Solutions 08

1. Euclid proves that there are infinitely many prime integers in the following way: if $p_1, p_2, \dots, p_k$ are prime numbers, then any prime factor of the integer $1 + p_1\, p_2 \cdots p_k$ must be different from p_i for all $1 \leqslant i \leqslant k$.

i. Adapt this argument to demonstrate that, for any field K, there are infinitely many monic irreducible polynomials in $K[x]$.

ii. Explain why the argument fails for the formal power series ring $K[[x]]$ over a field K.

iii. Adapt this argument to show that the set of prime integers of the form $4n - 1$ is infinite.

Solution.

i. Consider a nonempty finite set $\{f_1, f_2, \dots, f_k\}$ of monic irreducible polynomials in $K[x]$. Since the principal ideal domain $K[x]$ is a unique factorization domain, the polynomial $1 + f_1\, f_2\, \cdots\, f_k$, which is not a unit, is a product of a unit and monic irreducible polynomials. Any monic irreducible factor is necessarily distinct from all the f_j, because otherwise it would divide 1. No finite set of monic irreducible polynomials contains all monic irreducible polynomials, so the set of monic irreducible polynomials in $K[x]$ is infinite.

ii. This style of argument fails in formal power series ring $K[[x]]$; given irreducible formal power series $f_1, f_2, \dots, f_k$ in $K[[x]]$, the formal power series $1 + f_1\, f_2\, \cdots\, f_k$ is typically a unit, so not divisible by any irreducible elements.

iii. By considering remainders upon division by 4, we see that every prime integer, except for 2, has the form $4n \pm 1$ for some nonnegative integer n. Suppose that there are only finitely many primes numbers $p_1, p_2, \dots, p_k$ of the form $4n - 1$. The number $m := 4(p_1\, p_2\, \cdots\, p_k) - 1$ is a product of prime numbers. Because the product of two primes having the form $4n + 1$ also has the form $4n + 1$, the odd number m must be divisible by at least one prime of the form $4n - 1$. This prime factor of m is necessarily distinct from $p_1, p_2, \dots, p_k$, as otherwise it would divide -1. We conclude that the set of prime integers of the form $4n - 1$ is infinite. □

2. Let R be a principal ideal domain and let K be its field of fractions.

i. Suppose $R = \mathbb{Z}$. Write $r = 7/24 \in \mathbb{Q}$ in the form $r = a/8 + b/3$.

ii. Consider $g := pq$ in R where p and q are relatively prime. Prove that every fraction $f/g \in K$ can be written in the form

$$\frac{f}{g} = \frac{a}{q} + \frac{b}{p}$$

for some a and b in R.

iii. Let k be a positive integer and let $g := p_1^{m_1}\, p_2^{m_2}\, \cdots p_k^{m_k}$ be the factorization of the element g in R into irreducible elements $p_1, p_2, \dots, p_k$ such that the relation $p_i = u\, p_j$ for some unit u in R implies that $i = j$. Prove that every fraction

$r = f/g \in K$ can be written in the form

$$r = \sum_{i=1}^{k} \frac{h_i}{p_i^{m_i}}$$

for some h_i in R for all $1 \leqslant i \leqslant k$.

Solution.

i. Since $(-1)(8) + (3)(3) = 1$, we have

$$r = \frac{7}{24} = \frac{7[(-1)(8) + (3)(3)]}{24} = \frac{-7}{3} + \frac{21}{8}\,.$$

ii. As $\gcd(p, q) = 1$, there exists u and v in R such that $pu + qv = 1$. Hence, we have

$$r = \frac{f}{g} = \frac{f(pu + qv)}{pq} = \frac{fu}{q} + \frac{fv}{p}\,.$$

iii. We proceed by induction on k. The base case ($k = 1$) is trivially true. For the inductive step, set $p := p_1^{m_1}$ and $q := p_2^{m_2} p_3^{m_3} \cdots p_k^{m_k}$. By hypothesis, we have $\gcd(p, q) = 1$, so there exists u and v in R such that $pu + qv = 1$. Hence, we obtain

$$r = \frac{f}{g} = \frac{f(pu + qv)}{pq} = \frac{fu}{q} + \frac{fv}{p} = \frac{fu}{p_1^{m_1}} + \frac{fv}{p_2^{m_2} p_3^{m_3} \cdots p_k^{m_k}}\,.$$

The induction hypothesis establishes that

$$\frac{fv}{p_2^{m_2} p_3^{m_3} \cdots p_k^{m_k}} = \sum_{i=2}^{k} \frac{h_i}{p_i^{m_i}}$$

for some h_i in R. Setting $h_1 := fu$, we obtain $r = \sum_{i=1}^{k} h_i / p_i^{m_i}$ as required. □

3. Let R be a unique factorization domain such that the sum of two principal ideals in R is again a principal ideal. Prove that R is a principal ideal domain.

Solution. We first prove that every finitely-generated ideal in R is principal. We proceed by induction on the number n of generators for an ideal. When $n \leqslant 1$, the ideal is trivially principal. Assume that any ideal in R generated by less than n generators is principal. Consider an ideal I generated by the elements $g_1, g_2, \dots, g_n$ in R. The induction hypothesis implies that there exists an element h_{n-1} in R such that $\langle g_1, g_2, \dots, g_{n-1} \rangle = \langle h_{n-1} \rangle$, so $I = \langle h_{n-1}, g_n \rangle = \langle h_{n-1} \rangle + \langle g_n \rangle$. Since the sum of two principal ideals in R is again principal, there is an element h_n in R such that

$$\langle h_n \rangle = \langle h_{n-1} \rangle + \langle g_n \rangle = \langle g_1, g_2, \dots, g_{n-1} \rangle + \langle g_n \rangle = \langle g_1, g_2, \dots, g_n \rangle = I$$

which completes the induction.

We next show that every ideal in R is finitely generated. Suppose that an ideal in R is not finitely generated. Hence, there exists an infinite increasing chain

$$\langle f_0 \rangle \subset \langle f_0, f_1 \rangle \subset \langle f_0, f_1, f_2 \rangle \subset \langle f_0, f_1, f_2, f_3 \rangle \subset \cdots$$

of ideals in R. Since every finitely-generated ideal in R is principal, we obtain an infinite increasing chain $\langle g_0 \rangle \subset \langle g_1 \rangle \subset \langle g_2 \rangle \subset \langle g_3 \rangle \subset \cdots$ of principal ideals such that

$\langle g_j \rangle = \langle f_0, f_1, \dots, f_j \rangle$. The proper containment $\langle g_j \rangle \subset \langle g_{j+1} \rangle$ means that g_j is equal to the product of g_{j+1} and a nonzero nonunit in R. As R is a unique factorization domain, there exists a unit u in R and irreducible elements $q_1, q_2, \dots, q_m$ in R such that $g_0 = u\, q_1\, q_2 \cdots q_m$. It follows that there are only finitely many nonunits in R that divide g_0; at most the number of proper subsets of $\{q_1, q_2, \dots, q_m\}$ which equals $2^m - 1$. In other words, we cannot have an infinite increasing chain of principal ideals in R containing $\langle g_0 \rangle$. We conclude that every ideal in R is finitely generated and, therefore, principal. $\square$