UCLA ALGEBRA QUALIFYING EXAM

Solutions

JED YANG

R. Rings

Convention. We do not require proper containment when using $\subset$.

Errors. We require $S$ to be nonempty for Qual Problem R3f3. One direction of Qual Problem R1f3-b is (obviously) false.

R9s1. Show that the ring $\mathbb{Z}[2i]$ consisting of all complex numbers $a + 2bi$ with $a, b \in \mathbb{Z}$ is not principal.

Proof. Let $\mathcal{N}(a + 2bi) = a^2 + 4b^2$ be the norm. Notice that since $\mathcal{N}(z)$ coincides with the usual (square of the) norm $|z|^2$, it is multiplicative (it can also be checked by direct computation). Furthermore, $\mathcal{N}$ sends $\mathbb{Z}[2i] \setminus \{0\}$ to $\mathbb{Z}^+$. If $z$ is invertible, then $1 = \mathcal{N}(1) = \mathcal{N}(zz^{-1}) = \mathcal{N}(z)\mathcal{N}(z^{-1})$, yielding that $\mathcal{N}(z) = 1$. Conversely, if $\mathcal{N}(z) = 1$, then obviously $z = \pm 1$, so is a unit. Moreover, if $\mathcal{N}(z) = 4$ then $z$ is irreducible. Indeed, since the norm takes values 0, 1, 4, 5, . . ., if $\mathcal{N}(xy) = 4$, then one of $x$ or $y$ must have norm 1. Now notice that $2 \cdot 2 = 2i \cdot (-2i)$, each factor have norm 4 hence is irreducible. Finally, it suffice to notice that $2i$ and 2 does not differ by a unit, since $2i/2 = i$ is not even a member of $\mathbb{Z}[2i]$. Therefore 4 has different factorizations, so $\mathbb{Z}[2i]$ is not factorial, much less principal. \(\square\)

R9s2. Let $M_n(F)$ be the matrix ring of $n \times n$ matrices over a field $F$. Suppose that there is a subring of $M_n(F)$ isomorphic to $M_m(F)$ for some $m$. Prove that $m$ divides $n$.

Proof.

R9s3. Two polynomials $f, g \in R[x]$ over a commutative ring $R$ are called coprime over $R$ if $f$ and $g$ generate the unit ideal in $R[x]$. Let $f, g \in \mathbb{Z}[x]$ be two polynomials such that $f$ and $g$ are coprime over $\mathbb{Q}$ and the residues of $f$ and $g$ in $(\mathbb{Z}/p)[x]$ are coprime for every prime integer $p$. Prove that $f$ and $g$ are coprime over $\mathbb{Z}$.

Proof. Let $\frac{a}{b_1} f + \frac{a}{b_2} g = 1$, where $a_i, b_i \in \mathbb{Z}$ and $(a_i, b_i) = 1$. Let $s = b_1b_2 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where the $p_i$ are distinct primes. Then $a_1b_2f + a_2b_1g = s$.

Since (the residues of) $f$ and $g$ in $(\mathbb{Z}/p_i)[t]$ are coprime, there exists $c_i, d_i \in \mathbb{Z}$ such that $c_i f + d_i g = 1 + p_i h_i$, where $h_i \in R[x]$.

Since $p_1^{\alpha_1}$ and $p_2^{\alpha_2}$ are coprime, there exists $m_1, n_1 \in \mathbb{Z}$ such that $m_1p_2^{\alpha_2} + n_1p_1^{\alpha_1} = 1$, by the Euclidian algorithm. Then $m_1p_2^{\alpha_2}(c_1 f + d_1 g) + n_1p_1^{\alpha_1}(c_2 f + d_2 g) = 1 + p_1^{\alpha_1} p_2^{\alpha_2} k_2$, for some $k_2 \in R[x]$. We collect the coefficients of $f$ and $g$ as $u_2$ and $v_2$, respectively. Inductively, since $r_i = p_1^{\alpha_1} \cdots p_i^{\alpha_i}$ and $p_{i+1}^{\alpha_{i+1}}$ are coprime, there exists $m_i, n_i \in \mathbb{Z}$ such that $m_i p_{i+1}^{\alpha_{i+1}} + n_i r_i = 1$, by the Euclidian algorithm. Then
Let $D$ be a noetherian ring and $I$ any ideal of $R$. Prove that there exist prime ideals $p_1, \ldots, p_m$ of $R$ such that
\[ p_1 p_2 \cdots p_m \subset I. \]
Proof. Let $X$ be a collection of ideals that does not contain a finite product of prime ideals. Suppose, towards a contradiction, that $X$ is nonempty. Then as $R$ is noetherian, there is a maximal element $J$ with respect to inclusion. Obviously $J$ is not prime and is proper, thus there are $a, b \not\in J$ but $ab \in J$. Notice then that the ideals $(J,a)$ and $(J,b)$ properly contain $J$, and at the same time $(J,a) \cdot (J,b) \subset J$. Thus by maximality, each of them contain a finite product of prime ideals. But then the product of these two products give a finite product of prime ideals contained in $J$, a contradiction. □

R7f1. Let $F$ be a field and $A$ be a commutative $F$-algebra. Suppose $A$ is of finite dimension as a vector space of $F$.

(a) Prove that if $A$ is a domain, $A$ is a field.

Proof. It is obvious that a finite-dimensional vector space is artinian. Let $x \in A$ with $x \neq 0$. Notice that $(x) \supset (x^2) \supset \ldots \supset (x^n) \supset \ldots$ is a descending chain. Thus for some $n$, $(x^n) = (x^{n+1})$. In particular, there exists $y$ such that $x^n = x^{n+1}y$. By cancellation ($A$ a domain), we get $1 = xy$, so $x$ is invertible. □

(b) Prove that even if $A$ is not a domain, there are only finitely many prime ideals of $A$.

Proof. By Qual Problem R5w2, a commutative artinian ring has only finitely many prime ideals. □

R7f2. Let $A$ be a commutative ring with identity, and write $V$ for the set of all prime ideals of $A$. Put $D(x) = \{ p \in V : x \notin p \}$ for $x \in A$. Prove

(a) $D(a) = D(a^n)$ for integers $n > 0$.

Proof. Since $a \in p \iff a^n \in p$ by induction, the result follows. □

(b) $V = D(a) \cup D(b) \cup D(c)$ if $a^3 + b^3 + c^3$ is invertible in $A$.

Proof. Suppose not, and $p \in V$ is not in $D(a) \cup D(b) \cup D(c)$. Then $p$ contains $a$, $b$, and $c$, hence $a^3 + b^3 + c^3$, an invertible, hence $p = A$, a contradiction. □

Remark. The $D(x)$, $x \in A$, are known as principal open sets and form a basis of open sets in the Zariski topology.

R7f3. Determine all isomorphism classes of modules over the polynomial ring $\mathbb{F}_2[x]$ which are of dimension 2 over $\mathbb{F}_2$. Here $\mathbb{F}_2$ is a field of two elements.

Proof. See Qual Problem R2s3. Here instead of order 8 we have order 4, which gives $(\mathbb{F}_2[x]/x)^2$, $(\mathbb{F}_2[x]/(x+1))^2$, and the $\mathbb{F}_2[x]/f$ where $f$ is any of the four polynomials of degree 2. □

R.1. R7s1. Let $D$ be a division ring (a ring with identity in which every nonzero element is invertible). Let $R = M_n(D)$ be the ring of $n \times n$ matrices with entries from $D$. Prove that $R$ has no two-sided ideals other than $R$ itself and $\{0\}$. 
Proof. Let $I$ be a nonzero two-sided ideal. Then there exists a nonzero element $A \in I$. That is, there exists a position $(i, j)$ such that $A(i, j) \neq 0$. Let $E_k(a, b) = \delta_{ak}\delta_{bk}$ be a $(0, 1)$-matrix with only a single 1 at position $(k, k)$. Then $B = E_iAE_j \in I$ is a matrix with only one nonzero entry $x$ at $(i, j)$. Since $x \in D$ has an inverse, multiplying $B$ by the diagonal matrix $x^{-1}I$ gives a $(0, 1)$-matrix with only one 1 at position $(i, j)$. Now apply permutation matrices to move the 1 to any arbitrary position. It is obvious that these matrices generate $R$. \[\square\]

R.2. R7s2. Let $R = \text{End}(V)$ be the ring of all linear endomorphisms of an infinite dimension complex vector space $V$ with countable basis $\{e_1, e_2, \ldots\}$. Prove that $R$ and $R \oplus R$ are isomorphic as left $R$-modules.

Proof.

R.3. R7s3.

(a) Give a description of all maximal ideals of the ring $\mathbb{C}[x, y]$. You may use the Nullstellensatz.

Proof. By the Nullstellensatz, since $\mathbb{C}$ is algebraically closed, $m$ is a maximal ideal if and only if there exists $a, b \in \mathbb{C}$ such that $m = (x - a, y - b)$. \[\square\]

(b) Let $m = (x^2 - y, y^2 - 5)$ be an ideal in $R = \mathbb{Q}[x, y]$. Prove that $m$ is a maximal ideal.

Proof. First notice that $m = (x^2 - y, x^4 - 5)$. It suffices to show that $R/m$ is a field. To that end, consider a polynomial $f$ in $R$. It is obvious that it has a form $\bar{f} = a_0 + a_1x + a_2x^2 + \ldots + a_3x^3$ in $R/m$. Suppose $\bar{f} \neq 0$, and consider it as an element in $\mathbb{Q}[x]/(x^4 - 5)$, which is a field as $x^4 - 5$ is irreducible by Eisenstein. Thus there exists a polynomial $g = b_0 + b_1x + b_2x^2 + b_3x^3$ such that $\bar{f}g = 1$ in $\mathbb{Q}[x]/(x^4 - 5)$. This implies $fg = 1$ in $\mathbb{Q}[x, y]/(x^4 - 5, x^2 - y)$, which then means $fg = 1$ in the same ring as well. \[\square\]

R.4. R6f1. Determine all prime ideals in the polynomial ring $\mathbb{Z}[x]$.

Proof. Let $p$ be a prime ideal in $\mathbb{Z}[x]$, then $p \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. The prime ideals in $\mathbb{Z}$ consists of the zero ideal and $p\mathbb{Z}$ for $p$ prime. Thus we may consider the preimages of prime ideals in $\mathbb{Z}$. The preimage of the zero ideal consists of the zero ideal and ideals with only polynomials and no constant terms. The preimage of the ideal generated by $p$ consists of the same ideal and those with polynomials with constant term a multiple of $p$. If there are multiple polynomials, and if any two are relatively prime, then by Euclidean algorithm we can extract a constant term, which is contradictory. Thus a prime ideal with polynomials is either a principal one generated by an irreducible, or generated by $f$ and $p$ where $f$ is irreducible modulo $p$. TODO: More details? \[\square\]

R.5. R6f2. Let $R$ be a noetherian domain. A nonzero element $x$ in $R$ is called a prime element if $(x)$ is a prime ideal. Prove all of the following:

(a) Every nonzero non-unit in $R$ is a product of irreducible elements.
Proof. Let $X$ be the set of nonzero non-units in $R$ that cannot be written as a product of irreducible elements. We will show $X$ is empty. Suppose otherwise, and let $x_0 = x \in X$. Obviously $x$ is not irreducible, otherwise $x = x$ is a (product) decomposition into irreducibles. So there exists $a, b \in R$ such that $x = ab$ with $a, b$ non-units (and obviously nonzero). If both of them have decomposition into irreducibles, and not both $a, b$ admit decompositions into irreducibles, then so does $x$. Thus one of them is in $X$, call it $x_1$. Notice $(x_0) \subset (x_1)$. Repeating, we get a sequence $\{x_i\}$ in $X$ such that $(x_0) \subset (x_1) \subset \ldots \subset (x_n) \subset \ldots$ is an ascending chain in $R$. Since $R$ is noetherian, for some $n$, $(x_n) = (x_{n+1})$. Recall that for some $z$ non-unit, $x_n = zx_{n+1}$. But then if $x_{n+1} \in (zx_{n+1})$, some $w$ gives $x_{n+1} = wzx_{n+1}$. As $R$ is a domain, cancellation gives $1 = wz$, a contradiction to $z$ not a unit. Therefore $X$ is empty, as desired. □

(b) Every nonzero ideal $I \neq R$ in $R$ contains a (finite) product of nonzero prime ideals.

Proof. Follow the proof of Qual Problem R8s3, replacing prime ideals by nonzero prime ideals. □

(c) If every nonzero prime ideal in $R$ contains a prime element then every irreducible element in $R$ is a prime element.

Proof. [You may not use theorems about UFDs.]

R.6. R6f3. Let $R$ be a commutative ring and $M$ a finitely generated $R$-module. Suppose there exists a positive integer $n$ and a surjective $R$-module homomorphism $\varphi : M \to R^n$. Show that $\ker \varphi$ is also a finitely generated $R$-module.

Proof.

R.7. R6s1. Suppose $D$ is an integral domain and suppose that $D[x]$ is a principal ideal domain. Show $D$ is a field.

Proof. Let $a \in D$ be nonzero. It suffices to prove that $a$ is a unit. Consider the ideal $(a, x)$ in $D[x]$. It consists of polynomials whose constant term is in $(a)$. As $D[x]$ is principal, there exists $y$ such that $(y) = (a, x)$. Since $y$ divides $a$, it is a constant, hence is in $(a)$. Since $y$ is a constant dividing $x$, it must be a unit. Thus there is a unit in $(a)$, and hence $a$ is also a unit. □

R.8. R6s2. Let $R$ be a commutative noetherian ring with unit, and suppose $M$ is a finitely generated $R$-module. Suppose $f : M \to M$ is an $R$-module homomorphism which is onto. Show that $f$ is an isomorphism.

Proof. Recall that a finitely generated $R$-module is left noetherian. Indeed, recall that if we have a short exact sequence of $R$-modules

$$0 \to M' \to M \to M'' \to 0,$$

then $M$ is noetherian if and only if $M'$ and $M''$ are noetherian. Thus as we have

$$0 \to R^n \to R^{n+1} \to R \to 0,$$

$R^n$ is noetherian (as $R$-module) by induction. If $M$ is finitely generated then there exists $R^n \to M \to 0$. So $M$ is noetherian. This then becomes a special case of Qual Problem R3f2. □
R.9. **R6s3.** Let $R$ be a commutative ring with unit and $\mathfrak{m}$ a maximal ideal of $R$.

(a) Suppose $I_1, \ldots, I_n$ are ideals of $R$ and that

$$\mathfrak{m} \supset I_1 \cdot \ldots \cdot I_n,$$

where $I_1 \cdot \ldots \cdot I_n$ is the product of the ideals. Show

$$\mathfrak{m} \supset I_k$$

for some $k$.

**Proof.** Suppose not, then there exists $a_i \in I_i \setminus \mathfrak{m}$ for each $i$. Now $a_1 \cdot \ldots \cdot a_n \in I_1 \cdot \ldots \cdot I_n \subset \mathfrak{m}$. Since $\mathfrak{m}$ is prime, some $a_i \in \mathfrak{m}$ by induction, a contradiction.

(b) Suppose that $R$ satisfies the descending chain condition (dcc) on ideals, i.e., every strictly decreasing sequence of ideals is finite. Show $R$ has only a finite number of maximal ideals. You may use part (a), but not theorems on the structure of rings satisfying the dcc.

**Proof.** Suppose $\mathfrak{m}_i$ is an infinite family of distinct maximal ideals. Notice that $\mathfrak{m}_1 \supset \mathfrak{m}_2 \supset \ldots \supset \prod_{i=1}^{n} \mathfrak{m}_i \supset \ldots$ is a descending chain. Thus there exists $n$ such that $\prod_{i=1}^{n} \mathfrak{m}_i = \prod_{i=1}^{n+1} \mathfrak{m}_i \subset \mathfrak{m}_{n+1}$. By part (a), $\mathfrak{m}_k \subset \mathfrak{m}_{n+1}$ for some $k \leq n$, contradicting the maximality of $\mathfrak{m}_k$.

R.10. **R5f1.** Let $I$ and $J$ be ideals of a commutative ring $R$ with unit such that $I + J = R$. Prove that $I \cdot J = I \cap J$.

**Proof.** See Qual Problem R2f2-a.

R.11. **R5f2.** Prove that the factor ring $R = \mathbb{R}[x, y]/(y^2 - x^3)$ is not a P.I.D.

**Proof.** A factorial domain is integrally closed. Indeed, let $R$ be factorial, and suppose $\frac{a}{b}$ satisfies $x^n + a_1 x^{n-1} + \ldots + a_n \in R[x]$. Since $R$ is factorial, we may require gcd$(a, b) = 1$, where $= \in$ is up to a unit. Substituting $\frac{a}{b}$ for $x$ and multiplying by $b^n$, we get $a^n + a_1 a^{n-1} b + \ldots + a_n b^n = 0$. Thus $b \mid a^n$ as it divides all other terms. As gcd$(a^n, b) = 1$, we get that $b = 1$ (again, up to a unit), hence $\frac{a}{b} \in R$, and $R$ is integrally closed, as desired.

Notice that $\frac{x}{y}$ satisfies $t^3 - x \in R[t]$, so $\frac{y}{x}$ is integral. Suppose there exists $f \in \mathbb{R}[x, y]$ such that $\frac{a}{b} = f$ in $R$, then $y - x f = 0$ in $R$. That is, $y^2 - x^3 \mid y - x f$ in $\mathbb{R}[x, y]$, which is impossible by degree considerations. Therefore $R$ is not integrally closed. Thus $R$ is not even factorial, much less principal.

R.12. **R5f3.** Let $x, y, z, t$ be elements of a (non-commutative) ring $R$ such that $xz = yt = 1$, $xt = yz = 0$, and $zx + ty = 1$. Prove that the left $R$-modules $R$ and $R \oplus R$ are isomorphic.

**Proof.** Let $f : R \rightarrow R \oplus R$ be given by $f(r) = (rz, rt)$. Notice that $f(x) = (xz, xt) = (1, 0)$ and $f(y) = (yz, yt) = (0, 1)$ give surjectivity. If $f(r) = (rz, rt) = (0, 0)$, then $r = (zx + ty) = r(x + ty) = 0$, giving injectivity.

R.13. **R5w1.** Let $R$ be an integral domain. If $\mathfrak{m}$ is a maximal ideal in $R$, view the localization $R_{\mathfrak{m}} := S^{-1}R$, with $S = R \setminus \mathfrak{m}$, in the quotient field of $R$. Show that

$$R = \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}.$$
Proof. It is obvious that $R \subset R_m$ for any maximal ideal $m$. Conversely, consider $\frac{y}{x}$ in the quotient field of $R$. If $y$ is not invertible in $R$, then $y$ generates a proper ideal, contained in some maximal ideal $m$, hence $\frac{y}{x} \notin R_m$. Otherwise, $y$ is invertible yields $\frac{y}{x} = \frac{xy^{-1}}{1} \in R$, as desired.

Remark. I am uncertain whether this is correct. Indeed, perhaps we should allow $\frac{y}{x}$ to be amplified (by different elements) for each $R_m$.

R.14. **R5w2.** Let $R$ be a commutative Artinian ring. Show that there are only finitely many prime ideals in $R$ and every one of them is maximal.

Proof. Let $p$ be a prime, then $R/p$ is integral and artinian. Recall that $p$ is maximal if and only if $R/p$ is a field. So let $x \in R/p$ be nonzero. It suffice to show that $x$ is a unit. Notice that $(x^n)$ is a descending chain, thus for some $n$, $(x^n) = (x^{n+1})$. Namely, there exists $y$ such that $x^n = x^{n+1}y$. As $R/p$ is integral, by cancellation we get $1 = xy$, as desired. By Qual Problem **R6s3**, there are only finitely many maximal (hence prime) ideals.

R.15. **R5w3.** Let $R \subset A \subset B$ be commutative rings. Suppose that $R$ is noetherian and $B$ is a finitely generated $R$-algebra. Suppose that as an $A$-module $B$ is finitely generated. Show that $A$ is a finitely generated $R$-algebra.

Proof. (See Atiyah–MacDonald §7.) Let $x_1, \ldots, x_m$ generate $B$ as an $R$ algebra, and let $y_1, \ldots, y_n$ generate $B$ as an $A$-module. Then we have $a_{ij}, a_{ijk} \in A$ such that

\begin{align*}
x_i &= \sum_j a_{ij}y_j \quad (1) \\
y_iy_j &= \sum_k a_{ijk}y_k. \quad (2)
\end{align*}

Let $A'$ be an $R$-algebra generated by the $a_{ij}$ and the $a_{ijk}$, thus $R \subset A' \subset A$. An element in $B$ is a polynomial in the $x_i$ with coefficients from $R$. Replacing the $x_i$ using (1) and repeatedly using (2), we write it as a linear combination of the $y_i$ with coefficients from $A'$. Thus $B$ is finitely generated as an $A'$-module. Since $R$ is noetherian, thus so is $A'$, a finitely generated $R$-algebra (Hilbert’s Basis Theorem). Therefore $B$ is a noetherian $A'$-module, as it is finitely generated over a noetherian ring $A'$. Thus $A$ is finitely generated as an $A'$-module, as it is a submodule of a noetherian $A'$-module $B$. But since $A'$ is finitely generated as an $R$-algebra, we conclude that $A$ is also finitely generated as an $R$-algebra.

R.16. **R4f1.** Let $X$ be a finite set and let $A$ be the ring of all functions from $X$ to the field $\mathbb{R}$ of real numbers. Prove that an ideal $m$ of $A$ is maximal if and only if there is an element $x \in X$ such that

\[ m = \{ f \in A : f(x) = 0 \}. \]

Proof. Let $x \in X$ and $m = \{ f \in A : f(x) = 0 \}$. Now $m$ is maximal if and only if $A/m$ is a field. Take $f \in A \setminus m$. Then $f(x) \neq 0$, thus we may define $g(y)$ to be $1/f(x)$ if $x = y$ and 0 otherwise. Then $(fg)(x) = f(x)g(x) = 1$, so $fg$ is 1 modulo $m$.

Conversely, let $m$ be maximal and suppose, towards a contradiction, that $m$ does not vanish on any $x \in X$. Then for each $x \in X$, there is $f_x \in m$ such that $f_x(x) \neq 0$. Define $g_x(y)$ to be $1/f_x(x)$ if $x = y$ and 0 otherwise. Then $f_xg_x$ is 1 on $x$ and 0
otherwise. Since \( m \) is an ideal, \( f_x g_x \in m \). But it is apparent that the \( f_x g_x \) for \( x \in X \) generate \( A \), so \( m \) is not proper, a contradiction. \( \square \)

R.17. **R4f2.** Describe all \( n \in \mathbb{Z} \) such that the ring \( \mathbb{Z}/n \) has no idempotents other than 0 and 1.

**Proof.** Suppose \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) where the \( p_i \) are distinct primes and \( \alpha_i \geq 1 \). For \( e \in \mathbb{Z} \), if \( e^2 = e \) in \( \mathbb{Z}/n \), then \( e(e-1) \in n\mathbb{Z} \), that is, \( n \mid e(e-1) \). Since \( p_i \) is prime, it cannot divide both \( e \) and \( e-1 \). Thus either \( p_i^{\alpha_i} \mid e \) or \( p_i^{\alpha_i} \mid e-1 \). So for each idempotent \( e \), we have a set \( I \subset \{1, \ldots, k\} \) such that \( a = \prod_{i \in I} p_i^{\alpha_i} \mid e \) and \( b = \prod_{j \in J} p_j^{\alpha_j} \mid e-1 \), where \( J = \{1, \ldots, k\}\setminus I \). Notice that two different choices of \( I \) cannot yield the same idempotent. The point is to show that any choice of \( I \) does indeed yield an idempotent. Then we will have a bijection between the idempotents and the power set of \( \{1, \ldots, k\} \). Notice that \( a \) and \( b \) are coprime, hence by the Chinese Remainder Theorem, we have an isomorphism \( \mathbb{Z}/n \cong \mathbb{Z}/a \times \mathbb{Z}/b \). That \( a \mid e \) and \( b \mid e-1 \) gives a unique pair in \( \mathbb{Z}/a \times \mathbb{Z}/b \), hence a unique \( e \in \mathbb{Z}/n \). Thus we have precisely \( 2^k \) idempotents in \( \mathbb{Z}/n \). Therefore \( \mathbb{Z}/n \) has no idempotents other than 0 and 1 if and only if \( n \) is a prime power. \( \square \)

R.18. **R4f3.** A (non-commutative) ring \( R \) is called local if for every \( a \in R \) either \( a \) or \( 1-a \) is invertible. Prove that non-invertible elements of a local ring form a (two-sided) ideal.

**Proof.** Let \( R \) be a local ring and \( m \) the set of non-invertible elements. If \( m \in m \) and \( r \in R \), then \( mr \in m \). Indeed, if \( mr \) were invertible, then \( m(r(mr)^{-1}) = 1 \), making \( m \) invertible. Similarly for \( rm \). It remains to check that \( m \) is closed additively, that is, if \( a, b \in m \), then \( a+b \in m \). Indeed, if \( a+b \) were invertible, then it has inverse \( y \), yielding \( ay + by = 1 \), so either \( ay \) or \( by \) is invertible (\( R \) local), a contradiction. \( \square \)

**Remark.** The converse is also true. Furthermore, \( m \) is both the unique maximal left and right ideal, hence it is two-sided. Moreover, if \( R \) is commutative, then conversely if \( R \) admits a unique maximal (two-sided) ideal then \( R \) is local. But this is not true in general, see Qual Problem R2w2 for an example, where there is a unique maximal two-sided ideal, but infinitely many maximal left ideals.

R.19. **R4s1.** Let \( R \) be a commutative noetherian ring with unity 1 and \( f : R \rightarrow R \) a surjective ring homomorphism, i.e., \( f(1) = 1 \). Show \( f \) is an isomorphism.

**Proof.** Recall that \( R \) is noetherian means \( R \) is a noetherian (left) \( R \)-module over itself. Thus this is a special case of Qual Problem R3f2. \( \square \)

R.20. **R4s2.** Let \( R \) be the ring \( \mathbb{Q}[x] \) and let \( M \) be the submodule of \( R^2 \) generated by the elements \( (1-2x, -x^2) \) and \( (1-x, x-x^2) \). According to the theory of modules over principal ideal domains, \( R^2/M \) is a direct sum of cyclic \( R \) modules of the form \( R/P(x) \) for monic polynomials \( P(x) \). Find such a direct sum decomposition explicitly in this case.
Proof. Consider the exact sequence \( 0 \to M \to R^2 \to R^2/M \to 0 \). We put the matrix associated with \( \alpha \) in Smith Normal Form and take the kernel to get a decomposition of \( R^2/M \) as a direct sum of cyclic modules. The calculation gives
\[
\begin{pmatrix}
1 - 2x & 1 - x \\
-2x + x^2 & x - x^2
\end{pmatrix} \sim \begin{pmatrix}
-1 & 1 - 2x \\
-2x + x^2 & -x^2
\end{pmatrix} \sim \begin{pmatrix}
1 & 0 \\
2x - x^2 & -2x + 4x^2 - 2x^3
\end{pmatrix}.
\]
Hence \( R^2/M \cong R/(x - 2x^2 + x^3) \). \( \square \)

R.21. R4s3. Suppose we are given a collection of polynomials in \( r \) variables with rational coefficients:
\[ f_1, \ldots, f_N \in \mathbb{Q}[T_1, \ldots, T_r]. \]
We define the complex algebraic set \( V_C \subseteq \mathbb{C}^r \) by
\[ V_C = \{(a_1, \ldots, a_r) : f_i(a_1, \ldots, a_r) = 0 \text{ for all } i \text{ from } 1 \text{ to } N\}. \]
Suppose \( V_C \) is not empty. Show that there is a finite extension \( K \) of \( \mathbb{Q} \) and a point \( (a_1, \ldots, a_r) \in V_C \) with all \( a_k \in K \).

Proof.

R.22. R3f1.

(a) Let \( R \) be a commutative ring with 1. Suppose \( f \in R[x] \) is a nonzero 0-divisor in the polynomial ring \( R[x] \). Assume that \( R \) has no nonzero nilpotent elements. Show there is a nonzero element \( a \in R \) so that \( a \cdot f = 0 \).

Proof. Let \( f(x) = a_0 + a_1 x + \ldots + a_n x^n \) be a zero divisor in \( R[x] \). Let \( g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_m x^m \in R[x] \) such that \( g(x) f(x) = 0 \) and \( g \neq 0 \) has the minimal degree. Now it is clear that the coefficient of \( x^{n+m} \) is \( a_n c_m = 0 \). Since \( gf = 0 \), we also have \( a_n g f = 0 \). But \( a_n g = a_n c_0 + \ldots + a_n c_{m-1} x^{m-1} \) since the coefficient of \( x^m \) is \( a_n c_m = 0 \). Now \( a_n g \) is another polynomial that kills \( f \). By minimality of the degree of \( g \), we conclude that actually \( a_n g = 0 \). That is, \( a_n c_i = 0 \) for all \( i \leq m \). Therefore \( (f(x) - a_n x^n)g = 0 \), and thus \( (a_0 + a_1 x + \ldots + a_n x^{n-1})g = 0 \). By repeating this process \( n \) more times, we get that \( a_n c_m = 0 \) for all \( i \leq n \), as desired. \( \square \)

(b) Give an example of an \( R \) and \( f \) so that all coefficients of \( f \) are 0-divisors in \( R \), but \( f \) is not a 0-divisor in \( R[x] \).

Proof. Let \( R = \mathbb{Z}/6 \) and \( f(x) = 2x + 3 \). By above, we need only test to see if \( a \cdot f = 0 \) for some \( a \neq 0 \), which does not happen. \( \square \)

R.23. R3f2. Let \( R \) be a ring, not necessarily commutative, and \( M \) a noetherian left \( R \)-module. Suppose \( f : M \to M \) is a surjective \( R \)-module map from \( M \) to \( M \). Prove that \( f \) is an isomorphism.

Proof. Consider the ascending chain \( \ker(f) \subseteq \ker(f^2) \subseteq \ldots \subseteq \ker(f^n) \subseteq \ldots \) in \( M \). As \( M \) is noetherian, there exists some \( n \) such that \( \ker(f^n) = \ker(f^{n+1}) \). Let \( x \in \ker(f) \). Since \( f \) is surjective, by induction, there exists \( y \in M \) such that \( f^n(y) = x \). Therefore \( f^{n+1}(y) = f(x) = 0 \), so \( y \in \ker(f^{n+1}) = \ker(f^n) \), and thus \( x = f^n(y) = 0 \), yielding \( \ker(f) = 0 \), as desired. \( \square \)
(a) Let \( R \) be a commutative ring with 1, and \( S \) a multiplicatively closed subset of \( R \) not containing 0. Suppose \( I \) is an ideal of \( R \) maximal with respect to exclusions of \( S \) (i.e., \( I \cap S \) is empty and \( I \) is largest such). Prove that \( I \) is a prime ideal of \( R \).

Proof. [The statement is obviously false if \( S \) is empty.] Let \( I \) be maximal with respect to exclusions of \( S \). Suppose, towards a contradiction, that \( I \) is not prime. Then there exists \( a, b \notin I \) such that \( ab \in I \). Consider the ideal \( (I, a) \) generated by \( I \) and \( a \). As \( I \) is properly contained in \( (I, a) \), by maximality of \( I \), we have \( s \in S \cap (I, a) \). Similarly \( t \in S \cap (I, b) \). Notice \( (I, a)(I, b) \subset (I, ab) = I \), hence \( st \in I \). But as \( S \) is multiplicatively closed, \( st \in S \) as well, a contradiction. \( \Box \)

(b) Show that every prime ideal of \( R \) arises as in part (a).

Proof. Let \( \mathfrak{p} \) be a prime ideal. Let \( S = R \setminus \mathfrak{p} \). Notice that \( S \) is multiplicatively closed (and obviously does not contain 0). Indeed, if \( a, b \in S \), then \( a, b \notin \mathfrak{p} \), hence \( ab \notin \mathfrak{p} \) as \( \mathfrak{p} \) is prime. Then \( \mathfrak{p} \) is obviously maximal with respect to exclusions of \( S \). \( \Box \)

R.25. R3w1. Give an example of two integral domains \( A \) and \( B \) which contain a field \( F \) such that \( A \otimes_F B \) is not an integral domain.

Proof. Let \( A = B = \mathbb{F}_p(x) \), and let \( F = \mathbb{F}_p(x^p) \). Consider \( \alpha = 1 \otimes x - x \otimes 1 \). Since it is in characteristic \( p \), we have Freshmen’s dream, that is, \( \alpha^p = (1 \otimes x)^p - (x \otimes 1)^p = 1 \otimes x^p - x^p \otimes 1 = 0 \). Thus \( \alpha \) is nilpotent, thus \( A \otimes_F B \) is not integral. \( \Box \)

R.26. R3w2. Let \( \mathbb{F}_q \) be the finite field of \( q \) elements, and put \( F = \mathbb{F}_q \) and \( K = \mathbb{F}_{q^2} \).

Write \( \sigma : K \rightarrow K \) for the field automorphism given by \( x^q = x^q \). Let

\[ B = \left\{ \begin{pmatrix} a & b \\ db^\sigma & a^\sigma \end{pmatrix} : a, b \in K \right\} \]

for a given \( d \in F^\times \). Prove the following three facts:

(a) \( B \) is a subalgebra of dimension 4 over \( F \) inside the \( F \)-algebra of 2x2 matrices over \( K \).

Proof. Throughout this problem, we will denote \( \begin{pmatrix} a & b \\ db^\sigma & a^\sigma \end{pmatrix} \) simply by \( (a, b) \). It suffice to check closure of \( B \). By direct computation, we have \( (a, b) + (c, e) = (a + c, b + e) \), using \( (a + c)^q = a^q + c^q \). Recall that elements of \( \mathbb{F}_q \) satisfy \( x^q - q \). Thus \( d^q = d \), and for \( a \in K \), \( (a^q)^q = a \). Using these facts, direct computation yields \( (a, b) \cdot (c, e) = (ac + dbe^\sigma, ae + bc^\sigma) \). Finally, for \( c \in F \), \( c(a, b) = (ca, cb) \), as \( c^q = c \). Thus \( B \) is closed. For its dimension, notice that \( B \) has \( q^4 \) elements while \( F \) has \( q \). \( \Box \)

(b) \( B \) is a division algebra if and only if there exists no \( c \in K \) such that \( d = cc^\sigma \).

Proof. Recall that \( (a, b) \) is invertible if and only if its determinant \( a^{q+1} - db^{q+1} \) is nonzero. Suppose \( (a, b) \neq 0 \) is non-invertible, then \( a^{q+1} = db^{q+1} \). Since \( b \neq 0 \) (lest \( a = 0 \), a contradiction), we may divide and get \( (ab^{-1})^{q+1} = d \). Thus \( c = ab^{-1} \) satisfy \( d = c^{q+1} \). Conversely, if \( d = c^{q+1} \), then \( (c, 1) \) has zero determinant, thus \( B \) is not division. \( \Box \)

(c) \( B \) cannot be a division algebra.
Proof. Notice that for each \( c \in K \), \( c^{q+1} \) satisfy \( x^q - x \) (recall \( c^{q^2} = c \)), thus \( c^{q+1} \in F \). Consider the map \( f : K \to F \) defined by \( c \mapsto c^{q+1} \). By part (b), it remains to show that \( f \) is surjective. Since \( F \) is a field, \( \ker f \) is trivial. Furthermore, besides that, each fibre has size at most \( q+1 \), since it is the solution set of \( x^{q+1} - d \), \( d \in F \), some polynomial of degree \( q+1 \). As such, the preimage of \( F \) under \( f \) has size at most \((q+1)(q-1)+1 = q^2 = |K| \). Obviously the preimage should be the entirety of \( K \), this proves that each fibre attains the maximal size, and in particular, \( f \) is surjective. \( \square \)

R.27. **R3w3.** Let \( A \) be a discrete valuation ring with maximal ideal \( \mathfrak{m} \), and define

\[ B = \{(a,b) \in A \times A : a \equiv b \mod \mathfrak{m}\} \]

Prove the following facts:

(a) \( B \) has only one maximal ideal.

Proof. \( a \)

(b) \( B \) has exactly two non-maximal prime ideals.

Proof. \( b \)

R.28. **R2f1.** Let \( R \) be a commutative ring with 1, and let \( S = R[x] \) be the polynomial ring in one variable. Suppose \( \mathfrak{m} \) is a maximal ideal of \( S \). Prove that \( \mathfrak{m} \) cannot consist entirely of 0-divisors.

Proof. By Qual Problem **R3f1**, a nonzero polynomial \( f \) is a 0-divisor if and only if there is some \( a \in R \) such that \( a \cdot f = 0 \), that is, the coefficients are all killed by the same element. Thus \( x \) is not a 0-divisor as 1 is not. Suppose, towards a contradiction, that \( \mathfrak{m} \) only has 0-divisors. Then \( x \notin \mathfrak{m} \), hence \((\mathfrak{m},x) = S \) by maximality. As such, there exists \( m \in \mathfrak{m} \) and \( f \in S \) such that \( m + fx = 1 \). But then the constant term of \( m \) is 1, unbecoming of a 0-divisor. \( \square \)

R.29. **R2f2.** Let \( R \) be a commutative ring with 1, and suppose \( I \) and \( J \) are ideals of \( R \) so that \( I + J = R \). Show that:

(a) \( IJ = I \cap J \).

Proof. It is obvious that \( I \cdot J \subseteq I \cap J \). Conversely, since \( I + J = R \), there exists \( a \in I \) and \( b \in J \) such that \( a + b = 1 \). If \( x \in I \cap J \), then \( x = x \cdot 1 = x(a + b) = ax + xb \in I \cdot J \), as desired. \( \square \)

(b) \( R/IJ \cong R/I \oplus R/J \).

Proof. Let \( f : R \to R/I \oplus R/J \) be given by \( r \mapsto (r + I, r + J) \), the product of the projection maps. Since \( I + J = R \), we have some \( a \in I \) and \( b \in J \) such that \( a + b = 1 \). Notice that \( a \mapsto (0,1) \) and \( b \mapsto (1,0) \). As such, \( f \) is surjective. Its kernel is obviously \( I \cap J \), so by part (a), and the first isomorphism theorem, we are done. \( \square \)

R.30. **R2f3.** Let \( R \) be a commutative ring with 1, and let \( S = R[x] \) be the polynomial ring in one variable. Let \( f \in S \). If \( f \) is a unit of \( S \) (that is, \( f \) is invertible in \( S \)), show that \( f \) has the form \( f = u + g \) where \( u \) is a unit in \( R \) and \( g \in S \) is a nilpotent element without constant term.
Proof. By Qual Problem R13, if \( f = a_0 + a_1 x + \ldots + a_n x^n \) is invertible in \( S \), then \( a_0 \) is invertible and the \( a_i \) are nilpotent, \( i \geq 1 \). By the binomial theorem, \( g = a_1 x + \ldots + a_n x^n \) is nilpotent. \( \square \)

R.31. R2s1. Let \( R \) be a ring and \( A \) and \( B \) be two non-isomorphic simple, left \( R \)-modules (a left-module is simple if it has no proper submodules, i.e., submodules other than \( \{0\} \) and itself). Show that the only proper submodules of \( M = A \oplus B \) are \( \{(\alpha, 0) : \alpha \in A\} \) and \( \{(0, \beta) : \beta \in B\} \).

Proof. Let \( N \subseteq M \) be a proper submodule. Then \( N \cap A \) is a submodule of \( A \), hence is either \( 0 \) or \( A \). Thus \( N \) is either disjoint from \( A \) or contains \( A \). Similarly for \( B \). If \( N \) is disjoint from both, then \( N \) is zero and not proper. If \( N \) contains both, then \( N = M \) is also not proper. Thus \( N = A \) or \( N = B \), which are different as \( A \) and \( B \) are non-isomorphic. \( \square \)

R.32. R2s2. Let \( R \) be a commutative local ring, that is, \( R \) has a unique maximal ideal \( \mathfrak{m} \).

(a) Show that if \( x \) lies in \( \mathfrak{m} \), then \( 1 - x \) is invertible.

Proof. Let \( x \in \mathfrak{m} \). If \( 1 - x \) is non-invertible, then the ideal it generates is proper, hence is in some maximal ideal, namely \( \mathfrak{m} \). But then \( \mathfrak{m} \) contains the sum of \( x \) and \( 1 - x \), namely \( 1 \), and is not proper, a contradiction. \( \square \)

(b) Show that if \( R \) is noetherian and \( I \) is an ideal satisfying \( I^2 = I \), then \( I = 0 \).

Proof. Suppose, towards a contradiction, that \( I \neq 0 \). As \( R \) is noetherian, \( I \) is finitely generated. (Indeed, otherwise we would have a non-stationary infinite chain \( (x_1) \subset (x_1, x_2) \subset \ldots \) by progressively adding generators of \( I \).) Let \( I = (x_1, \ldots, x_m) \), with \( m \geq 2 \) minimal. Since \( I^2 = I \), we have \( x_1 = \sum_{i=2}^m m_i x_i \) for \( m_i \in I \). Then \( (1 - m_1) x_1 = \sum_{i=2}^m m_i x_i \). But \( 1 - m_1 \) is invertible by part (a), so \( x_1 = (1 - m_1)^{-1} \sum_{i=2}^m m_i x_i \), contradicting the minimality of \( n \). \( \square \)

R.33. R2s3. Let \( \mathbb{F}_2 \) be the field with 2 elements and let \( R = \mathbb{F}_2[X] \). List, up to isomorphism, all \( R \)-modules of order 8.

Proof. Since \( \mathbb{F}_2 \) is a field, \( R \) is principal. As such, the fundamental theorem of finitely generated modules over PID gives us unique isomorphism classes. A finite module is the direct sum of \( R/a_i \), \( i = 1, \ldots, n \), where \( a_1 \mid a_2 \mid \ldots \mid a_n \), where the \( a_i \) are polynomials of degree \( d_i \geq 1 \). The order of the module is \( 2^d \), where \( d = \sum d_i \). As such, the possible cases are \( d_1 = d_2 = d_3 = 1; d_1 = 1, d_2 = 2 \); and \( d_1 = 3 \). The first one gives \( (R/x)^3 \) or \( (R/(x + 1))^3 \); the second one gives \( R/x \oplus R/x^2 \), \( R/x \oplus R/(x(x + 1)) \), \( R/(x + 1) \oplus R/(x + 1)^2 \), or \( R/(x + 1) \oplus R/(x(x + 1)) \); while the last gives \( R/a \) where \( a \) is the 8 polynomials of degree 3. \( \square \)

R.34. R2w1. Let \( F \) be a field and \( A \) be a commutative \( F \)-algebra. Suppose \( A \) is of finite dimension as a vector space of \( F \).

(a) Prove all prime ideals of \( A \) are maximal.
Proof. Notice that the submodules of $A$ are its vector subspaces, so $A$ is artinian. By Qual Problem R5w2, primes ideals in an artinian ring are maximal.

(b) Prove that there are only finitely many maximal ideals of $A$. By Qual Problem R6s3, there are only finitely many maximal ideals in an artinian ring.

R.35. R2w2. Let $A = M_n(F)$ be the ring of $n \times n$ matrices with entries in an infinite field $F$ for $n > 1$. Prove the following facts:

(a) There are only 2 two-sided ideals of $A$.

Proof. Since a field is a division ring, by Qual Problem R7s1, $A$ has only the trivial two-sided ideals. □

(b) There are infinitely many maximal left ideals of $A$.

Proof. Notice that for $x, y \in A$, $Ax = Ay$ implies the row spaces of $x$ and $y$ are the same, which in turn implies the null spaces are the same. Contrapositively, if $x$ and $y$ have different null space, then $Ax \neq Ay$ are different left ideals. If, moreover, the null spaces are 1-dimensional, then the left ideals are maximal. But there are infinitely many 1-dimensional subspaces, as $F$ is infinite. □

R.36. R2w3. Let $F_2$ be the field with 2 elements and $A = F_2[T, \frac{1}{T}]$ for an indeterminate $T$. Prove the following facts:

(a) The group of units in $A$ is generated by $T$.

Proof. It is obvious that $\langle T \rangle \subset A^\times$. Conversely, let $x$ be a unit. An element of $A$ is of the form $a_n(T^n) + \cdots + a_1(T) + a_0$ for some $a_i \in F_2$. Factoring out $(\frac{1}{T})^n$, we can write each element as $f/T^n$ for $f \in F_2[T]$ and for some suitably large $n$. Thus if $x = f/T^n$ is a unit, then there exists $g/T^m, g \in F_2[T], m \geq 0$ such that $fg/T^{n+m} = 1$, that is, $fg = T^{n+m}$. But then that means $f$ is $T^k$ for some $k$. So $x = T^{k-n}$ is a power of $T$. As $x$ was arbitrary, we conclude that $A^\times \subset \langle T \rangle$, as desired. □

(b) There are infinitely many distinct ring endomorphisms of $A$.

Proof. It is easy to check that $T \mapsto T^n$ (and $\frac{1}{T} \mapsto (\frac{1}{T})^n$) is a ring endomorphism of $A$ for any $n$, and that they are distinct for different $n$. □

(c) The ring automorphism group $\text{Aut}(A)$ is of order 2.

Proof. A ring automorphism induces a group automorphism of $A^\times \cong Z$. Automorphisms of $Z$ are given by $1 \mapsto \pm 1$. As such, we have either the identity map or $T \mapsto \frac{1}{T}$. It is obvious that each one extends uniquely to a ring automorphism of $A$ (as $F_2$ is fixed), thus $\text{Aut}(A)$ is of order 2. □

R.37. R1f1. Let $R$ be a commutative ring, $I \subset R$ a nonzero ideal. Prove that if $I$ is a free $R$-module then $I = aR$ for an element $a \in R$ which is not a zero divisor in $R$. 
Proof. Let $I$ be a free $R$-module, thus it has a minimal generating set $E \subset R$. Then $E$ is a basis, that is, every element in $I$ can be written uniquely as a linear combination of elements of $E$. If $a, b \in E$ are distinct, then $ba + 0b = 0a + ab$, a contradiction. Thus $E = \{a\}$ is a singleton, hence $I = Ra$. If $a$ is a zero divisor, then there exists nonzero $b \in R$ such that $ba = 0 = 0a$, a contradiction. □

R.38. R1f2.

(a) Give an example of a prime ideal in a commutative ring that is not maximal.

Proof. Take an integral domain that is not a field, say $\mathbb{Z}$. Then the zero ideal is prime (there are no zero divisors), but is not maximal (a nonunit generate a nonzero proper ideal).

(b) Let $R$ be a commutative ring with identity. Suppose for every element $x \in R$ there exists an integer $n = n(x) > 1$ such that $x^n = x$. Show that every prime ideal in $R$ is maximal.

Proof. Let $\mathfrak{p}$ be a prime ideal, and take $x \in R \setminus \mathfrak{p}$. Let $\bar{x}$ be the projection of $x$ in $R/\mathfrak{p}$. As $R/\mathfrak{p}$ is integral, $\bar{x}^n = \bar{x}$ gives $\bar{x}^{n-1} = 1$, thus $\bar{x}$ is invertible. Hence $R/\mathfrak{p}$ is a field, thus $\mathfrak{p}$ is maximal. □

Remark. Since this problem is so elementary, perhaps we should not hide behind the (equally elementary) fact that $R/\mathfrak{p}$ is integral, and that $R/\mathfrak{p}$ is a field if and only if $\mathfrak{p}$ is maximal. We may unravel the wonders explicitly: As $x^n = x$, we get $x(x^{n-1} - 1) = 0 \in \mathfrak{p}$, yielding $x^{n-1} - 1 \in \mathfrak{p}$. Thus $(\mathfrak{p}, x)$ contains both $x^{n-1}$ and $x^n - 1$, thus containing 1 and is not proper. Since this holds for any $x \notin \mathfrak{p}$, we conclude that $\mathfrak{p}$ is maximal.

R.39. R1f3. Let $R$ be a ring. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial in $R[x]$ of degree $n$, that is $a_n \neq 0$.

(a) Prove that if $a$ is a nilpotent element in a ring $R$ with identity, then the element $1 + a$ is invertible.

Proof. As $a$ is nilpotent, there exists some $k \geq 0$ such that $a^{k+1} = 0$. Notice that $(1 + a) \cdot (1 - a)(1 + a^2)(1 + a^4) \cdot \ldots (1 + a^{2^k}) = 1 - a^{2^{k+1}} = 1$, hence $1 + a$ is invertible. □

(b) Show that if $R$ is an integral domain, then $f(x)$ is invertible in $R[x]$ if and only if $n = 0$.

Proof. By part (c) below, if $f$ is invertible, then $a_i$ is nilpotent for $i \geq 1$. In particular, if $n > 0$, then $a_n$ is nilpotent. But as $R$ is integral, there are no nonzero nilpotents, hence $a_n = 0$, a contradiction. Thus $n = 0$. The converse statement is false: $f$ is invertible if and only if $f \in R^\times$. □

(c) Show that if $R$ is a commutative ring, $f(x)$ is invertible in $R[x]$ if and only if $a_0$ is invertible and all $a_i$ are nilpotent in $R$ for every $i \geq 1$.

Proof. Suppose $a_0$ is invertible and all $a_i$ are nilpotent for $i \geq 1$. It is clear that the $a_i x^i$ are nilpotent for $i \geq 1$ as well. Therefore $f - a_0$ is nilpotent by the Binomial Theorem. Now $a_0^{-1}(f - a_0)$ is also nilpotent, so $1 + a_0^{-1}(f - a_0)$ is invertible by part (a). Multiplying by $a_0$, we get that $f$ is invertible.

Conversely, suppose $f$ is invertible and take $g = c_0 + c_1 x + \ldots + c_m x^m$ as above. We may obviously assume $n > 0$. It is obvious that the constant
term is \(a_0c_0 = 1\), hence \(a_0\) is invertible. It remains to show that the \(a_i\) are nilpotent for \(i \geq 1\). We claim that for \(r \leq m\), \(a_i^{r+1}c_j = 0\) for \(j \geq m - r\). Proceed by induction on \(r\). When \(r = 0\), \(a_n c_m\) is the coefficient of \(x^{n+m}\) in \(gf\) hence is zero. Now look on the coefficient of \(x^{n+m-r}\) in \(gf\). It is \(a_n c_m + a_{n-1} c_{m-1} + \ldots + a_{m-r} c_m\), which is zero (we adopt the convention that \(a_0 = 0\) for \(i < 0\)). Now multiplying by \(a_n^r\) we get \(a_n^{r+1}c_m + a_{n-1} a_n c_{m-r+1} + \ldots + a_{m-r} a_n c_m = 0\). All the summands beside the first one is zero by induction, hence \(a_n^{r+1}c_m = 0\), as desired. Therefore we know that \(a_n^{m+1}c_0 = 0\), which implies that \(a_n^{m+1} = 0\) since \(c_0\) is invertible. We have concluded that \(a_n\) is nilpotent. Of course, then \(a_n x^n\) is also nilpotent, hence as above, \(f - a_n x^n\) is still invertible. By induction on the degree of \(f\) (or by doing this \(n - 1\) more times, taking the minimum counter-example, etc.), we are done. \(\square\)

**R.40. R1s1.** A commutative ring \(R\) with unit is said to be a local ring if it has a unique maximal ideal. Show that a commutative ring \(R\) with unit is a local ring if and only if for any two elements \(u, v \in R\) satisfying \(u + v = 1\) at least one of \(u, v\) is a unit of \(R\).

**Proof.** Let \(R\) be local with maximal ideal \(m\). If \(u\) is not a unit, then \(Ru\) is proper, hence is contained in \(m\). In particular, the non-units are all in \(m\). Let \(u, v \in R\) satisfying \(u + v = 1\). If \(u, v\) are not units, then \(1 = u + v \in m\), a contradiction.

Conversely, if for all \(u \in R\), at least one of \(u\) and \(1 - u\) is a unit, then by Qual Problem **R4f3**, the non-units form an ideal \(m\). Since proper ideals do not contain units, any proper ideal is contained in \(m\), hence \(m\) is the unique maximal ideal. \(\square\)

**R.41. R1s2.** Let \(R = \mathbb{R}[x, y]\). Find a finitely generated \(R\)-module \(M\) that is not a direct sum of cyclic \(R\)-modules.

**Proof.**

**R.42. R1s3.** Let \(f_1(z_1, \ldots, z_n), f_2(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n)\) be \(n\) polynomials in \(\mathbb{C}[z_1, \ldots, z_n]\). Assume that \(f_i(0, 0, \ldots, 0) = 0\) for all \(i = 1, \ldots, n\). Prove that the origin is the only point of \(\mathbb{C}^n\) where all of the \(f_i\) vanish if and only if the ideal \(I\) generated by \(f_1, \ldots, f_n\) contains all monomials of degree \(N\) for some sufficiently large \(N\).

**Proof.** Let \(V(I)\) be the affine variety, that is, \(V(I) = \{\bar{x} = (x_1, \ldots, x_n) \in \mathbb{C}^n : f(\bar{x}) = 0, f \in I\}\). First notice that \(V(I)\) is also the common zero set of the \(f_i\). If \(I\) contains \(z_i^N\), then \(I\) can only vanish at \(\bar{x}\) if \(x_i = 0\). Thus \(V(I)\) consists only of the origin. Conversely, if \(V(I)\) consists only of the origin, then \(z_i\) vanishes on \(V(I)\). Thus by the Nullstellensatz, there exists some \(N\) such that \(z_i^N \in I\). \(\square\)

**R.43. R0f1.** Let \(M\) be a module over a commutative ring \(A\). If every strictly increasing (resp., decreasing) sequence of \(A\)-submodules of \(M\) terminates after finite steps, the \(A\)-module \(M\) is called noetherian (resp., artinian).

(a) Prove that the \(\mathbb{Z}\)-module \(\mathbb{Z}\) is noetherian and not artinian.
Proof. Recall that a ring $R$ is noetherian if and only if it is noetherian as an $R$-module. Furthermore, since $\mathbb{Z}$ is principal, it is noetherian as a ring, hence noetherian as a $\mathbb{Z}$-module. It is not artinian as the descending chain of submodules $2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \ldots \supset 2^n\mathbb{Z} \supset \ldots$ is not stationary. □

(b) Prove that the $\mathbb{Z}$-module $M = \bigcup_{n=1}^{\infty} (p^{-n}\mathbb{Z}/\mathbb{Z})$ is artinian and not noetherian.

Proof. Notice that $p^{-1}\mathbb{Z}/\mathbb{Z} \subset p^{-2}\mathbb{Z}/\mathbb{Z} \subset \ldots \subset p^{-n}\mathbb{Z}/\mathbb{Z} \subset \ldots$ provide an ascending chain of submodules that is not stationary. Now consider a descending chain of submodules $q_1^{-1}\mathbb{Z}/\mathbb{Z} \supset q_2^{-1}\mathbb{Z}/\mathbb{Z} \supset \ldots q_n^{-1}\mathbb{Z}/\mathbb{Z} \ldots$. Notice that if $q_2^{-1}\mathbb{Z}/\mathbb{Z} \subset q_1^{-1}\mathbb{Z}/\mathbb{Z}$, then $q_2 | q_1$. So in general, we have a descending chain of integers $q_i$ one dividing the previous one. This must be stationary at some point. Equivalently, if we have strict inclusion, then this must terminate. Therefore $M$ is artinian. □

R.44. R0f2. Let $A$ be a commutative ring with indentity. Suppose that $a \in A$ is not nilpotent (that is, $a^n \neq 0$ for all $n > 0$).

(a) Prove that there exists a prime ideal $p \subset A$ such that $a \notin p$.

Proof. Let $S = \{1, a, a^2, \ldots, a^n, \ldots\}$. Notice that $S$ is a multiplicative subset not containing 0. Let $p$ be an ideal of $A$ maximal with respect to exclusions of $S$. This $p$ exists as 0 is one such ideal. Then by Qual Problem R3f3, $p$ is prime. □

(b) Give an example of a ring $A$ and a non-nilpotent $a \in A$ such that $a$ is contained in $m$ for all maximal ideals $m \subset A$.

Proof. Consider the ring of formal power series $\mathbb{Q}[x]$. This is a local ring with maximal ideal generated by $x$, which is a non-nilpotent element. □

R.45. R0f3. Let $A$ be a commutative noetherian ring with identity $1 \neq 0$. Write $V(a)$ for the set of prime ideals of $A$ containing a given ideal $a$. Suppose that $V(0) = V(a) \cup V(b)$ and $V(a) \cap V(b) = \emptyset$ for two ideals $a$ and $b$. Prove the following facts:

(a) $A = a + b$.

Proof. We will prove a (seemingly) stronger statement that $A = a^n + b^n$ for $n \geq 1$. Let $I = a^n + b^n$, and suppose, towards a contradiction, that it is proper. Then by Zorn, there exists a maximal ideal $m$ containing $I$. But maximal ideals are prime ideals, so $m \supset a^n$ contains $a$. Similarly for $b$, a contradiction to the disjointness of $V(a)$ and $V(b)$. □

(b) $a \cap b = ab$.

Proof. Use $a + b = 1$, $a \in a$, $b \in b$ to write $x \in a \cap b$ as $ax + xb \in ab$ (See Qual Problem R2f2). □

(c) The ideal $ab$ consists of nilpotent elements.

Proof. Notice $x \in ab \subset a \subset \bigcap V(a)$, and similarly for $b$. So if $x \in ab$ then $x$ is in the intersection of all prime ideals (which is the nilradical). If $x$ is not nilpotent, then by Qual Problem R0f2-a, some prime does not contain $x$. Thus $ab$ consists of nilpotent elements, that is, $ab$ is a nil ideal. □

(d) There exists a positive integer $n$ such that $A$ is isomorphic to the product ring $(A/a^n) \times (A/b^n)$.
Proof. In a commutative noetherian ring, nil ideals are nilpotent. [Indeed, let $I$ be a nil ideal. As $A$ is noetherian, $I$ is finitely generated, say, by $E = \{x_1, \ldots, x_m\}$. For each $i$, we have $n_i \geq 1$ such that $x_i^{n_i} = 0$. Let $n = \sum_{i=1}^{m} n_i$ and $y_1, \ldots, y_n \in I$. Write each $y_i$ as linear combination of the $x_i$, and expand $y_1 \leq \cdots \leq y_n$. Each monomial has degree (in $E$) at least $n$, hence by the pigeon hole principle, some $x_i^{n_i}$ occurs, forcing each monomial to be zero, thus yielding $I^n = 0$, as desired.]

By part (c), $ab$ is nil, thus there exists $n \geq 1$ such that $(ab)^n = 0$. Furthermore, by part (a), $a^n$ and $b^n$ are coprime. Thus by the Chinese Remainder Theorem (see Qual Problem R2F2), $A \cong A/a^n b^n \cong A/a^n \times A/b^n$. □

R.46. R0s1. List, up to isomorphism, all commutative rings with 4 elements.

Proof. Let $(R, +, \cdot)$ be a commutative ring with 4 elements. Then $(R, +)$ is an abelian group of order 4. By the fundamental theorem of finitely generated abelian groups, this is either $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$. In the former case, $\cdot$ is forced. In the latter, write $1, a, 1 + a$ as the three elements of (additive) order 2. Recall that in a ring, 0 and 1 are distinguished, and multiplication involving those are forced. The remainder of the multiplication table is determined completely by value of $a^2$, which can be 0, 1, $a$, or $1 + a$. Since $a$ and $1 + a$ are indistinguishable algebraically, the case $a^2 = 0$ forcing $(1 + a)^2 = 1$ is isomorphic with $a^2 = 1$ forcing $(1 + a)^2 = 0$. This is obviously distinct from the cases $a^2 = a$ and $a^2 = 1 + a$. We can then check that these indeed define ring structures by checking the (finitely many) required relations by hand. Thus we get 4 isomorphism classes of rings with 4 elements. □

R.47. R0s2. Let $p$ be a prime number. Show that a free $\mathbb{Z}$-module of rank 2 has $p + 1$ submodules of index $p$.

Proof. Recall that a $\mathbb{Z}$-module is simply an abelian group. Thus this problem asks to find the number of subgroups of index $p$ in the free abelian group $\mathbb{Z}^2$. By Qual Problem G7s2 or Qual Problem G2w1, we have that the number is $(p^2 - 1)/(p - 1) = p + 1$, as desired. □

R.48. R0s3. Let $R$ be a commutative noetherian ring in which each ideal $I$ is principal and satisfies $I^2 = I$. Show that $R$ is isomorphic to a finite product of fields.

Proof.