many minimal primes. If $\mathscr{F} \neq \emptyset$, note that $\mathscr{F}$ must have a maximal element I, and I is not prime itself. Find ideals J_1, J_2 strictly larger than I, such that $J_1 J_2 \subseteq I$, and deduce a contradiction.)

Solution. Consider such a family $\mathscr{F}$ and maximal element I. Certainly I is not prime itself so there exists elements $a, b \notin I$ such that $ab \in I$. Consider the ideals $J_1 = I + (a), J_2 = I + (b)$, both of which are strictly larger than I. Both of these are proper. Indeed, if $I + (b) = R$, then we would have $(a)I + (a)(b) = (a)$. However, $(a)I + (a)(b) \subseteq I$, contradicting the fact that $a \notin I$. Thus, we have $J_1 J_2 \subseteq I$. Any prime ideal containing I also contains either J_1 or J_2. That is, any prime minimal over I is also minimal over J_1 or J_2. But J_1 and J_2 only have finitely many primes by the maximality of I, a contradiction. $\square$

Problem I.1.10. By Proposition 1.1, a ring R is Noetherian if and only if it satisfies the a.c.c. for ideals. A ring is *Artinian* if it satisfies the d.c.c (descending chain condition) for ideals. Prove that if R is Artinian and $I \subseteq R$ is an ideal, then R/I is Artinian. Prove that if R is an Artinian integral domain, then it is a field. (Hint: Let $r \in R, r \neq 0$. The ideals (r^n) form a descending sequence; hence $(r^n) = (r^{n+1})$ for some n. Therefore....) Prove that Artinian rings have Krull dimension 0 (that is, prime ideals are maximal in Artinian rings).

Solution. Ideals of R/I are ideals of R containing I. Therefore, a chain of ideals in R/I is of the form $I_1/I \supseteq I_2/I \supseteq I_3/I \supseteq \cdots$. This corresponds to a descending chain of ideals in R, namely $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ which stabilizes since R is Artinian. That is, there is some n such that $I_n = I_{n+1} = \cdots$. Then $I_n/I = I_{n+1}/I = \cdots$ so the descending chain in R/I also stabilizes. Thus, R/I is Artinian.

Let R be an Artinian integral domain and consider the descending chain $(r) \supseteq (r^2) \supseteq (r^3) \supseteq \cdots$ which stabilizes for some n. That is, there is some n for which $(r^n) = (r^{n+1})$. Then there exists $s \in R$ such that $r^n = r^{n+1}s$. Since R is an integral domain, cancellation applies and we can write $1 = rs$. Thus r is a unit and hence R is a field.

Recall that an ideal I is prime if and only if R/I is an integral domain. If R is Artinian and I is a prime ideal, then R/I is an Artinian integral domain and hence a field. An ideal I is maximal if and only if R/I is a field. Thus, I is maximal in R. Since all prime ideals are maximal, the longest chain of prime ideals has length 0. Thus, the Krull dimension of an Artinian ring is 0. $\square$

Problem I.1.11. Prove that the 'associate' relation is an equivalence relation.

Solution. Say $a \sim b$ if a is associate with b. Certainly $(a) = (a)$ so $a \sim a$ and the relation is reflexive. If $a \sim b$ then $(a) = (b)$. Then $(b) = (a)$ so $b \sim a$ and the relation is symmetric. Finally, if $a \sim b$ and $b \sim c$, then $(a) = (b) = (c)$ so $a \sim c$ and the relation is transitive. Thus the associate relation is an equivalence relation. $\square$

Problem I.1.12. Let R be an integral domain. Prove that $a \in R$ is irreducible if and only if (a) is maximal among proper principal ideals of R.

Solution. Suppose a is irreducible. Consider the principal ideals of R. Suppose there exists b such that $(a) \subseteq (b)$. That is, there exists $c \in R$ such that $a = bc$. Since a is irreducible, either b or c is a unit. WLOG, suppose b is a unit (the proof is analogous for the ideal (c). Then there is an element $b^{-1} \in R$ such that $bb^{-1} = 1$. In particular, $1 \in (b)$ so $(b) = R$. Thus, (a) is maximal among principal ideals.

Now suppose that (a) is maximal among principal ideals of R. That is, if $(a) \subseteq (b)$ then either $(a) = (b)$ or $(b) = R$. If $(a) = (b)$ then a and b are associates and $a = ub$ for some unit u by Lemma 1.5. If $(b) = R$ then $1 \in (b)$ and there exists some element $c \in R$ such that $1 = bc$. Thus b is a unit and $a = bd$ for some d (by the assumption that $(a) \subseteq (b)$. In either case, a is irreducible. $\square$

Problem I.1.13. Prove that prime $\iff$ irreducible in $\mathbb{Z}$.

Solution. Suppose p is prime and that $p = ab$. Certainly $p \mid ab$ so $p \mid a$ or $p \mid b$. WLOG, assume $p \mid a$. We can write $a = pc$ for some c. That is, $a = abc$ so $1 = bc$. Thus, b is a unit and p is irreducible.

Now suppose that p is irreducible and that $p \mid ab$ but $p \nmid a$. Let $g = \gcd(p, a)$. Then $g \mid p$ and by the irreducibility of p, g is a unit. The only units of $\mathbb{Z}$ are 1 and -1 but just assume that $g = 1$ for the sake of simplicity. By Bezout's Theorem, there exist x, y such that $ax + py = 1$. Then $abx + bpy = b$, and since p divides the left side we also have $p \mid b$. Therefore, p is prime. $\square$

Problem I.1.14. For a, b in a commutative ring R, prove that the class of a in $R/(b)$ is prime if and only if the class of b in $R/(a)$ is prime.

Solution. Denote the class of a as $\bar{a}$. Suppose that $\bar{a}$ is prime in $R/(b)$. That is, the ideal $(\bar{a})$ is prime. Then the quotient $(R/(b))/(\bar{a})$ is an integral domain. However, recall that

$$\frac{R/(b)}{(\bar{a})} \cong \frac{R}{(a, b)} \cong \frac{R/(a)}{(\bar{b})}$$

Thus, $(R/(a))/(\bar{b})$ is also an integral domain so $\bar{b}$ is prime in $R/(a)$. $\square$

Problem I.1.15. Identify $S = \mathbb{Z}[x_1, \ldots, x_n]$ in the natural way with a subring of the polynomial ring in countably infinitely many variables $R = \mathbb{Z}[x_1, x_2, x_3, \ldots]$. Prove that if $f \in S$ and $(f) \subseteq (g)$ in R, then $g \in S$ as well. Conclude that the ascending chain condition for principal ideals holds in R, and hence R is a domain with factorizations.

Solution. If $(f) \subseteq (g)$, then there is a polynomial $h \in R$ such that $f = gh$. Suppose g involves m variables. Then $m \leq n$. Indeed, if $m > n$, there would be some variable x_m in g which vanishes when multiplied by h. However, $\mathbb{Z}$ is an integral domain so this only occurs if $h = 0$, in which case $f = 0$. Thus, g is a polynomial in fewer degrees than f so it can be identified in S by setting all coefficients of $x_{m+1}, x_{m+2}, \ldots, x_n$ to 0. The ascending chain condition for principal ideals holds in S since it is Noetherian by Hilbert's basis theorem. Therefore, it also holds in R since, given any element $f \in R$, the ascending chain $(f) \subseteq (f_1) \subseteq (f_2) \subseteq \cdots$ stabilizes in S. Thus, R is a domain with factorizations. $\square$

Problem I.1.16. Let

$$R = \frac{\mathbb{Z}[x_1, x_2, x_3, \ldots]}{(x_1 - x_2^2, x_2 - x_3^2, \ldots)}.$$

Does the ascending chain condition for principal ideals hold in R?

Solution. By construction, we have $x_n = x_{n+1}^2$ so $(x_n) \subseteq (x_{n+1})$. To show that the inclusion is strict, suppose that $x_{n+1} \in (x_n)$. Then there is some polynomial $p \in R$ such that $p \cdot x_{n+1} = x_n$ or $x_{n+1}(p \cdot x_{n+1} - 1) = 0$, so we simply show that R is an integral domain.

Let $a, b \in R$ be nonzero. Using the relations in the ideal, we can write $a = p(x_n)$ and $b = q(x_n)$ for nonzero polynomials p, q. Then $ab = p(x_n)q(x_n) \neq 0$ since $\mathbb{Z}[x_n] \cap (x_1 - x_2^2, \cdots) = 0$ inside $\mathbb{Z}[x_1, x_2, \cdots]$.

Therefore, R is an integral domain and the equation $x_{n+1}(p \cdot x_{n+1} - 1) = 0$ implies that $p \cdot x_{n+1} = 1$, or x_{n+1} is a unit. But units are preserved by homomorphisms and evaluating at $x_n = 0$ yields $0 = 1$ in $\mathbb{Z}$, a contradiction. Thus, we have $x_{n+1} \notin (x_n)$ so we can construct an ascending chain $(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$ which never stabilizes since there are countably infinite variables. □

Problem I.1.17. Consider the subring of $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{-5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}.$$

- Prove that this ring is isomorphic to $\mathbb{Z}[t]/(t^2 + 5)$.
- Prove that it is a Noetherian integral domain.
- Define a 'norm' N on $\mathbb{Z}[\sqrt{-5}]$ by setting $N(a + bi\sqrt{5}) = a^2 + 5b^2$. Prove that $N(zw) = N(z)N(w)$. (Cf. Exercise III.4.10.)
- Prove that the units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. (Use the preceding point.)
- Prove that $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ are all irreducible nonassociate elements of $\mathbb{Z}[\sqrt{-5}]$.
- Prove that no element listed in the preceding point is prime. (Prove that the rings obtained by modding out the ideals generated by these elements are not integral domains.)
- Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Solution. Consider the evaluation homomorphism $\varphi : \mathbb{Z}[t] \to \mathbb{Z}[\sqrt{-5}]$ sending $f(t) \mapsto f(i\sqrt{5})$. Clearly the homomorphism is surjective since $a + bi\sqrt{5}$ is mapped to by $f(t) = a + bt \in \mathbb{Z}[t]$. Thus, we have

$$\frac{\mathbb{Z}[t]}{\ker(\varphi)} \cong \mathbb{Z}[\sqrt{-5}]$$

By definition, $t^2 + 5 \in \ker(\varphi)$ so certainly $(t^2 + 5) \subseteq \ker(\varphi)$. Now let $f \in \ker(\varphi)$. By polynomial division, $f(t) = (t^2 + 5)g(t) + r(t)$ for some $g(t), r(t) \in \mathbb{Z}[t]$ where $\deg(r) < 2$. If $f(\sqrt{-5}) = 0$, then $r(\sqrt{-5}) = 0$, but r has degree at most one and integer coefficients. Thus, $r(t) = 0$ and $f(t) \in (t^2 + 5)$. That is, $\ker(\varphi) = (t^2 + 5)$ and $\mathbb{Z}[t]/(t^2 + 5) \cong \mathbb{Z}[\sqrt{-5}]$.

Since $\mathbb{Z}$ is Noetherian, by Hilbert's basis theorem, $\mathbb{Z}[t]$ is also Noetherian. Exercise 1 shows that quotients of Noetherian rings are Noetherian so $\mathbb{Z}[t]/(t^2+5) \cong \mathbb{Z}[\sqrt{-5}]$ is Noetherian. Furthermore, $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$, a field. Thus, it has no non-trivial zero divisors and is an integral domain.

Let $z = a + bi\sqrt{5}$ and $w = c + di\sqrt{5}$. Then

$$\begin{aligned}
N(zw) &= N((ac - 5bd) + (ad + bc)i\sqrt{5}) \\
&= (ac - 5bd)^2 + 5(ad + bc)^2 \\
&= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2 \\
&= (a^2 + 5b^2)(c^2 + 5d^2) \\
&= N(z)N(w)
\end{aligned}$$

Suppose that z is a unit. That is, there is an element w such that $zw = 1$. Note that N is a ring homomorphism from $\mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$. Thus, we have $1 = N(1) = N(zw) = N(z)N(w)$ so $N(z)$ is a unit in $\mathbb{Z}$. However, the only units of $\mathbb{Z}$ are ± 1. Then we have $N(z) = a^2 + 5b^2 = 1$ (we can ignore -1 since all terms are positive). Since $5 > 1$, it must be the case that $b = 0$. Then the only remaining choices are $a = \pm 1$. That is, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

It is easy to see that all of $2, 3, 1 + i\sqrt{5}, 1 - \sqrt{5}$ are irreducible. Indeed, suppose $z = w_1 w_2$. Then $N(z) = N(w_1)N(w_2)$. Notice that for each element listed, $N(z)$ is prime in $\mathbb{Z}$. Thus, if $N(z) \mid N(w_1)$, then $N(w_2) = \pm 1$ (since prime $\iff$ irreducible in $\mathbb{Z}$). Then $w_2 = \pm 1$ in $\mathbb{Z}[\sqrt{-5}]$ so z is irreducible. Since we have shown that $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, associate elements are unit multiples of one another. However, we have shown that the only units are ± 1 and clearly none of the listed elements are unit multiplies of each other. Therefore, none of them are associate.

I'll show that 2 is not prime, the rest follow somewhat similarly. First note that $\mathbb{Z}[\sqrt{-5}]/(2) = \mathbb{Z}_2[\sqrt{-5}]$. Then we have that $(1 + i\sqrt{5})^2 = 1 + 2i\sqrt{5} - 5 = 0$. Thus, $\mathbb{Z}_2[\sqrt{-5}]$ is not an integral domain so 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Simply note that $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Since none of these factors are associates, the factorization of 6 is not unique. Hence, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. $\square$

I.2 UFDs, PIDs, Euclidean domains

Problem I.2.1. 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 I.2.2. 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 I.2.3. 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. □

Problem I.2.4. 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. □

Problem I.2.5. 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. □

Problem I.2.6. 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 $ab = dm = dar \implies b = dr \implies d \mid b$. 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 $cr_1 b = cx \implies (x) \subseteq (b)$. Similarly, $(x) \subseteq (a)$. Then $(x) \subseteq (a) \cap (b) = (m)$ so

$x = ms$ for some s. Finally, we have $dm = ab = cx = c(ms) \implies d = cs \implies c \mid d$. 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 $(r_n) = I$. $\square$

Problem I.2.7. 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. $\square$

Problem I.2.8. 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. $\square$

Problem I.2.9. 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. $\square$

Problem I.2.10. 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. $\square$

Problem I.2.11. 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 I.2.12. 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 I.2.13. 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 $0 \leq r < a$, and take 'size' into account.)

Solution. Since $\mathbb{Z}$ is a Euclidean domain, we may write $b = ad+r$ with $0 \leq r < a$. 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 I.2.14. 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 I.2.15. 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. □

Problem I.2.16. 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. □

Problem I.2.17. 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. □

Problem I.2.18. 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 I.2.19. 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

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

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

$$v\left(\frac{p^{k_1} z_1 b_2 + p^{k_2} z_2 b_1}{b_1 b_2}\right) = v\left(p^{k_1} \frac{z_1 b_2 + p^{k_2 - k_1} z_2 b_1}{b_1 b_2}\right) = k_1 \geq \min(v(x), v(y))$$

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. $\square$

Problem I.2.20. 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

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

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

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

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 I.2.21. 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 I.2.22. 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. $\square$

Problem I.2.23. 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 $b=-1987$. $\square$

Problem I.2.24. 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. $\square$

Problem I.2.25. 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 $f(p_1\cdots p_N ax)$. 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 $f(p)$. $\square$

I.3 Intermezzo: Zorn's lemma

Problem I.3.1. Prove that every well-ordering is total.

Solution. Recall that a well-ordering on Z is an order relation such that every nonempty subset of Z has a least element. For any two elements $a, b \in Z$, consider the subset $\{a, b\} \subseteq Z$. Since this subset has a least element, it must be the case that either $a \preceq b$ or $b \preceq a$. As this holds for any pair of elements in Z, it follows that $\preceq$ is total on Z. □

Problem I.3.2. Prove that a totally ordered set $(Z, \preceq)$ is a woset if and only if every descending chain

$$z_1 \succeq z_2 \succeq z_3 \succeq \cdots$$

in Z stabilizes.

Solution. Suppose every such descending chain stabilizes. Let $S \subseteq Z$ be a nonempty subset. Since Z is totally ordered, the elements of S form a descending chain as described above. Then there is some element a such that for all $b \in Z$, $a \preceq b$. That is, a is a least element in S. Then Z is well-ordered.

Now suppose Z is a woset. Assume there is a descending chain which does not stabilize. Then the set formed by these elements does not have a minimum element, a contradiction. Therefore, every descending chain in Z stabilizes. □

Problem I.3.3. Prove that the axiom of choice is equivalent to the statement that a set-function is surjective if and only if it has a right-inverse (cf. Exercise I.2.2).

Solution. The proof of the statement about surjective set-functions assumes the axiom of choice, showing that it is sufficient. To see that it is necessary, assume that every surjective set-function has a right-inverse. Let A be a set of disjoint nonempty sets and $B = \bigcup A$. Then for each $b \in B$, there exists exactly one set $X \in A$ such that $b \in X$. Thus, we have a surjective function $f : B \to A$. Then it has a right-inverse g. Define $C := \{g(X) \mid X \in A\}$. Then C is a choice set. □

Problem I.3.4. Construct explicitly a well-ordering on $\mathbb{Z}$. Explain why you know that $\mathbb{Q}$ can be well-ordered, even without performing an explicit construction.

Solution. The well-ordering on $\mathbb{N}$, namely $\leq$, does not work because of the negative numbers so we work around this by imposing conditions. Let $a, b \in \mathbb{Z}$ and set $a \preceq b$ if and only if one of the following holds:

- $|a| < |b|$.
- $|a| = |b|$ and $a \leq b$.

This well ordering yields the following visualization: $0, -1, 1, -2, 2, \ldots$ Assuming the Well-ordering Theorem, every set admits a well-ordering, including $\mathbb{Q}$. Without directly invoking the theorem, we also know that $\mathbb{Q}$ is a countable set and thus is in bijection with $\mathbb{N}$, which has a well-ordering. $\square$

Problem I.3.5. Prove that the (ordinary) principle of induction is equivalent to the statement that $\leq$ is a well-ordering on $\mathbb{Z}^{>0}$. (To prove by induction that $(\mathbb{Z}^{>0}, \leq)$ is well-ordered, assume it is known that 1 is the least element of $\mathbb{Z}^{>0}$ and that $\forall n \in \mathbb{Z}^{>0}$ there are no integers between n and $n+1$.)

Solution. In Claim 3.2, it was shown that the principle of induction holds for any well-ordered set. That is, $\leq$ being a well-ordering on $\mathbb{Z}^{>0}$ implies that the principle of induction holds. To show the converse, we can assume that 1 is the least element of $\mathbb{Z}^{>0}$ and that there are no integers between n and $n+1$ for all $n \in \mathbb{Z}$. Suppose that there exist a non-empty subset S of $\mathbb{Z}^{>0}$ such that S has no minimum element. Then $1 \notin S$ or else it would be a minimal element. Similarly, $2 \notin S$ because there are no integers between 1 and 2, which would make 1 a minimal element. If none of $1, 2, \ldots, n$ are in S, then $n+1 \notin S$ or it would be minimal. Thus, the principle of induction implies that S is empty, a contradiction. Therefore, S must have a minimal element so $\leq$ is a well-ordering on $\mathbb{Z}^{>0}$. $\square$

Problem I.3.6. In this exercise assume the truth of Zorn's lemma and the conventional set-theoretic constructions; you will be proving the well-ordering theorem.

Let Z be a nonempty set, and let $\mathscr{Z}$ be the set of pairs $(S, \leq)$ consisting of a subset S of Z and of a *well-ordering* $\leq$ on S. Note that $\mathscr{Z}$ is not empty (singletons can be well-ordered). Define a relation $\preceq$ on $\mathscr{Z}$ by prescribing

$$(S, \leq) \preceq (T, \leq')$$

if and only if $S \subseteq T, \leq$ is the restriction of $\leq'$ to S, and every element of S precedes every element of $T \setminus S$ w.r.t. $\leq'$.

- Prove that $\preceq$ is an order relation in $\mathscr{Z}$.
- Prove that every chain in $\mathscr{Z}$ has an upper bound in $\mathscr{Z}$.
- Use Zorn's lemma to obtain a maximal element $(M, \leq)$ in $\mathscr{Z}$. Prove that $M = Z$.

Thus every set admits a well-ordering, as stated in Theorem 3.3.

Solution. Recall that an order relation is reflexive, transitive, and antisymmetric. Given a pair $(S, \leq)$, certainly we have $S \subseteq S$ and every element of S precedes every element of $S \setminus S = \emptyset$ with respect to $\leq$. Therefore, $\preceq$ is reflexive. Let $(T, \leq'), (R, \leq'') \in \mathscr{Z}$ such that $(S, \leq) \preceq (T, \leq')$ and $(T, \leq') \preceq (R, \leq'')$. Then $S \subseteq R$ (by transitivity of subsets) and $\leq$ is the restriction of $\leq'$ to S, which is the restriction of $\leq''$ to S. Furthermore, $S \subseteq T$ and every element of T precedes every element of $R \setminus T$ w.r.t. $\leq''$. In particular, every element of S precedes the elements of $R \setminus T$ w.r.t. $\leq''$. Thus, we have $(S, \leq) \preceq (R, \leq'')$, proving transitivity. Finally, suppose we have $(S, \leq) \preceq (T, \leq')$ and $(T, \leq') \preceq (S, \leq)$. Then $S \subseteq T$ and $T \subseteq S$ so $S = T$. To show the two order relations are equivalent, let $a, b \in S$ such that $a \leq b$. Since $\leq$ is the restriction of $\leq'$, we have $a \leq' b$. Similarly, we find $a \leq' b \Longrightarrow a \leq b$. Thus, the two order relations are equivalent and we find $(S, \leq) = (T, \leq')$, proving antisymmetry and showing that $\preceq$ is in fact an order relation on $\mathscr{Z}$.

Now consider a chain $\mathscr{C}$ of subsets. We must show it has an upper bound in $\mathscr{Z}$. Consider the set

$$U := \bigcup_{S \in \mathscr{C}} S.$$

Certainly each $S \subseteq U$. Furthermore, there is a natural order relation on U since for all $a, b \in U$, there exists some $S \in \mathscr{C}$ containing both a and b. Then the order relation on S has $a \leq b$ which also holds in U. Thus, U is well-ordered and is an upper bound for $\mathscr{C}$.

Since every chain has an upper bound, Zorn's lemma states that there is a maximal element $(M, \leq)$ in $\mathscr{Z}$. Clearly $M \subseteq Z$. To show that $M = Z$, suppose otherwise. That is, suppose there is some element $x_0 \in Z \setminus M$. Then consider the set $M \cup \{x_0\}$ with the order relation $\leq'$ such that for all $x \in M$, $x \leq' x_0$. Then $(M, \leq) \preceq (M \cup \{x_0\}, \leq')$, contradicting the maximality of M. Thus, $M = Z$ so Z has a well-ordering. $\square$

Problem I.3.7. In this exercise assume the truth of the axiom of choice and the conventional set-theoretic constructions; you will be proving the well-ordering theorem.

Let Z be a nonempty set. Use the axiom of choice to choose an element $\gamma(S) \notin S$ for each proper subset $S \subsetneq Z$. Call a pair $(S, \leq)$ a γ-*woset* if $S \subseteq Z$, $\leq$ is a well-ordering on S, and for every $a \in S$, $a = \gamma(\{b \in S, b < a\})$.

- Show how to begin constructing a γ-woset, and show that all γ-wosets must begin in the same way.

Define an ordering on γ-wosets by prescribing that $(U, \leq'') \preceq (T, \leq')$ if and only if $U \subseteq T$ and $\leq''$ is the restriction of $\leq'$.

- Prove that if $(U, \leq'') \prec (T, \leq')$, then $\gamma(U) \in T$.
- For two γ-wosets $(S, \leq)$ and $(T, \leq')$, prove that there is a maximal γ-woset $(U, \leq'')$ preceding both w.r.t. $\preceq$. (Note: There is no need to use Zorn's lemma!)

- Prove that the maximal γ-woset found in the previous point in fact equals $(S, \leq)$ or $(T, \leq')$. Thus, $\preceq$ is a total ordering.
- Prove that there is a maximal γ-woset $(M, \leq)$ w.r.t. $\preceq$. (Again, Zorn's lemma need not and should not be invoked.)
- Prove that $M = Z$.

Thus every set admits a well-ordering, as stated in Theorem 3.3.

Solution. Given $\gamma(S)$, one can begin constructing a γ-woset $(S, \leq)$ by including $\gamma(\emptyset)$. In some sense, $a = \gamma(\emptyset)$ is minimal in S since no elements precede it. Furthermore, since every γ-woset is well-ordered, they all have a minimal element. That is, they all contain $\gamma(\emptyset)$. One can continue the construction of the γ-woset by letting the next element be γ of the elements currently in the set. The well-ordering on the set follows naturally.

Now suppose we have $(U, \leq'') \prec (T, \leq')$. By the definition of $\prec$, we have $U \subset T$. Since T is well-ordered, there is some minimum element a such that for all $b \in U$, $b <' a$. Then $a = \gamma(\{b \in S, b <' a\}) = \gamma(U)$.

Given two γ-wosets $(S, \leq)$ and $(T, \leq')$, consider the set $R = S \cap T$ with the obvious well ordering. Indeed, since $R \subseteq S$ and $R \subseteq T$, R precedes both w.r.t. $\preceq$. Furthermore, if there were any more elements then it would not satisfy the defining property of being a subset of both S and T so it is maximal.

If $R = S$, then there is nothing to prove so suppose otherwise. Then $R \prec S$ so $\gamma(R) = a \in S$ for some s. If $R \prec T$ then $\gamma(R) = b \in T$ for some b. But then $a = b \in S \cap T = R$, a contradiction (since $\gamma(R) \notin R$). Thus, $R = S$ or $R = T$ and $\preceq$ is a total ordering.

Since $\preceq$ is a total ordering, we can construct a chain of γ-wosets. Let M be the union of these γ-wosets with the ordering inherited from the wosets. Certainly each γ-woset $S \subseteq M$ so M is maximal.

Finally, we know $M \subseteq Z$. Suppose $Z \subsetneq M$. Then there exists some element $x \in Z \setminus M$. Consider $M \cup \{x\}$. Since $\gamma(\{x\})$ is defined, this set is a γ-woset properly containing M, contradicting the maximality of M. Thus, $M = Z$ so there is a well-ordering on Z. $\square$

Problem I.3.8. Prove that every nontrivial finitely generated group has a maximal proper subgroup. Prove that $(\mathbb{Q}, +)$ has no maximal proper subgroup.

Solution. Let $\mathscr{S}$ be the set of all proper subgroups of a finitely generated group G. Then $\mathscr{S}$ is partially ordered by inclusion so let $\mathscr{C}$ be a chain in this poset. Let H be the union of all subgroups in this chain. Since the chain is nonempty, there is one subgroup K_0 containing the identity, so H contains the identity. Furthermore, suppose $x, y \in H$. Then there are subgroups K_1, K_2 with $x \in K_1$, $y \in K_2$. Suppose WLOG that $K_1 \subseteq K_2$. Then both $x, y \in K_2$ and since K_2 is a subgroup, $xy^{-1} \in K_2 \subseteq H$. Thus H is a subgroup.

To show H is a proper subgroup, suppose otherwise. In particular, H contains the generators $g_1, g_2, \dots, g_n$ of G. Then there is some subgroup K_n containing all such generators, implying that $K_n = G$, a contradiction. Thus, H must be proper.

Since every chain in $\mathscr{S}$ has an upper bound in $\mathscr{S}$, Zorn's lemma applies and $\mathscr{S}$ has a maximal element. That is, G has a maximal proper subgroup.

Suppose that $(\mathbb{Q}, +)$ has a maximal proper subgroup H. Then the quotient $\mathbb{Q}/H$ is simple and abelian, so it must be cyclic with prime order. Say $\mathbb{Q}/H \cong \mathbb{Z}/p\mathbb{Z}$. Choose $x \in \mathbb{Q} \setminus H$. Then $H = p(\frac{x}{p} + H) = x + N$, implying that $x \in N$, a contradiction. Thus, $\mathbb{Q}$ has no maximal proper subgroup. $\square$

Problem I.3.9. Consider the rng (= ring without 1; cf. §III.1.1) consisting of the abelian group $(\mathbb{Q}, +)$ endowed with the trivial multiplication $qr = 0$ for all $q, r \in \mathbb{Q}$. Prove that this rng has no maximal ideals.

Solution. Suppose the ring R has a maximal ideal M. Then M is also a maximal subgroup of $\mathbb{Q}$ (a larger subgroup would also act as an ideal). As shown above, $\mathbb{Q}$ does not contain maximal subgroups so neither can M be a maximal ideal. $\square$

Problem I.3.10. As shown in Exercise III.4.17, every maximal ideal in the ring of continuous real-valued functions on a *compact* topological space K consists of the functions vanishing of a point of K.

Prove that there are maximal ideals in the ring of continuous real-value functions on the *real line* that do not correspond to points of the real line in the same fashion. (Hint: Produce a proper ideal that is not contained in any maximal ideal corresponding to a point, and apply Proposition 3.5.)

Solution. I still don't know topology but I imagine the solution uses something about the fact that the real line is not compact (whatever that means). $\square$

Problem I.3.11. Prove that a UFD R is a PID if and only if every nonzero prime ideal in R is maximal. (Hint: One direction is Proposition III.4.13. For the other, assume that every nonzero prime ideal in a UFD R is maximal, and prove that every maximal ideal in R is principal; then use Proposition 3.5 to relate arbitrary ideals to maximal ideals, and prove that every ideal of R is principal.)

Solution. First suppose that R is a PID and let $I = (a)$ be a nonzero prime ideal. Assume $I \subseteq J$ for an ideal $J = (b)$ of R. Since $a \in (b)$, we have $a = bc$ for some $c \in R$. But since a is prime, we have $b \in (a)$ or $c \in (a)$. In the first case, there is nothing more to prove. In the second, we have $c = da$. Then

$$a = bda \Longrightarrow bd = 1 \Longrightarrow (b) = (1) = R.$$

Thus, I is maximal.

Now let R be a UFD such that every prime ideal is maximal. Let I be a maximal ideal. Then I is also a prime ideal of height 1. By Exercise 2.9, I is principal. Thus, every maximal ideal is principal. Now let I_0 be an arbitrary ideal. It is contained in some maximal ideal $\mathfrak{m}_0 = (a_0)$. In particular, every element admits a factor of a, which is irreducible (by Exercise 1.12). Then we may write $I = a_0 J_0$ for an ideal J_0. If $J_0 = R$ then $I = (a_0)$ and we are done. Otherwise, J_0 is properly contained in a maximal ideal $\mathfrak{m}_1 = (a_1)$ so we may write $J_0 = a_1 J_1$. We may repeat this and it will terminate since the elements of I only have finitely many irreducible factors. When it terminates, we find that $J_t = R$ so $I = (a_0 a_1 \cdots a_t)$. □

Problem I.3.12. Let R be a commutative ring, and let $I \subseteq R$ be a proper ideal. Prove that the set of prime ideals containing I has minimal elements. (These are the *minimal primes* of I.)

Solution. Consider the set $\mathscr{I}$ of prime ideals of R which contain I. The set is ordered by inclusion so consider a chain $\mathscr{C}$ and let $\mathfrak{B}$ be the intersection of the prime ideals in $\mathscr{C}$. Certainly $I \subseteq \mathfrak{B}$. Now we must check that $\mathfrak{B}$ is in fact prime. Suppose $ab \in \mathfrak{B}$ but neither a nor b is. Then there exist two prime ideals $\mathfrak{p}, \mathfrak{p}'$ such that $a \notin \mathfrak{p}, b \notin \mathfrak{p}'$ and WLOG $\mathfrak{p} \subseteq \mathfrak{p}'$. Then $a, b \notin \mathfrak{p}$ but $ab \in \mathfrak{p}$, contradicting that $\mathfrak{p}$ is prime. Thus, $\mathfrak{B}$ is prime. Since every chain in $\mathscr{I}$ has a lower bound, $\mathscr{I}$ has a minimal element. □

Problem I.3.13. Let R be a commutative ring, and let N be its nilradical (Exercise III.3.12). Let $r \notin N$.

- Consider the family $\mathscr{F}$ of ideals of R that do not contain any power r^k of r for $k > 0$. Prove that $\mathscr{F}$ has maximal elements.
- Let I be a maximal element of $\mathscr{F}$. Prove that I is prime.
- Conclude $r \notin N \implies r$ is not in the intersection of all prime ideals of R.

Together with Exercise III.4.18, this shows that the nilradical of a commutative ring R equals the intersection of all prime ideals of R.

Solution. Recall that the nilradical of a ring is the set of nilpotent elements (elements a such that $a^n = 0$ for some n). The nilradical is an ideal of R.

The family $\mathscr{F}$ of ideals not containing any power of r^k is ordered by inclusion. Each chain in this family has a maximal element, namely the union of all of the ideals in the chain. Therefore, by Zorn's lemma $\mathscr{F}$ has maximal elements.

Let I be a maximal element of $\mathscr{F}$ and suppose $ab \in I$ but $a, b \notin I$. Then the ideals $I + (a)$ and $I + (b)$ both properly contain I. By the maximality of I, we have $r^m \in I + (a)$ and $r^n \in I + (b)$. But then we find

$$r^{m+n} = (s_1 + ax)(s_2 + by) = s_1 s_2 + s_1 \cdot by + ax \cdot s_2 + ax \cdot by \in I$$

for $s_1, s_2 \in I$, a contradiction. Thus one of $a, b \in I$ so I is prime.

Suppose r is not in the nilradical of R. Then there is some prime ideal not containing any power of r, so r is not in the intersection of all prime ideals. In particular, $\bigcap \mathfrak{p} \subseteq N$. $\square$

Problem I.3.14. The *Jacobson radical* of a commutative ring R is the intersection of the maximal ideals in R. (Thus, the Jacobson radical contains the nilradical.) Prove that r is in the Jacobson radical if and only if $1 + rs$ is invertible for every $s \in R$.

Solution. If r is in the Jacobson radical, then it is in every maximal ideal. Suppose there exists some $s \in R$ such that $1 + rs$ is not invertible. Then $(1 + rs)$ is a proper ideal and hence is contained in a maximal ideal $\mathfrak{m}$. But $r \in \mathfrak{m}$ so $1 = rs - r \cdot s \in \mathfrak{m}$, a contradiction. Thus $1 + rs$ is invertible for all $s \in R$.

Now suppose that $1 + rs$ is invertible for all $s \in R$ and let $\mathfrak{m}$ be a maximal ideal. If $r \notin \mathfrak{m}$ then $\mathfrak{m} + (r) = R$ so there exists $y \in \mathfrak{m}$ and $s \in (r)$ such that $rs + y = 1$. But then $y = 1 - rs$ is invertible so $1 = yy^{-1} \in \mathfrak{m}$, a contradiction. Thus, $r \in \mathfrak{m}$. $\square$

Problem I.3.15. Recall that a (commutative) ring R is Noetherian if every ideal of R is finitely generated. Assume the seemingly weaker condition that every *prime* ideal of R is finitely generated. Let $\mathscr{F}$ be the family of ideals that are not finitely generated in R. You will prove $\mathscr{F} = \emptyset$.

- If $\mathscr{F} \neq 0$, prove that it has a maximal element I.
- Prove that R/I is Noetherian.
- Prove that there are ideals J_1, J_2 properly containing I, such that $J_1 J_2 \subseteq I$.
- Give a structure of R/I module to I/J_1J_2 and J_1/J_1J_2.
- Prove that I/J_1J_2 is a finitely generated R/I-module.
- Prove that I is finitely generated, thereby reaching a contradiction.

Thus, a ring is Noetherian if and only if its *prime* ideals are finitely generated.

Solution. If $\mathscr{F}$ is nonempty, it is partially ordered by inclusion. For each chain $\mathscr{C}$ in $\mathscr{F}$, the ideal defined as the union of ideals in the chain is an upper bound for $\mathscr{C}$. Indeed, if it were finitely generated then the generating set would be contained in one of the ideals, contradicting the assumption that ideals in $\mathscr{F}$ are not finitely generated. By Zorn's lemma, $\mathscr{F}$ has maximal elements. Let I be one such maximal element.

Suppose R/I is not Noetherian. That is, there is some ideal of the form J/I which is not finitely generated. Then J is an ideal of R containing I and it is not finitely generated. But by the maximality of I, we have $J = R$ which is finitely generated by 1, a contradiction. Thus R/I is Noetherian.

Since I is not finitely generated, it is not prime. Thus, there exist elements $a, b \notin I$ with $ab \in I$. Then $J_1 = I + (a)$ and $J_2 = I + (b)$ both properly contain I (and thus are finitely generated) and elements of $J_1 J_2$ are of the form

$$(r_1 + ax)(r_2 + by) = r_1 \cdot r_2 + r_1 \cdot by + r_2 \cdot ax + ab \cdot xy \in I,$$

so $J_1 J_2 \subseteq I$.

We can give the quotient $I/J_1 J_2$ the structure of an R/I module by defining

$$(r + I)x = rx$$

for $r \in R$ and $x \in I/J_1 J_2$. Indeed, since $x = a + J_1 J_2$ for $a \in I$, we find

$$r(a + J_1 J_2) = ra + rJ_1 J_2 \in \frac{I}{J_1 J_2}$$

The other module axioms can be checked easily. We can define the same structure on $J_1/J_1 J_2$.

Recall that J_1 is finitely generated. Then $J_1/J_1 J_2$ is also finitely generated over R and hence over R/I. Since R/I is Noetherian and $I/J_1 J_2$ is a submodule of $J_1/J_1 J_2$, we find that $I/J_1 J_2$ is finitely generated.

Finally, observe that $J_1 J_2 \subseteq I$ is finitely generated and $I/J_1 J_2$ is finitely generated. Thus, I is finitely generated and we arrive at a contradiction. Therefore, a ring is Noetherian if and only if its prime ideals are finitely generated. □

I.4 Unique factorization in polynomial rings

Problem I.4.1. Prove Lemma 4.1.

Lemma 4.1. *Let R be a ring, and let I be an ideal of R. Then*

$$\frac{R[x]}{IR[x]} \cong \frac{R}{I}[x].$$

Solution. The map from $R \to R/I$ induces a map from $R[x]$ to $R/I[x]$ which sends the coefficients of each polynomial to their coset. Clearly this map is surjective. Its kernel is the set of polynomials whose coefficients are in I. That is, the kernel is $IR[x]$. The isomorphism follows. □

Problem I.4.2. Let R be a ring, and let I be an ideal of R. Prove or disprove that if I is maximal in R, then $IR[x]$ is maximal in $R[x]$.

Solution. If I is maximal in R, then R/I is a field. By Lemma 4.1, the ring $R[x]/IR[x]$ is a polynomial ring over a field, or a PID. In particular, the polynomial $f(x) = x$ has no inverse so the ring is not a field and $IR[x]$ is not maximal in $R[x]$. It is, however, prime in $R[x]$ which is interesting in its own right. $\square$

Problem I.4.3. Let R be a PID, and let $f \in R[x]$. Prove that f is primitive if and only if it is very primitive. Prove that this is not necessarily the case in an arbitrary UFD.

Solution. If f is primitive, then for all principal prime ideals $\mathfrak{p}$, $f \notin \mathfrak{p}R[x]$. Since R is a PID, every prime ideal is principal. Thus, f is very primitive. The other direction follows from the definition.

For a counterexample in the more general case, consider the UFD $\mathbb{Z}[x]$ (note that we are only told this in §5.2 but we haven't proven it yet). Let $f = x + y \in \mathbb{Z}[x][y]$. Then f is primitive because $\gcd(x, y) = 1$ but $1 \notin (x, y)$ so $(x, y) \neq (1)$. In general, $d = \gcd(a_0, \ldots, a_d)$ does not imply that $(d) = (a_0, \ldots, a_d)$. $\square$

Problem I.4.4. Let R be a commutative ring, and let $f, g \in R[x]$. Prove that

$$fg \text{ is very primitive } \iff \text{ both } f \text{ and } g \text{ are very primitive.}$$

Solution. Suppose fg is very primitive. Then for all prime ideals $\mathfrak{p}$ in R, $fg \notin \mathfrak{p}R[x]$. That is, $f \notin \mathfrak{p}R[x]$ and $g \notin \mathfrak{p}R[x]$, or f is very primitive and g is very primitive. An equivalent reasoning proves the reverse direction. $\square$

Problem I.4.5. Prove Lemma 4.7.

Lemma 4.7. *Let R be a UFD, and let $f \in R[x]$. Then*

- $(f) = (\mathrm{cont}_f)(\underline{f})$*, where* $\underline{f}$ *is primitive;*
- *if* $(f) = (c)(g)$*, with* $c \in R$ *and* g *primitive, then* $(c) = (\mathrm{cont}_f)$*.*

Solution. Recall that cont_f is the gcd of the coefficients of f. Let $\underline{f}$ be the polynomial obtained by dividing each coefficient of f by cont_f. Then $(\mathrm{cont}_{\underline{f}}) = (1)$ since the remaining coefficients have no common factors. Thus, $\underline{f}$ is primitive and $(f) = (\mathrm{cont}_f)(\underline{f})$.

For the second point, note that we have $f = ucg$ for some unit $u \in R$. Then $\mathrm{cont}_f = \mathrm{cont}_{ucg} = uc$ since g is primitive. But then $(c) = (uc) = (\mathrm{cont}_f)$. $\square$

Problem I.4.6. Let R be a PID, and let K be its field of fractions.

- Prove that every element $c \in K$ can be written as a finite sum

$$c = \sum_i \frac{a_i}{p_i^{r_i}}$$

where the p_i are nonassociate irreducible elements in R, $r_i \geq 0$, and a_i, p_i are relatively prime.

- If $\sum_i \frac{a_i}{p_i^{r_i}} = \sum_j \frac{b_j}{q_j^{s_j}}$ are two such expressions, prove that (up to reshuffling) $p_i = q_i$, $r_i = s_i$, and $a_i \equiv b_i \mod p_i^{r_i}$.

- Relate this to the process of integration by 'partial fractions' you learned about when you took calculus.

Solution. Since R is a PID, it is in particular a UFD. Consider an element $c = \frac{x}{y}$. Then y has a unique factorization into non-associate irreducible elements (the p_i). Then we can write

$$\frac{x}{y} = \sum_i \frac{a_i}{p_i^{r_i}}$$

where the sum is guaranteed to have the same denominator by the way in which addition is defined in the field of fractions. To determine the a_i, note that expanding the sum on the right side yields a numerator whose terms are relatively prime. Thus, their gcd is a unit and since R is a PID, Bezout's identity holds. That is, there is a set of elements $a_1, \dots, a_n$ which satisfy the equation $u = a_1x_1 + \cdots + a_nx_n$ where x_i is y divided by the i-th irreducible factor and u is some unit. Multiplying both sides by $u^{-1}x$ yields a set of a_i which satisfy the equation above. Furthermore, they must be relatively prime to their corresponding p_i or the product with x_i would simply yield y.

With regards to the second point, I don't know that the expressions are always equivalent if the unique factorization of y is multiplied by a unit. However, the process described is precisely what occurs in partial fraction decomposition. Since R is a field, $R[x]$ is a PID. The elements of its field of fractions K can be written as above. $\square$

Problem I.4.7. A subset S of a commutative ring R is a *multiplicative subset* (or *multiplicatively closed*) if (i) $1 \in S$ and (ii) $s, t \in S \implies st \in S$. Define a relation on the set of pairs (a, s) with $a \in R, s \in S$ as follows:

$$(a, s) \sim (a', s') \iff (\exists t \in S), t(s'a - sa') = 0.$$

Note that if R is an integral domain and $S = R \setminus 0$, then S is a multiplicative subset, and the relation agrees with the relation introduced in §4.2.

- Prove that the relation $\sim$ is an *equivalence* relation.

- Denote by $\frac{a}{s}$ the equivalence class of (a, s), and define the same operations $+, \cdot$ on such 'fractions' as the ones introduced in the special case of §4.2. Prove that these operations are well-defined.

- The set $S^{-1}R$ of fractions, endowed with the operations $+, \cdot$, is the *localization of R at the multiplicative subset S* . Prove that $S^{-1}R$ is a commutative ring and that the function $a \mapsto \frac{a}{1}$ defines a ring homomorphism $\ell : R \to S^{-1}R$.
- Prove that $\ell(s)$ is invertible for every $s \in S$.
- Prove that $R \to S^{-1}R$ is initial among ring homomorphisms $f : R \to R'$ such that $f(s)$ is invertible in R' for every $s \in S$.
- Prove that $S^{-1}R$ is an integral domain if R is an integral domain.
- Prove that $S^{-1}R$ is the zero-ring if and only if $0 \in S$.

Solution. The relation is clearly reflexive. Let $t = 1$ and we find $t(sa - sa) = 0$ so $(a, s) \sim (a, s)$. Now suppose $(a, s) \sim (a', s')$. That is, there is a $t \in S$ such that $t(s'a - sa') = 0$. But then $-t(sa' - s'a) = 0$ so $t(sa' - s'a) = 0$. Thus, $(a', s') \sim (a, s)$. Finally, suppose $(a, s) \sim (a', s')$ and $(a', s') \sim (a'', s'')$. We have $t_1(s'a - sa') = 0$ and $t_2(s''a' - s'a'') = 0$. Then

$$s't_1t_2(s''a - sa'') = t_2s'' \cdot t_1(s'a - sa') + t_1s \cdot t_2(s''a' - s'a'') = 0$$

so the relation is transitive and hence an equivalence relation.

To verify that the operations are well-defined, suppose $(a_1, s_1) \sim (a_2, s_2)$. Then

$$t\left((s'a_1 + s_1a')(s_2s') - (s'a_2 - s_2a')(s_1s')\right) = (s')^2 \cdot t(a_1s_2 - a_2s_1) = 0$$

so addition is well-defined. Similarly,

$$t\left((s_2s')(a_1a') - (s_1s')(a_2a')\right) = a's' \cdot t(s_2a_1 - s_1a_2) = 0$$

so multiplication is well-defined.

To show that $S^{-1}R$ is a commutative ring, let $+, \cdot$ be the operations on the set of fractions. Clearly the set under $+$ forms a group with additive identity $\frac{0}{1}$ and inverses $-\frac{a}{s}$. Furthermore, we have

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'} = \frac{sa' + s'a}{s's} = \frac{a'}{s'} + \frac{a}{s}$$

so this group is abelian. Similarly, multiplication is commutative (assuming R is commutative). Lastly, we can see that distributivity holds since

$$\frac{a}{r}\left(\frac{b}{s} + \frac{c}{t}\right) = \frac{a}{r}\frac{(bt + cs)}{st} = \frac{abt}{rst} + \frac{acs}{rst} = \frac{a}{r} \cdot \frac{b}{s} + \frac{a}{r} \cdot \frac{c}{t}.$$

It is easy to verify that ℓ is a ring homomorphism since $\ell(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \ell(a) + \ell(b)$ and $\ell(a \cdot b) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = \ell(a) \cdot \ell(b)$. The identity is also preserved.

If $s \in S$, then $\ell(s) = \frac{s}{1}$. But we have $\frac{s}{1} \cdot \frac{1}{s} = 1$ and $\frac{1}{s} \in S^{-1}R$ since $s \in S$. Thus, $\ell(s)$ is invertible.

To prove that $R \to S^{-1}R$ is initial among homomorphisms $f : R \to R'$ such that $f(s)$ is invertible in R' for $s \in S$, we need to define an induced homomorphism $\hat{f} : S^{-1}R \to R'$ such that the diagram

$$\begin{tikzcd} S^{-1}R \arrow[rr, "\hat{f}"] & & R' \\ & R \arrow[ul, "\ell"] \arrow[ur, "f"'] & \end{tikzcd}$$

commutes, and we must require that $\hat{f}$ is unique. Note that if $\hat{f}$ exists then we must have

$$\hat{f}\left(\frac{a}{s}\right) = \hat{f}\left(\frac{a}{1}\right)\hat{f}\left(\frac{1}{s}\right) = \hat{f}(\ell(a))\hat{f}(\ell(s)^{-1}) = f(a)f(s)^{-1}$$

so the definition of $\hat{f}$ is unique. Furthermore, the definition $\hat{f}\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$ is in fact a well-defined ring homomorphism from $S^{-1}R$ to R', showing that ℓ is initial.

Suppose that $S^{-1}R$ is not an integral domain. That is, there exist nonzero $\frac{a_1}{s_1}, \frac{a_2}{s_2}$ whose product is zero. That is, we have

$$\frac{a_1a_2}{s_1s_2} = \frac{0}{1} \Longrightarrow (\exists t \in S), t(a_1a_2) = 0$$

which can only occur if R is not an integral domain. The contrapositive is that if R is an integral domain then so is $S^{-1}R$.

First assume $0 \in S$. Then $\ell(0)$ is invertible in $S^{-1}R$, say its inverse is r. But then we have $\ell(0)r = 0 \cdot r = 1$ so $0 = 1$ implying that $S^{-1}R$ is the zero-ring. Now suppose $0 \notin S$. Then 0 is not invertible in $S^{-1}R$ so $S^{-1}R$ is not the zero ring. $\square$

Problem I.4.8. Let S be a multiplicative subset of a commutative ring R, as in Exercise 4.7. For every R-module M, define a relation $\sim$ on the set of pairs (m, s), where $m \in M$ and $s \in S$:

$$(m, s) \sim (m', s') \Longleftrightarrow (\exists t \in S), t(s'm - sm') = 0.$$

Prove that this is an equivalence relation, and define an $S^{-1}R$-module structure on the set $S^{-1}M$ of equivalence classes, compatible with the R-module structure on M. The module $S^{-1}M$ is the *localization* of M at S.

Solution. This can be shown to be an equivalence relation in the same manner as above. To define an $S^{-1}R$-module structure on $S^{-1}M$, let

$$\frac{r}{s} \cdot \frac{m}{t} = \frac{r \cdot m}{st}.$$

Clearly this satisfies the definition of a module as

$$\frac{r}{s}\cdot\left(\frac{m_1}{t_1}+\frac{m_2}{t_2}\right)=\frac{r}{s}\cdot\frac{t_2m_1+t_1m_2}{t_1t_2}=\frac{r}{s}\cdot\frac{m_1}{s_1}+\frac{r}{s}\cdot\frac{m_2}{s_2}$$

The remaining axioms can be checked similarly. Furthermore, it is compatible with the R-module structure on M. □

Problem I.4.9. Let S be a multiplicative subset of a commutative ring R, and consider the localization operation introduced in Exercises 4.7 and 4.8.

- Prove that if I is an ideal of R such that $I \cap S = \emptyset$, then $I^e := S^{-1}I$ is a proper ideal of $S^{-1}R$.
- If $\ell : R \to S^{-1}R$ is the natural homomorphism, prove that if J is a proper ideal of $S^{-1}R$, then $J^c := \ell^{-1}(J)$ is an ideal of R such that $J^c \cap S = \emptyset$.
- Prove that $(J^c)^e = J$, while $(I^e)^c = \{a \in R \mid (\exists s \in S) sa \in I\}$.
- Find an example showing that $(I^e)^c$ need not equal I, even if $I \cap S = \emptyset$. (Hint: Let $S = \{1, x, x^2, \dots\}$ in $R = \mathbb{C}[x, y]$. What is $(I^e)^c$ for $I = (xy)$?)

Solution. Clearly $0 \in S^{-1}I$ since $0 \in I$. Now let $\frac{a}{s}, \frac{b}{t} \in I^e$. Then

$$\frac{a}{s}-\frac{b}{t}=\frac{ta-sb}{st}\in I^e$$

since $ta - sb \in I$ and $st \in S$. Furthermore, let $\frac{r}{s} \in S^{-1}R$. Then

$$\frac{r}{s}\cdot\frac{a}{s'}=\frac{ra}{ss'}\in I^e$$

because $ra \in I$. Thus I^e is an ideal of $S^{-1}R$. Clearly it is proper because I does not contain any elements in S. Otherwise we would have $1 = \frac{s}{s} \in I^e$ and I^e would be all of $S^{-1}R$.

Now let J be a proper ideal of $S^{-1}R$. Since $0 \in J$, we have $\ell(0) = 0$ so $0 \in \ell^{-1}(J)$. Now suppose $a, b \in J^c$. Then $a - b = \ell^{-1}(\frac{a}{1}) - \ell^{-1}(\frac{b}{1}) \in J^c$. Similarly, it is closed under multiplication by R. Finally, suppose $J^c \cap S$ is nonempty. Then $\frac{s}{1} \in J$. But then $1 = \frac{1}{s} \cdot \frac{s}{1} \in J$ so J is all of $S^{-1}R$, a contradiction to it being proper. Thus, $J^c \cap S = \emptyset$.

Let $\frac{a}{s} \in (J^c)^e$. Then $\frac{a}{s} \in S^{-1}\ell^{-1}(J)$. In particular, $a \in \ell^{-1}(J)$ so $\frac{a}{1} \in J$. Therefore $\frac{a}{s} \in J$ so $(J^c)^e \subseteq J$. Now suppose $\frac{a}{s} \in J$. Then $a \in \ell^{-1}(J) = J^c$. It follows that $\frac{a}{s} \in (J^c)^e$ so $(J^c)^e = J$. Given an ideal $I \subseteq R$, suppose $a \in (I^e)^c$. Then $\ell(a) = \frac{a}{1} \in I^e = S^{-1}I$. In particular, $a \in I$ so $\subseteq$ holds. Now let $a \in R$ such that there is an $s \in S$ with $sa \in I$. Then $\ell(sa) \in I^e$ so $\frac{a}{1} \in I^e$. But then $a \in \ell^{-1}(I^e)$ showing that $\supseteq$ holds, meaning the two sets are equal.

Using the hint, consider the set $S = \{1, x, x^2, \dots\}$ in the ring $R = \mathbb{C}[x, y]$. Clearly the ideal $I = (xy)$ does not intersect S since every nonzero element of I contains a factor of y. In fact, this means that $(I^e)^c = (y)$. □

Problem I.4.10. With notation as in Exercise 4.9, prove that the assignment $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ gives an inclusion-preserving bijection between the set of *prime* ideals of R disjoint from S and the set of prime ideals of $S^{-1}R$. (Prove that $(\mathfrak{p}^e)^c = \mathfrak{p}$ if $\mathfrak{p}$ is a prime ideal disjoint from S.)

Solution. Let $\mathfrak{p}$ be a prime ideal disjoint from S. First we will show that $\mathfrak{p}^e$ is a prime ideal. Let $\frac{r}{s} \cdot \frac{a}{t} \in \mathfrak{p}^e$ with $\frac{r}{s} \notin \mathfrak{p}^e$. That is, $ra \in \mathfrak{p}$ but $r \notin \mathfrak{p}$ so $a \in \mathfrak{p}$. Since $t \in S$, we have $\frac{a}{t} \in \mathfrak{p}^e$, showing that it is prime. Now we must show the assignment is a bijection. Recall that $(\mathfrak{p}^e)^c = \{a \in R \mid (\exists s \in S) sa \in \mathfrak{p}\}$. However, since $s \notin \mathfrak{p}$, $sa \in \mathfrak{p}$ if and only if $a \in \mathfrak{p}$. In particular, $(\mathfrak{p}^e)^c = \mathfrak{p}$. Since $(\mathfrak{p}^c)^e = \mathfrak{p}$ as well, the assignment has a two-sided inverse and is a bijection. Finally, we show the bijection preserves inclusion. Suppose $\mathfrak{p} \subseteq \mathfrak{p}'$. Let $\frac{a}{s} \in \mathfrak{p}^e$. Since $a \in \mathfrak{p}'$ and $s \in S$, we have $\frac{a}{s} \in \mathfrak{p}'^e$. Thus, the inclusion is preserved. $\square$

Problem I.4.11. A ring is said to be *local* if it has a single maximal ideal.

Let R be a commutative ring, and let $\mathfrak{p}$ be a prime ideal of R. Prove that the set $S = R \setminus \mathfrak{p}$ is multiplicatively closed. The localization $S^{-1}R, S^{-1}M$ are then denoted $R_\mathfrak{p}, M_\mathfrak{p}$.

Prove that there is an inclusion-preserving bijection between the prime ideals of $R_\mathfrak{p}$ and the prime ideals of R contained in $\mathfrak{p}$. Deduce that $R_\mathfrak{p}$ is a local ring.

Solution. Since $\mathfrak{p}$ is a proper ideal, we have $1 \in R \setminus \mathfrak{p}$. Suppose $s, t \in S$. If $st \in \mathfrak{p}$ then one of $s, t \in \mathfrak{p}$, a contradiction. Thus, $st \in S$ so it is multiplicatively closed.

The assignment defined in Exercise 4.10 yields the desired inclusion-preserving bijection since a prime ideal contained in $\mathfrak{p}$ is obviously disjoint from S. Thus, the only maximal ideal is $\mathfrak{p}^e$. To show this, let I be an ideal in $R_\mathfrak{p}$. Then I is contained in some maximal ideal. If $\frac{a}{b} \in I$ with $a, b \in R \setminus \mathfrak{p}$ then $\frac{b}{a} \in R \setminus p$ so $\frac{a}{b} \cdot \frac{b}{a} = 1 \in I$ so $I = R_\mathfrak{p}$. Thus, $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal, meaning $R_\mathfrak{p}$ is a local ring. $\square$

Problem I.4.12. Let R be a commutative ring, and let M be an R-module. Prove that the following are equivalent:

- $M = 0$.
- $M_\mathfrak{p} = 0$ for every prime ideal $\mathfrak{p}$.
- $M_\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$.

(Hint: For the interesting implication, suppose that $m \neq 0$ in M; then the ideal $\{r \in R \mid rm = 0\}$ is proper. By Proposition 3.5, it is contained in a maximal ideal $\mathfrak{m}$. What can you say about $M_\mathfrak{m}$.

Solution. Suppose $M = 0$. For a prime ideal $\mathfrak{p}$, we have $M_\mathfrak{p} = \{\frac{a}{b} \mid a \in M, b \in R \setminus \mathfrak{p}\} = \{0\}$ since the only element of M is 0. The second statement clearly implies the third since every maximal ideal $\mathfrak{m}$ is prime. To show the third point implies the first, suppose $m \neq 0$ in M. The ideal specified in the hint is proper so it is contained in a maximal ideal $\mathfrak{m}$. Then $M_\mathfrak{m} = \{\frac{a}{b} \mid a \in M, b \in R \setminus \mathfrak{m}\}$ contains the nonzero element $\frac{m}{1}$. Thus, if $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$, then $M = 0$, showing that all of the listed properties are equivalent. $\square$

Problem I.4.13. Let k be a field, and let v be a discrete valuation on k. Let R be the corresponding DVR, with local parameter t (see Exercise 2.20).

- Prove that R is local, with maximal ideal $\mathfrak{m} = (t)$. (Hint: Note that every element of $R \setminus \mathfrak{m}$ is invertible.)
- Prove that k is the field of fractions of R.
- Now let A be a PID, and let $\mathfrak{p}$ be a prime ideal in A. Prove that the localization $A_\mathfrak{p}$ is a DVR. (Hint: If $\mathfrak{p} = (p)$, define a valuation on the field of fractions of A in terms of 'divisibility by p'.)

Solution. First, recall that a local parameter $t \in R$ is an element such that $v(t) = 1$. We have shown in Exercise 2.20 that local parameters have the property that for any nonzero ideal I of R, we have $I = (t^k)$ for some $k \geq 1$. Thus, $I \subseteq (t)$ so (t) is the unique maximal ideal and R is local. Alternatively, suppose $a \in I$ is not divisible by t. If $v(a) > 0$ then $v(a/t) = v(a) - v(t) \geq 0$ so $a/t \in R$. Thus, $v(a) = 0$. Furthermore, $v(a^{-1}) = -v(a) = 0$ so $a^{-1} \in R$ and a is invertible. Therefore, $1 = a \cdot a^{-1} \in I$ so $I = R$.

Let K denote the field of fractions of R. There is an obvious embedding $f : R \to k$ so by the universal property of the field of fractions, there is an injective homomorphism $\hat{f} : K \to k$. To show the fields are isomorphic, we construct an explicit isomorphism. Consider $g : k \to K$ letting $g(a) = \frac{a}{1}$. Clearly g is a homomorphism so it is injective. To show that it is surjective, let $\frac{a}{b} \in K$. Then $\frac{a}{b} = \frac{ab^{-1}}{bb^{-1}} = g(ab^{-1})$ so the image of g is all of K. Thus, k is the field of fractions of R.

Let $\mathfrak{p} = (p)$. The localization $A_\mathfrak{p} = \{\frac{a}{b} \mid a \in A, b \in A \setminus \mathfrak{p}\}$. Since A is a PID, it is also a UFD so elements of $A_\mathfrak{p}$ can be expressed as $\frac{p^k a'}{b}$ for some $k \geq 0$. This is a generalization of the p-adic valuation defined over the rationals in Exercise 2.19. $\square$

Problem I.4.14. With notation as in Exercise 4.8, define operations $N \mapsto N^e$ and $\hat{N} \mapsto \hat{N}^c$ for submodules $N \subseteq M$, $\hat{N} \subseteq S^{-1}M$, respectively, analogously to the operations defined in Exercise 4.9. Prove that $(\hat{N})^c)^e = \hat{N}$. Prove that every localization of a Noetherian module is Noetherian.

In particular, all localizations $S^{-1}R$ of a Noetherian ring are Noetherian.

Solution. Let $\frac{a}{s} \in \hat{N}$. Then $a \in \ell^{-1}(\hat{N})$ so $\frac{a}{s} \in (\hat{N}^c)^e$. Now suppose $\frac{a}{s} \in (\hat{N}^c)^e$. Then $a \in \hat{N}^c$ so $a \in \ell^{-1}(\hat{N})$. That is, $\frac{a}{1} \in \hat{N}$. But then $\frac{1}{s} \cdot \frac{a}{1} = \frac{a}{s} \in \hat{N}$. Thus, $(\hat{N}^c)^e = \hat{N}$.

Consider a chain of ascending submodules

$$S^{-1}M_1 \subset S^{-1}M_2 \subset \cdots$$

of $S^{-1}N$ for some Noetherian module N. Then we can take the mapping $\hat{N} \mapsto \hat{N}^c$ for each submodule in the chain to obtain the chain

$$M_1 \subset M_2 \subset \cdots$$

which stabilizes since N is Noetherian. Thus, the original chain also stabilizes and $S^{-1}N$ is Noetherian. $\square$

Problem I.4.15. Let R be a UFD, and let S be a multiplicatively closed subset of R (cf. Exercise 4.7).

- Prove that if q is irreducible in R, then $q/1$ is either irreducible or a unit in $S^{-1}R$.
- Prove that if a/s is irreducible in $S^{-1}R$, then a/s is an associate of $q/1$ for some irreducible element q of R.
- Prove that $S^{-1}R$ is also a UFD.

Solution. Let q be an irreducible element of R. If q divides some element of S, say $s = qr$, then $q/1$ is a unit because

$$\frac{q}{1} \cdot \frac{r}{s} = \frac{qr}{s} = 1.$$

Now suppose q does not divide any element of S. If $q/1$ factorizes in $S^{-1}R$, then we have $\frac{q}{1} = \frac{a}{s} \cdot \frac{b}{s'}$. That is, there is some $t \in S$ such that

$$tqss' = tab.$$

Since R is a UFD, and there is only one factor of q on the left hand side, there is also only one factor of q on the right hand side. WLOG, say q divides a. Then the irreducible elements in the factorization of b divide elements of S. Thus $\frac{b}{s'}$ is a unit (by case one) and $\frac{1}{q}$ is irreducible.

Consider a factorization $\frac{a}{s} = \frac{q}{1} \cdot \frac{b}{t}$ for some irreducible element q. Since $\frac{a}{s}$ is irreducible, one of the factors is a unit. If $\frac{b}{t}$ is a unit, then $(\frac{q}{1}) = (\frac{a}{s})$. If $\frac{q}{1}$ is a unit, then so is $\frac{q}{t}$. In particular, we can rewrite the factorization as $\frac{a}{s} = \frac{q}{t} \cdot \frac{b}{1}$. Finally, b is irreducible in R because if it were not then $\frac{b}{1}$ would not be irreducible in $S^{-1}R$. Thus, $(\frac{a}{s}) = (\frac{b}{1})$ for an irreducible b.

Let $\frac{a}{s} \in S^{-1}R$. Suppose $a = u(p_1^{b_1} \cdots p_r^{b_r})(q_1^{c_1} \cdots q_t^{c_t})$ where the p_i are irreducible elements which divide elements in S and the q_i are irreducible elements which do not divide elements in S. Then we have

$$\frac{a}{s} = \frac{u}{s} \cdot \frac{p_1^{b_1}}{1} \cdots \frac{p_r^{b_r}}{1} \cdot \frac{q_1^{c_1}}{1} \cdots \frac{q_t^{c_t}}{1}$$

is a factorization of $\frac{a}{s}$ into a unit multiplied by a product of irreducibles (by the first point). Uniqueness follows from multiplying factors by a unit and using the second point. $\square$

Problem I.4.16. Let R be a Noetherian integral domain, and let $s \in R$, $s \neq 0$, be a prime element. Consider the multiplicatively closed subset $S = \{1, s, s^2, \ldots\}$. Prove that R is a UFD if and only if $S^{-1}R$ is a UFD. (Hint: By Exercise 2.10, it suffices to show that every prime of height 1 is principal. Use Exercise 4.10 to relate prime ideals in R to prime ideals in the localization.)

On the basis of results such as this and of Exercise 4.15, one might suspect that being factorial is a local property, that is, that R is a UFD if and only if $R_\mathfrak{p}$ is a UFD for all primes $\mathfrak{p}$, if and only if $R_\mathfrak{m}$ is a UFD for all maximals $\mathfrak{m}$. This is regrettably not the case. A ring R is *locally factorial* if $R_\mathfrak{m}$ is a UFD for all maximal ideals $\mathfrak{m}$; factorial implies locally factorial by Exercise 4.15, but locally factorial rings that are not factorial do exist.

Solution. We have shown that if R is a UFD then $S^{-1}R$ is also a UFD. To show the converse, let $\mathfrak{p}$ be a prime ideal of height 1 in R. There is a corresponding prime ideal $\mathfrak{p}^e \in S^{-1}R$ which also has height 1. If $S^{-1}R$ is a UFD then $\mathfrak{p}^e$ is principal. But then $\mathfrak{p}$ is principal as well, so R is a UFD. $\square$

Problem I.4.17. Let F be a field, and recall the notion of *characteristic* of a ring; the characteristic of a field is either 0 or a prime integer (Exercise III.3.14.)

- Show that F has characteristic 0 if and only if it contains a copy of $\mathbb{Q}$ and that F has characteristic p if and only if it contains a copy of the field $\mathbb{Z}/p\mathbb{Z}$.
- Show that (in both cases) this determines the smallest subfield of F; it is called the *prime subfield* of F.

Solution. Recall that the characteristic of a ring is the smallest nonnegative integer such that $n \cdot 1 = 0$. Suppose a field F contains a copy of $\mathbb{Q}$ and consider the homomorphism $f : \mathbb{Z} \to F$, $f(a) = a \cdot 1$. Let n denote the characterstic of the ring. If $n > 0$ then $f(n) = n \cdot 1 = 0$. However, $n \neq 0$ in F since $n \neq 0$ in $\mathbb{Q}$. Therefore, $n = 0$. Now suppose F has characteristic 0. Then there is an injective homomorphism $f : \mathbb{Z} \to F$. That is, there is an embedding of $\mathbb{Z}$ into K so K contains the inverses of the integers as well. Thus, K contains the field of fractions of $\mathbb{Z}$ which is isomorphic to $\mathbb{Q}$.

Now suppose a field F contains $\mathbb{Z}/p\mathbb{Z}$ and consider the homomorphism $f : \mathbb{Z} \to F, f(a) = a \cdot 1$. Let n denote the characteristic of F. Then $n \leq p$ since $f(p) = p \cdot 1 = 0$. If $n < p$ and $n \cdot 1 = 0$, we arrive at a contradiction since this does not hold in $\mathbb{Z}/p\mathbb{Z}$. Thus, $n = p$. Now suppose F has characteristic p and consider the homomorphism $f : \mathbb{Z} \to F$. The homomorphism has kernel $p\mathbb{Z}$. By the first isomorphism theorem,

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathrm{im} f \subseteq F$$

completing the proof. Note that in both cases, the desired subfield is generated by 1.

Consider the intersection of all subfields of F, denoted by K. Certainly $1 \in K$. If $\mathrm{char}(F) = p$ then K contains the subfield generated by 1 which we have shown is isomorphic $\mathbb{Z}/p\mathbb{Z}$. Similarly, if $\mathrm{char}(F) = 0$ then K contains $\mathbb{Z}$ and its multiplicative inverses which is isomorphic to $\mathbb{Q}$. The reverse inclusion is obvious, completing the proof. □

Problem I.4.18. Let R be an integral domain. Prove that the invertible elements in $R[x]$ are the units of R, viewed as constant polynomials.

Solution. Certainly the units of R are invertible in $R[x]$. To show that these are the only invertible elements, suppose $fg = 1$. Since R is a domain, we have the identity $\deg(fg) = \deg(f) + \deg(g)$. It follows that f and g are constant and thus are units in R. □

Problem I.4.19. An element $a \in R$ in a ring is said to be *nilpotent* if $a^n = 0$ for some $n \geq 0$. Prove that if a is nilpotent, then $1 + a$ is a unit in R.

Solution. Suppose a is nilpotent, say $a^n = 0$. Then

$$(1 + a)(1 - a + a^2 - \cdots + (-1)^{n-1}a^{n-1}) = 1$$

so $1 + a$ is invertible. □

Problem I.4.20. Generalize the result of Exercise 4.18 as follows: let R be a commutative ring, and let $f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$; prove that f is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_d$ are nilpotent. (Hint: If $b_0 + b_1x + \cdots + b_ex^e$ is the inverse of f, show by induction that $a_d^{i+1}b_{e-i} = 0$ for all $i \geq 0$, and deduce that a_d is nilpotent.)

Solution. First, note that if an element a is nilpotent, then so is ra for all $r \in R$. Furthermore, given a unit a_0 and a nilpotent element a_1, we have $a_0 + a_1 = a_0(1 + a_0^{-1}a_1)$ which is the product of two units and thus a unit itself.

We do a proof by induction for both directions. Suppose a_0 is a unit and a_i is nilpotent for $i > 0$. In the case $n = 1$, we have shown above that $a_0 + a_1 x$ is a unit. Now suppose this holds for $n = k$ and let $n = k + 1$. Consider the polynomial $p(x) = a_0 + a_1 x + \cdots a_{k+1} x^{k+1}$. By the hypothesis, $f(x) = a_0 + a_1 x + \cdots a_k x^k$ is a unit. Furthermore, $a_{k+1} x^{k+1}$ is nilpotent. Since the sum of a unit and a nilpotent element is a unit, $p(x)$ must be a unit.

For the reverse direction, suppose f is a unit with inverse g. Clearly $a_0 b_0 = 1$. Thus, a_0 and b_0 are both units. To show that $a_d^{i+1} b_{e-i} = 0$ for $i \geq 0$, we induct on i. For the case $i = 0$, the statement clearly holds as $a_d b_e$ is the leading term of fg. For $i > 0$, the coefficient of x^{d+e-i} is

$$a_d b_{e-i} + a_{d-1} b_{e-i+1} + \cdots + a_{d-i} b_e.$$

Multiplying through by a_d^i and applying the induction hypothesis proves the result. In particular, letting $i = e$ and using the fact that b_0 is a unit shows that a_d is nilpotent. Therefore $f - a_d x^d$ is a unit (by the first part of this solution). Repeating allows us to conclude that all a_i for $i > 0$ are nilpotent. $\square$

Problem I.4.21. Establish the characterization of irreducible polynomials over a UFD given in Corollary 4.17.

Corollary 4.17. *Let R be a UFD and K the field of fractions of R. Let $f \in R[x]$ be a nonconstant polynomial. Then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$ and primitive.*

Solution. One direction is proven in the chapter so we prove the other to establish the characterization. Suppose $f \in R[x]$ is irreducible in $K[x]$ and primitive. Assume $f = gh$ for $g, h \in R[x]$. The irreducibility of f in $K[x]$ implies that one of g, h is a unit in $K[x]$, say g. By Exercise 4.18, g has degree 0 so $\text{cont}(g) = g$. But then $1 = \text{cont}(f) = \text{cont}(g)\text{cont}(h)$ so g is a unit in R, implying that f is irreducible in $R[x]$. $\square$

Problem I.4.22. Let k be a field, and let f, g be two polynomials in $k[x, y] = k[x][y]$. Prove that if f and g have a nontrivial common factor in $k(x)[y]$, then they have a nontrivial common factor in $k[x, y]$.

Solution. Recall that $k(x)$ is the field of fractions of $k[x]$. Suppose f and g have a nontrivial common factor in $k(x)[y]$, say h. We can choose $c \in k(x)$ such that $h = ch'$ where $h' \in k[x, y]$. But then h' is a nontrivial factor of f and g. $\square$

Problem I.4.23. Let R be a UFD, K its field of fractions, $f(x) \in R[x]$, and assume $f(x) = \alpha(x)\beta(x)$ with $\alpha(x), \beta(x)$ in $K[x]$. Prove that there exists a $c \in K$ such that $c\alpha(x) \in R[x]$, $c^{-1}\beta(x) \in R[x]$, so that

$$f(x) = (c\alpha(x))(c^{-1}\beta(x))$$

splits $f(x)$ as a product of factors in $R[x]$.

Deduce that if $\alpha(x)\beta(x) = f(x) \in R[x]$ is monic and $\alpha(x) \in K[x]$ is monic, then $\alpha(x), \beta(x)$ are both in $R[x]$ and $\beta(x)$ is also monic.

Solution. First note that if f is not primitive then we can factor out the content and let $c = 1$ so we may assume f is primitive. Let $a, b \in K$ such that

$$\alpha = a\underline{\alpha}, \quad \beta = b\underline{\beta}$$

where $\underline{\alpha}, \underline{\beta}$ are primitive in $R[x]$. Note that by Gauss' lemma, ab is a unit in R. Then there exists a unit $u \in R$ such that $a = b^{-1}u$. Now let $c = a^{-1}$ and $c^{-1} = b^{-1}u$. Then we find $c\alpha = a^{-1}\alpha = \underline{\alpha} \in R[x]$. Similarly, $c^{-1}\beta = b^{-1}u\beta = u\underline{\beta} \in R[x]$. Then we find

$$(c\alpha)(c^{-1}\beta) = u\underline{\alpha}\underline{\beta} = ab\underline{\alpha}\underline{\beta} = f$$

so we are done.

We deduce that if f and α are monic, then β is monic as well so that the leading coefficient of f is 1. Furthermore, suppose $\alpha \notin R[x]$. Then there exists an element $c \in K$ such that $c\alpha \in R[x]$. Note that c is not a unit in R or else $\alpha \in R[x]$. But then the leading coefficient of $c^{-1}\beta$ is c^{-1} so $c^{-1}\beta \notin R[x]$. Similar reasoning shows that both $\alpha, \beta \in R[x]$. $\square$

Problem I.4.24. In the same situation as in Exercise 4.23, prove that the product of any coefficient of α with any coefficient of β lies in R.

Solution. Let α_i, β_i denote the i-th coefficient of α, β respectively. Using the result of the previous exercise, we have $c\alpha_i, c^{-1}\beta_i \in R$ for all i. Then $\alpha_i\beta_j = c\alpha_i \cdot c^{-1}\beta_j \in R$ for all i, j. $\square$

Problem I.4.25. Prove *Fermat's last theorem for polynomials:* the equation

$$f^n + g^n = h^n$$

has no solutions in $\mathbb{C}[t]$ for $n > 2$ and f, g, h not all constant. (Hint: First, prove that f, g, h may be assumed to be relatively prime. Next, the polynomial $1 - t^n$ factorizes in $\mathbb{C}[t]$ as $\prod_{i=1}^n (1 - \zeta^i t)$ for $\zeta = e^{2\pi i/n}$; deduce that $f^n = \prod_{i=1}^n (h - \zeta^i g)$. Use unique factorization in $\mathbb{C}[t]$ to conclude that each of the factors $h - \zeta^i g$ is an n-th power. Now let $h - g = a^n$, $h - \zeta g = b^n$, $h - \zeta^2 g = c^n$ (this is where the $n > 2$ hypothesis enters). Use this to obtain a relation $(\lambda a)^n + (\mu b)^n = (\nu c)^n$, where λ, μ, ν are suitable complex numbers. What's wrong with this?)

The same pattern of proof would work in any environment where unique factorization is available; if adjoining to $\mathbb{Z}$ a primitive n-th root of 1 and roots of other elements as needed in this argument led to a unique factorization domain, the full-fledged Fermat's last theorem would be as easy to prove as indicated in this exercise. This is not the case, a fact famously missed by G. Lamé as he announced a 'proof' of Fermat's last theorem to the Paris Academy on March 1, 1847.

Solution. First, note that if f, g, h have a common factor c then $(f/c)^n + (g/c)^n = (h/c)^n$ is another solution. Thus, we may assume that f, g, h are relatively prime. If we consider K to be the field of fractions of $\mathbb{C}[t]$ then we have

$$1 - \left(\frac{g}{h}\right)^n = \prod_{i=1}^{n} \left(1 - \zeta^i \frac{g}{h}\right).$$

Multiplying both sides by h^n yields the factorization $f^n = h^n - g^n = \prod_{i=1}^{n}(h - \zeta^i g)$. Now we show that $(h - \zeta^i g)$ is coprime to $(h - \zeta^j g)$ for $i \neq j$. Indeed, we find that

$$h - \zeta^i g - (h - \zeta^j g) = (\zeta^j - \zeta^i) g$$
$$h - \zeta^i g + \frac{\zeta^i}{\zeta^j - \zeta^i} \left(\zeta^j - \zeta^i\right) g = h$$

Since $\mathbb{C}[t]$ is a Euclidean domain, we have $\gcd(h - \zeta^i g, h - \zeta^j g) = \gcd(g, h) = 1$. Thus, the factors are all coprime.

In any UFD, if the product of coprime factors is an n-th power, then each factor is an n-th power. We prove this by induction on the number of prime factors of c which we denote by k. Indeed, suppose a, b are coprime and let $ab = c^n$. If $k = 0$ then c is a unit so a, b are units multiplied by 1^n. If $k > 0$ then there is a prime $p \mid c$ so $p^n \mid c^n = ab$. Therefore, $p^n \mid a$ or $p^n \mid b$ since a, b are coprime. WLOG, assume the latter. We find $a(b/p^n) = (c/p)^n$. Since c/p has fewer prime factors than c, the inductive hypothesis applies and $a = r^n, b/p^n = s^n \implies b = (ps)^n$. Thus, we have shown that we can write $h - g = a^n, h - \zeta g = b^n, h - \zeta^2 g = c^n$ for $a, b, c \in \mathbb{C}[t]$.

With this, we can derive the following.

$$g = \frac{1}{1 - \zeta}(b^n - a^n)$$
$$h = \frac{1}{1 - \zeta}(b^n - \zeta a^n)$$

$$\zeta a^n + (1 + \zeta) b^n = c^n$$

Since $\mathbb{C}$ is an algebraically closed field, there exist $x, y \in \mathbb{C}$ such that $x^n = \zeta$ and $y^n = 1 + \zeta$. Thus, we can write $(ax)^n + (by)^n = c^n$. But then we find $\max(\deg a, \deg b, \deg c) \leq \max(\deg f, \deg g, \deg h)/n < \max(\deg f, \deg g, \deg h)$. If we take a solution f, g, h to the initial equation such that the maximum degree is minimal among all solutions, then we arrive at a contradiction since we have constructed another solution of lower degree. $\square$