.1 Chain conditions and existence of factorizations

Problem .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 .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 .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 $\{1, x, x^2, \ldots, x^{n-1}\}$. 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. □

Problem .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. □

Problem .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 .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 .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. □

Problem .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. □

Problem .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. □

Problem .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. □

Problem .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. □

Problem .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. □

Problem .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. □

Problem .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 $R/(a)$. □

Problem .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. □

Problem .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 .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 $z = w_1w_2$. 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. $\square$