

1. For a field F , let $F(x)$ denote the field of fractions of the ring $F[x]$; in other words, the field of rational functions with coefficients in F . Prove that there is no element $f \in F(x)$ such that $f^2 = x$.

Suppose there is an f such that $f^2 = x$. Let f represent the equivalence class given by some (g, h) for $g, h \in F[x]$; informally we would say $f = \frac{g}{h}$. Then $(g, h)(g, h) = (g^2, h^2)$, which we know is in the same equivalence class as $(x, 1)$, so $g^2 = xh^2$ by the equivalence criterion; note that this is an equality among elements of the integral domain $F[x]$ instead of its field of fractions. Note that if $\deg g = m$, then $\deg(g^2) = \deg(g \cdot g) = (\deg g) + (\deg g) = 2m$, which is even, while if $\deg h = n$, then $\deg(xh^2) = \deg(x \cdot h \cdot h) = \deg x + \deg h + \deg h = 2n + 1$ which is odd; thus g^2 cannot equal xh^2 .

2. Prove that, if I is a prime ideal of a ring R , then $I[x]$ is a prime ideal of $R[x]$.

Since the sums and products of two elements of $I[x]$ are determined by finite sums and products of individual coefficients in I , and since I is closed under addition and multiplication, it is easy to show that the individual coefficients of sums and products of elements of $I[x]$ will have coefficients in I and thus $I[x]$ is closed under addition and multiplication. In addition, an additive inverse of an element of $I[x]$ is achieved by performing termwise additive inverses on the coefficients; the result of each individual procedure will lie in I , so the polynomial so formed lies in $I[x]$. Thus $I[x]$ is a subring of $R[x]$. It remains to show that $I[x]$ is absorbing and prime.

Consider some polynomial $i(x) \in I[x]$ and $r(x) \in R[x]$. Their product has coefficients which are finite sums of the form $\sum_{j=0}^k i_j r_j$ for some integer k and each $i_j \in I$ and $r_j \in R$. Note that since I is absorbing, each $i_j r_j \in I$, and since I is closed under addition, the sum $\sum_{j=0}^k i_j r_j \in I$. Thus each coefficient of $i(x) \cdot r(x)$ is in I , so $i(x) \cdot r(x) \in I[x]$, demonstrating that $I[x]$ is absorbing in $R[x]$.

Finally, let us prove primality. Suppose $a(x), b(x) \in R[x] - I[x]$; we shall show that $a(x)b(x) \in R[x] - I[x]$. Let $a(x) = a_m x^m + \cdots + a_0$ and $b(x) = b_n x^n + \cdots + b_0$. Since $a(x)$ and $b(x)$ are not in $I[x]$, at least one of the coefficients of each must be outside of I . Let i be the smallest integer such that $a_i \notin I$, and let j be the smallest integer such that $b_j \notin J$; now let us compute the $i + j$ th coefficient in $a(x)b(x)$:

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0$$

using the convention that the coefficients above the degree of a polynomial are zero for simplicity. Note that $a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} \in I$ because a_0, \dots, a_{i-1} are in I by the definition of i above, and making use of the absorption and additive closure properties. Likewise, $a_{i+1} b_{j-1} + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0 \in I$ because b_0, \dots, b_{j-1} must be in I . However, $a_i b_j$ is *not* in I because a_i and b_j are not in I and I is prime. Thus the complete sum, as the sum of an element of I and a non-element of I , must not be an element of I (by additive closure with additive inverses). Since at least one coefficient of $a(x)b(x)$ is not in I , $a(x)b(x)$ is not in $I[x]$.

3. Describe a field of order 25 and a field of order 27.

We know that for any finite field F and irreducible polynomial f in F of degree n , the quotient ring $F/\langle f \rangle$ is a field of order $|F|^n$. Thus, since $25 = 5^2$ and $27 = 3^3$, the question here can be satisfied by finding an irreducible quadratic in $\mathbb{Z}_5[x]$ and an irreducible cubic in $\mathbb{Z}_3[x]$. We know that a cubic or quadratic in $F[x]$ is irreducible iff it has no zero. Noting that 0, 1, and 4 are the only perfect squares (a.k.a. quadratic residues) in \mathbb{Z}_5 , the quadratic $x^2 + 2$ will fit the bill; likewise noting that $x^3 = x$ for each $x \in \mathbb{Z}_3$, the polynomial $x^3 - x + 1$ is nonzero everywhere in \mathbb{Z}_3 . Thus, $\mathbb{Z}_5[x]/\langle x^2 + 2 \rangle$ will be a field of order 25, and $\mathbb{Z}_3[x]/\langle x^3 - x + 1 \rangle$ will be a field of order 27. Note that these are not the only possible answers; there are other irreducible quadratics in \mathbb{Z}_5 and cubics in \mathbb{Z}_3 which work equally well.

4. Let $\alpha \in \mathbb{R}$ be a transcendental number, i.e., there is no nonzero polynomial with integer coefficients which has α as a zero. Prove that α^2 cannot be written as a linear combination of α and a rational number, i.e. $\alpha^2 = \alpha x + y$ for $x, y \in \mathbb{Q}$.

Suppose there are rational numbers $\frac{p}{q}$ and $\frac{r}{s}$ such that $\alpha^2 = \alpha \frac{p}{q} + \frac{r}{s}$. Then $\alpha^2 - \frac{p}{q}\alpha - \frac{r}{s} = 0$; multiplying by qs , we find that $\alpha^2 - (ps)\alpha - (qr) = 0$. Considering the polynomial $f(x) = x^2 - psx - qr$, which is in $\mathbb{Z}[x]$, the above result shows that $f(\alpha) = 0$, contradicting the premise that α is transcendental.

5. Prove that for a principal ideal domain D with p an irreducible element of D , $D/\langle p \rangle$ is a field. Show that if D is merely an integral domain, $D/\langle p \rangle$ may not be a field.

Note that for any integral domain D , the quotient ring $D/\langle p \rangle$ is a field if and only if $\langle p \rangle$ is maximal; we shall thus prove maximality of $\langle p \rangle$ for p an irreducible element of D . Since p is irreducible, p is not a unit, so $1 \notin \langle p \rangle$ and thus $\langle p \rangle \neq D$. Now let us suppose, contrary to the intended maximality property, that there is an ideal I such that $\langle p \rangle \subsetneq I \subsetneq D$. Since D is a principal ideal domain, $I = \langle q \rangle$ for some $q \in D$. Since $p \in I$, $p = kq$ for some $k \in D$. However, since p is irreducible, either k or q is a unit. Since $I \neq D$, q cannot be a unit, so k must be a unit, but then $q = k^{-1}p$ so that $q \in \langle p \rangle$ and so $I \subseteq \langle p \rangle$, leading to the contradictory conclusion that $I = \langle p \rangle$.

A simple counterexample for an integral domain is $\mathbb{Z}[x]$, which is an integral domain in which x is irreducible, and yet $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ is not a field.