1. (Jan-06.2) Let \( R \) be the subring of \( \mathbb{Z}[x] \) consisting of all polynomials with zero \( x \)- and \( x^2 \)-coefficients.

   (a) Show that \( \mathbb{Q}(x) \) is the field of fractions of \( R \).

   (b) Find the integral closure of \( R \) in \( \mathbb{Q}(x) \).

   (c) Does there exist a polynomial \( g(x) \in R \) such that \( R \) is generated as a ring by 1 and \( g(x) \)?

**Solution:**

\( a) \) Clearly \( \mathbb{Q}(x) \), the field of fractions of \( \mathbb{Z}[x] \), contains the field of fractions of \( R \). Conversely, \( x \) and 1 are in the field of fractions of \( R \), because \( x = \frac{x^2}{x^3} \), so the field of fractions of \( R \) contains the field of fractions of \( \mathbb{Z}[x] \).

\( b) \) The integral closure is \( \mathbb{Z}[x] \) – this ring is integrally closed since it is a UFD, so we need only show that the integral closure of \( R \) contains \( \mathbb{Z}[x] \). But \( x \) is in the integral closure, since it is a root of \( p(t) \) where \( p(t) = t^3 - x^3 \in R[t] \), hence by integrality properties, \( \mathbb{Z}[x] \) is contained in the integral closure.

\( c) \) No: if there were such a polynomial, then \( x^3 \) and \( x \) would necessarily be polynomials in \( g(x) \), hence \( \deg(g) \) divides 3 and 4, hence would have to be 1, but no polynomial of degree 1 is in \( R \).

\( c-alt) \) No: if there were, then \( R \) would be isomorphic to \( \mathbb{Z}[g(x)] \cong \mathbb{Z}[y] \), but the latter is integrally closed while \( R \) is not.

---

2. (Aug-09.2/Jan-08.2a) Let \( R \subseteq S \) be commutative rings with the same 1, and assume that every element of \( S \) is integral over \( R \).

   (a) If \( r \in R \) has an inverse in \( S \), prove this inverse is in \( R \).

   (b) Suppose \( R \) is a field and \( s \in S \) is regular (i.e., if \( sx = 0 \) for some \( x \in S \), then \( x = 0 \)). Show that \( s \) is invertible in \( S \).

   (c) If \( P \) is a prime ideal of \( S \), prove that \( P \) is maximal in \( S \) iff \( R \cap P \) is maximal in \( R \).

**Solution:**

\( a) \) Since \( u = r^{-1} \) is integral over \( R \), it satisfies a monic polynomial with coefficients in \( R \): \( u^n + a_{n-1}u^{n-1} + \cdots + a_1u + a_0 = 0 \). Now multiply by \( r^{n-1} \) to obtain \( u + a_{n-1}r + a_{n-2}r^2 + \cdots + a_0r^{n-1} \), whence \( u = -a_{n-1} - a_{n-2}r - \cdots - a_0r^{n-1} \in R \).

\( b) \) By hypothesis \( s \) is integral over \( R \), so again we can write \( s^n + b_{n-1}s^{n-1} + \cdots + b_0 = 0 \) for some monic polynomial of minimal degree. If \( b_0 = 0 \) then we would have \( s(s^{n-1} + \cdots + b_1) = 0 \) so by regularity we would have \( s^{n-1} + \cdots + b_1 = 0 \), contradicting minimality. Hence \( b_0 \neq 0 \); then we may write \( s(s^{n-1} + \cdots + b_1) = -b_0 \), so since \( R \) is a field we can divide by \( -b_0 \) to see \( s \cdot \left[ -\frac{s^{n-1} + \cdots + b_1}{b_0} \right] = 1 \), so \( s \) is invertible.

\( c) \) By passing to the quotient, we know that every element of \( S/P \) is integral over \( R/(R \cap P) \).

\( \Rightarrow \): If \( P \) is maximal in \( S \), let \( \bar{r} \in R/(R \cap P) \) be nonzero. Then \( \bar{r} \) is invertible in \( S/P \) since \( S/P \) is a field and \( r \notin P \). So by part (a), \( \bar{r} \) is invertible in \( R/(R \cap P) \), hence the latter is a field and \( R \cap P \) is maximal in \( R \).

\( \Leftarrow \): If \( R \cap P \) is maximal in \( R \), then \( R/(R \cap P) \) is a field and \( R/P \) is a domain since \( P \) is prime. Hence every nonzero element of \( R/P \) is regular, so by part (b) \( R/P \) is a field and \( P \) is maximal.
3. (Jan-01.3) Let \( f(x) \in \mathbb{Z}[x] \) be monic and such that \( f(\alpha) = f(2\alpha) = 0 \) for some \( \alpha \in \mathbb{C} \).

(a) Show that \( f(0) \neq 1 \).

(b) If \( f \) is irreducible, prove \( \alpha = 0 \).

**Solution:**

a) Since \( f \) is monic, all its roots \( r_1, \ldots, r_n \) are algebraic integers, with \( r_1 = \alpha \) and \( r_2 = 2\alpha \). Then \( \frac{1}{2} f(0) = \frac{1}{2} (-1)^n r_1 r_2 \cdots r_n = (-1)^n \alpha^2 r_3 \cdots r_n \) is a product of algebraic integers hence also an algebraic integer. Since it is also a rational number, it is an integer. We conclude that \( f(0) \) is an even integer, so it is not 1.

b) Consider \( \gcd(f(x), f(2x)) \); it has positive degree since \( x - \alpha \) divides both terms, hence since \( f \) is irreducible it must equal \( f(x) \). Since \( f(x) \) and \( f(2x) \) have the same degree, the latter is a scalar multiple of the former. We conclude that if \( \beta \) is a root of \( f \), then so is \( 2\beta \), meaning that \( \alpha, 2\alpha, 4\alpha, \ldots \) are all roots of \( f \). Since \( f \) has finite degree, it must be the case that \( \alpha = 0 \).

**Remark** Part (b) is showing that multiplication by 2 is an element of the Galois group of \( f \). Examples of such irreducible \( f \) exist in any positive odd characteristic: for example, over \( \mathbb{F}_3 \), the irreducible polynomial \( p(x) = x^2 + 1 \) has roots 1 and \( 2i = -i \), where \( i^2 = -1 \) in \( \mathbb{F}_3 \).

4. (Aug-12.5) Let \( R \) be a not necessarily commutative ring with 1, such that \( x^5 = x \) for every \( x \in R \).

(a) Show that \( J(R) = 0 \).

(b) Now assume \( R \) is right-Artinian. Prove that \( R \) is a direct sum of division rings.

(c) Let \( D \) be a division ring direct summand of \( R \). If \( F \) is any subfield of \( D \), show that \( F = \mathbb{F}_2, \mathbb{F}_3, \) or \( \mathbb{F}_5 \).

(d) Deduce that \( D \) above is isomorphic to \( \mathbb{F}_2, \mathbb{F}_3, \) or \( \mathbb{F}_5 \), and conclude that \( R \) is commutative.

**Solution:**

a) If \( y \in J \), then \( 1 - syr \) is a unit for any \( s, r \in R \), so in particular \( 1 - y^4 \) is a unit. Since \( 0 = y - y^5 = y(1 - y^4) \), multiplying by the inverse of \( 1 - y^4 \) yields \( y = 0 \).

b) A right-Artinian ring has a finite number of maximal right ideals \( m_1, \ldots, m_k \), as otherwise \( m_1, m_1 \cap m_2, \ldots \) would yield an infinite increasing chain of right ideals. Now since the Jacobson radical is the intersection of the maximal right ideals of \( R \), part (a) implies that \( \bigcap m_k = 0 \). Now by the Chinese Remainder Theorem, we see that \( R \cong \bigoplus \langle R/m_k \rangle \), since by maximality it must be the case that \( m_i + m_j = R \) for any \( (i, j) \), and so \( \bigcap m_j = \bigcap m_j = 0 \). Finally, \( R/m_k \) is a division ring.

b-alt) By the Artin-Wedderburn theorem, we see that \( R \) is a direct sum of matrix rings over division rings: \( R \cong \bigoplus M_k(k \langle D_i \rangle) \). But the Jacobson radical is only zero if all of the matrix rings are 1-dimensional since (for example) there are nilpotent elements in a \( k \times k \) matrix ring if \( k > 1 \).

c) Suppose \( F \) is a field in which \( x^5 - x = 0 \) for all \( x \in F \). By unique factorization we see that \( |F| \leq 5 \), and so \( |F| \) can only be 2, 3, 4, or 5. It is then trivial to see that \( |F| = 2, 3, 5 \) work, but \( |F| = 4 \) does not work.

d) Let \( F \) be the subfield generated by 1 in \( D \). If \( z \in D \) is any element of \( D \), then \( F(z) \) is commutative hence also a subfield of \( D \), but by part (c) it must be the case that \( F(z) = F \), so \( z \in F \) hence \( D = F \). Thus, \( R \) is a direct sum of fields hence commutative.

**Remark** This is a special case of a theorem, due to Jacobson, that if \( R \) is such that \( x^n(x) = x \) for every \( x \in R \) (where the exponent can depend on \( x \)), then \( R \) is commutative.
5. (Aug-04.2) Let $R$ be a ring with 1, $M$ be a finitely-generated (right) $R$-module, and $N \subset M$ a proper submodule of $M$.

(a) Prove that there exists a maximal submodule of $M$ containing $N$.
(b) Show that $N + MJ$ is a proper submodule of $M$, where $J = J(R)$ is the Jacobson radical of $R$.

Solution:

a) This is the module version of Krull’s lemma (that a commutative ring with 1 contains a maximal ideal). Let $\Sigma$ be the set of proper submodules of $M$ containing $N$, partially ordered by inclusion; it is nonempty since it contains $N$. If $C : M_1 \subset M_2 \subset \cdots$ is a chain, we claim $M' = \bigcup M_i$ is an upper bound and a proper submodule of $M$. It is clearly an upper bound, and it is proper since otherwise it would necessarily contain each of the generators of $M$ at some finite stage, but then one of the $M_i$ would necessarily equal $M$, contradiction. Hence Zorn’s lemma gives a maximal element, as desired.

b) This is Nakayama’s lemma. Without loss of generality we can replace $N$ with the maximal submodule $K$ from part (a); then the result is equivalent to showing that $K + MJ$ is proper, which is in turn equivalent to showing that $MJ$ is contained in $K$—i.e., that $MJ$ is contained in every maximal submodule of $M$. This last statement is equivalent to the more usual statement of Nakayama’s lemma, which says that if $M$ is finitely-generated and $M/MJ = 0$ then $M = 0$: to prove it, suppose that $n$ is the smallest possible number of generators $m_1, \ldots, m_n$ of $M$ and write $m_n = r_1m_1 + \cdots + r_nm_n$ with the $r_j \in J$; then $m_n(1 - r_n) = r_1m_1 + \cdots + r_{n-1}m_{n-1}$, but now since $r_n \in J$ we know that $1 - r_n$ is a unit (else $1 - r_n$ would be contained in some maximal ideal of $R$ hence in $J$, but then $r_n + (1 - r_n) = 1$ would be in $J$, contradiction) hence $m_n$ is in the span of $m_1, \ldots, m_{n-1}$. This is a contradiction since then $m_1, \ldots, m_{n-1}$ would generate $M$.

6. (Aug-06.2) Let $R$ be a ring with 1 and $N$ a nil ideal of $R$ such that $R/N$ has no zero divisors.

(a) Show that the only idempotents of $R$ are 0 and 1.
(b) If $R/N$ is a division ring, show that every zero divisor in $R$ is nilpotent.

Solution:

a) Suppose $e^2 = e$ in $R$ so that $e(1 - e) = 0$. Passing to $R/N$ shows that $\bar{e} \cdot (1 - \bar{e}) = 0$ in $R/N$, so since $R/N$ has no zero divisors we see that $e$ or $1 - e$ is in $N$. But then since $N$ is a nil ideal, $e^n = 0$ or $(1 - e)^n = 0$ for some $n$, and since $e^2 = e$ and $(1 - e)^2 = (1 - e)$ a trivial induction shows $e = 0$ or $1 - e = 0$, hence $e = 0$ or $e = 1$.

b) Suppose $x \in R$ has $\bar{x} \neq 0$ in $R/N$ (which is to say, $x \notin N$). Then since $R/N$ is a division ring, $\bar{x}$ has a left inverse $\bar{y}$, so there exists $y$ with $xy = 1 + n$ for some $n \in N$. But then $xy(1 - n + n^2 + \cdots + (-n)^k) = 1$ where $n^k = 0$, so $x$ has a left inverse. Symmetrically, we see $x$ has a right inverse, so it is a unit. Hence every nonunit is contained in $N$, so in particular every zero divisor is nilpotent.
7. (Jan-14.1): Let $R$ be a commutative ring and $I$ an ideal of $R$.

(a) Show that the radical of $I$, $\text{rad}(I)$, is an ideal of $R$. (Recall that the radical is given by the set of all elements $x \in R$ such that there exists an integer $n$ such that $x^n \in I$.)

(b) Give an example of an ideal $I$ in $\mathbb{Q}[x, y]$ such that $I$ is non-principal but $\text{rad}(I)$ is principal.

(c) Suppose we try to define $\text{rad}(0)$ in $R = M_{2 \times 2}(\mathbb{R})$ to be the set of all elements $r \in R$ such that there exists an integer $n$ with $r^n = 0$. Show that this set $\text{rad}(0)$ is not an ideal of $R$.

Solution:

a) Suppose $r \in R$ and $x, y \in \text{rad}(I)$, so that $x^n \in I$ and $y^m \in I$. Then $(rx)^n = r^n x^n \in I$, and $(x+y)^{m+n} \in I$, since after expanding with the binomial theorem we see that each term has an $x^m$ or $y^m$ (and these are in $I$). Also, $0 \in \text{rad}(I)$, so we see $\text{rad}(I)$ is nonempty and closed under addition and $R$-multiplication.

b) One example is $I = (x^2, xy)$: it is nonprincipal because any generator would necessarily divide both $x^2$ and $xy$ hence divide their gcd $x$, but $I$ contains no polynomials of degree less than 2. But then $\text{rad}(I) = (x)$: clearly $\text{rad}(I)$ contains $x$ since $x^2 \in I$, and since $I \subset (x)$ we see $\text{rad}(I) \subseteq \text{rad}(x)$, but since $(x)$ is prime, it equals its radical.

c) This set is not closed under addition or multiplication: \( \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \) and \( \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \) are both nilpotent, but neither their sum nor their product (in either order) is.

c-alt) A matrix ring over a field is a simple ring, so the only two-sided ideals of $R$ are 0 and $R$, but the set $\text{rad}(0)$ is neither of those.

8. (Aug-08.2) Let $S = \mathbb{Z} \oplus \mathbb{Z}$, and $R = \{(a, b) \in S : a \equiv b \mod 6\}$.

(a) Show that $R$ is a finitely-generated $\mathbb{Z}$-module and conclude that $R$ is a Noetherian ring.

(b) Prove that the ideal $P = \{(a, 0) \in R : a \equiv 0 \mod 6\}$ is prime in $R$.

(c) If $Q$ is a primary ideal of $R$ with $P = \text{rad}(Q)$, show that $Q = P$.

Solution:

a) It is easy to see that $R = \{(a, a+6k), a, k \in \mathbb{Z}\}$, so $R$ is generated by $(1, 1)$ and $(0, 6)$. Since $\mathbb{Z}$ is Noetherian, so is $R$.

a-alt) $S$ is a Noetherian $\mathbb{Z}$-module, so any submodule (e.g., $R$) is Noetherian as well, and a Noetherian module is finitely-generated.

b) Suppose $(a, b) \cdot (c, d) = (6t, 0)$; then one of $b, d$ is zero. By interchanging, we can assume $b = 0$; then since $(a, b) \in R$ we see $a \equiv 0 \mod 6$, so $(a, b) \in P$. So $P$ is prime.

b-alt) Observe that the homomorphism $\varphi : R \to \mathbb{Z}$ sending $(a, b) \mapsto b$ is surjective and has kernel $P$. The first isomorphism theorem then says $R/P \cong \mathbb{Z}$, which is an integral domain.

c) If $P = \text{rad}(Q)$ then $Q$ is contained in $P$, and also there is some element $(a, b) \in Q$ with $(a, b)^n = (6, 0) \in P$ but this forces $(a, b) = (6, 0)$ so $(6, 0)$ hence all of $P$ is in $Q$ so $Q = P$.

c-alt) In fact this result holds if $P$ is any principal prime ideal $(x)$: if $P = \text{rad}(Q)$, we need only see that $x \in Q$: since $x \in P = \text{rad}(Q)$, there is some $y \in Q$ with $y^n = x \in P$. But since $P$ is prime, a trivial induction shows $y \in P$ whence we conclude $x \in Q$. 


9. (Jan-12.2) Let $R$ be a commutative ring with 1 and $Q$ be a primary ideal of $R$. Suppose that $Q = \bigcap X_i$ is a finite intersection of the ideals $X_i$.

(a) If each $X_i$ is prime, prove that $Q = X_j$ for some $j$. [Hint: Show that $Q$ is prime.]
(b) If $R$ is Noetherian and each $X_i$ is primary, and the radicals of the $X_i$ are distinct, prove again that $Q = X_j$ for some $j$.

Solution:

a) We claim that $Q$ is prime. To see this suppose $xy \in Q$. Then since $Q$ is primary we know that $x \in Q$ or $y^n \in Q$. In the latter case we have $y^n \in X_i$ for all $i$, but then since each $X_i$ is prime (hence equal to its radical) we see $y \in X_i$ for all $i$, hence $y \in Q = \bigcap X_i$. We conclude that if $xy \in Q$ then $x \in Q$ or $y \in Q$, meaning $Q$ is prime.

The result then follows from: if $Q$ is a prime ideal and $Q = \bigcap X_i$ is a finite intersection of ideals, then some $X_i = Q$. If any $X_i$ contains the intersection of the others, we can throw it away without changing anything. If after we do this we are left with only one $X_i$ then it is equal to $Q$ and we are done. Otherwise, suppose we have 2 or more, and pick $x_k \in X_i \cap \bigcap_{i \neq k} X_i$. Then $x_1 x_2 \cdots x_k \in Q$ whence some $x_j \in Q$ since $Q$ is prime. But this is a contradiction since then $x_j \in X_j$, contrary to our assumption.

b) This follows from the uniqueness part of the primary decomposition theorem: if we reduce this intersection by throwing out ideals contained in the intersection of all the others like in part (a), we get a minimal primary decomposition of $Q$. There is one associated prime for $Q$, namely $\text{rad}(Q)$, so there must be only a single $X_i$ that survives, and it must be equal to $Q$.

b) From taking radicals yields $\text{rad}(Q) = \bigcap \text{rad}(X_i)$, and applying part (a) we see that $\text{rad}(Q) = \text{rad}(X_j)$ for some $j$ and all of the other $\text{rad}(X_j)$ contain elements not in $\text{rad}(X_i)$. Then if we localize $Q$ at the prime ideal $P = \text{rad}(Q)$, because $\text{rad}(X_j) \cap (R \setminus P) \neq \emptyset$ for $j \neq i$, all of the $X_j$ except for $X_i$ are sent to zero. Then taking a contraction shows $Q = X_i$, as desired.

10. (Aug-02.2) Let $R$ be a commutative ring with 1 in which every proper ideal is primary.

(a) If $P$ is a prime ideal and $I$ is any ideal, show that either $I \subseteq P$ or $P = IP \subseteq I$.
(b) If $M$ is a maximal ideal of $R$, show that $M$ is the set of nonunits of $R$.
(c) Show that $J$ is prime in $R$ iff for all $r \in R$, $r^2 \in J$ implies $r \in J$.

Solution:

a) If $I \subseteq P$ we are done, so choose $a \in I \setminus P$ and let $b \in P$ be arbitrary. Then $ba \in IP$ so since $IP$ is primary, either $b \in IP$ or $a^n \in IP$: however it cannot be that $a^n \in IP$ since this would imply $a^n \in P$ and primality of $P$ would give $a \in P$, which is not true. Hence $b \in IP$, so $P \subseteq IP \subseteq P$, whence $P = IP$.

b) By part (a), for every ideal $I$ of $R$, it is either the case that $I \subseteq M$ or $M \subseteq I$. Since $M$ is maximal the latter cannot happen unless $I = M$ or $I = R$, so every proper ideal of $R$ is contained in $M$, hence $R$ has a unique maximal ideal. Then it is standard to see that a local ring (a ring with a unique maximal ideal) has the property that the maximal ideal is the set of nonunits: a nonunit generates a proper ideal (as it doesn’t contain 1) hence the ideal hence the nonunit must be contained in $M$, and no unit is contained in $M$.

c) We only need that $J$ is primary for this part. If $J$ is prime then we immediately have that $r^2 \in J$ implies $r \in J$. Conversely, suppose $J$ is a primary ideal and $xy \in J$. Then either $x \in J$ and we are done, or $y^n \in J$. We claim that $y^n \in J$ implies $y \in J$: this follows by a downward induction on $n$: if $n$ is even then the criterion implies $y n/2 \in J$; if $n$ is odd then the criterion implies $y n(n+1)/2 \in J$, and in either case we see that a lower power of $y$ is in $J$.