5.5 Exercises

5.1 Let R be a ring and m be a fixed element of R. Prove that the congruence $a \equiv b \pmod{m}$ defined by (5.1) is an equivalence relation.

5.2 Let R be a ring and $m \in R$. Prove that the definitions (5.2) and (5.3) are well-defined.

5.3 Let R be a ring and m be a unit of R. Describe the residue class ring $R/(m)$.

5.4 Let R be a ring and $m = 0 \in R$. Describe the residue class ring $R/(0)$.

5.5 Let D be an integral domain and $m, m' \in D$. If $D/(m) = D/(m')$, then m and m' are associates.

5.6 Let F be any field and x, y be indeterminates. Prove that $F[x,y]/(x) \simeq F[y]$.

5.7 Let Ax^2+Bx+C be an irreducible quadratic polynomial in $\mathbb{R}[x]$. Prove that the map (5.4) is an isomorphism from $\mathbb{R}[x]/(Ax^2+Bx+C)$ onto $\mathbb{C}$.

5.8 Write down the addition and multiplication tables of F_8 in Example 5.8.

✎ 5.9 Prove that x^4+x+1 is an irreducible polynomial over $\mathbb{Z}_2$. Then give a rule analogue to (5.8) for multiplying elements in the field $\mathbb{Z}_2[x]/(x^4+x+1)$ and write down its multiplication table.

✎ 5.10 Prove that $x^4+x^3+x^2+x+1$ is an irreducible polynomial over $\mathbb{Z}_2$. Then give a rule analogue to (5.8) for multiplying elements in the field $\mathbb{Z}_2[x]/(x^4+x^3+x^2+x+1)$ and write down its multiplication table.

5.11 Prove that the fields $\mathbb{Z}_2[x]/(x^4+x+1)$ and $\mathbb{Z}_2[x]/(x^4+x^3+x^2+x+1)$ are isomorphic.

✎ 5.12 Prove that x^2-x-1 is an irreducible polynomial over $\mathbb{Z}_3$. Give a rule analogue to (5.8) for multiplying elements in the field $\mathbb{Z}_3[x]/(x^2-x-1)$ and write down its addition and multiplication tables.

1.25. Let $f_1,\ldots,f_n$ be nonzero polynomials in $F[x]$. By considering the intersection $(f_1)\cap\cdots\cap(f_n)$ of principal ideals, prove the existence and uniqueness of the monic polynomial $m\in F[x]$ with the properties attributed to the least common multiple of $f_1,\ldots,f_n$.

1.26. Prove (1.6).

1.27. If $f_1,\ldots,f_n\in F[x]$ are nonzero polynomials that are pairwise relatively prime, show that $\operatorname{lcm}(f_1,\ldots,f_n)=a^{-1}f_1\cdots f_n$, where a is the leading coefficient of $f_1\cdots f_n$.

1.28. Prove that $\operatorname{lcm}(f_1,\ldots,f_n)=\operatorname{lcm}(\operatorname{lcm}(f_1,\ldots,f_{n-1}),f_n)$ for $n\geqslant 3$.

1.29. Let $f_1,\ldots,f_n\in F[x]$ be nonzero polynomials. Write the canonical factorization of each f_i, $1\leqslant i\leqslant n$, in the form

$$f_i=a_i\prod p^{e_i(p)},$$

where $a_i\in F$, the product is extended over all monic irreducible polynomials p in $F[x]$, the $e_i(p)$ are nonnegative integers, and for each i we have $e_i(p)>0$ for only finitely many p. For each p set $m(p)=\min(e_1(p),\ldots,e_n(p))$ and $M(p)=\max(e_1(p),\ldots,e_n(p))$. Prove that

$$\gcd(f_1,\ldots,f_n)=\prod p^{m(p)},$$

$$\operatorname{lcm}(f_1,\ldots,f_n)=\prod p^{M(p)}.$$

1.30. Kronecker's method for finding divisors of degree $\leqslant s$ of a nonconstant polynomial $f\in\mathbb{Q}[x]$ proceeds as follows:

(1) By multiplying f by a constant, we can assume $f\in\mathbb{Z}[x]$.

(2) Choose distinct elements $a_0,\ldots,a_s\in\mathbb{Z}$ that are not roots of f and determine all divisors of $f(a_i)$ for each $i, 0\leqslant i\leqslant s$.

(3) For each $(s+1)$-tuple $(b_0,\ldots,b_s)$ with b_i dividing $f(a_i)$ for $0\leqslant i\leqslant s$, determine the polynomial $g\in\mathbb{Q}[x]$ with $\deg(g)\leqslant s$ and $g(a_i)=b_i$ for $0\leqslant i\leqslant s$ (for instance, by the Lagrange interpolation formula).

(4) Decide which of these polynomials g in (3) are divisors of f.

If $\deg(f)=n\geqslant 1$ and s is taken to be the greatest integer $\leqslant n/2$, then f is irreducible in $\mathbb{Q}[x]$ in case the method only yields constant polynomials as divisors. Otherwise, Kronecker's method yields a nontrivial factorization. By applying the method again to the factors and repeating the process, one eventually gets the canonical factorization of f. Use this procedure to find the canonical factorization of

$$f(x)=\tfrac{1}{3}x^6-\tfrac{5}{3}x^5+2x^4-x^3+5x^2-\tfrac{17}{3}x-1\in\mathbb{Q}[x].$$

1.31. Construct the addition and multiplication table for $\mathbb{F}_2[x]/(x^3+x^2+x)$. Determine whether or not this ring is a field.

1.32. Let $[x+1]$ be the residue class of $x+1$ in $\mathbb{F}_2[x]/(x^4+1)$. Find the residue classes comprising the principal ideal $([x+1])$ in $\mathbb{F}_2[x]/(x^4+1)$