A COURSE ON INTEGRAL DOMAINS

ALGEBRA II - SPRING 2004

Updated - March 3, 2004

1. The Fundamental Theorem of Arithmetic

My son who is in the 4^{th} grade is learning about prime numbers and cancelling prime numbers in order to reduce fractions into lowest forms. I have told him that every number (positive integer) can be expressed as a product of primes, and surely along the road, his teachers will confirm this. We will consider this property in integral domains.

We say that a *divides* b in the domain R, and write $a \mid b$, if there exists a $c \in R$ such that $ac = b$.

Definitions . Let R be an integral domain.

- An element u in R is called a *unit*, if for some $v \in R$, $uv = vu = 1$.
- An element $a \in R$ that is not a unit is called *irreducible*, if $a = bc$ for some $b, c \in R$ implies that c or b is a unit in R.
- An element $a \in R$ that is not a unit is called *prime*, if $a \mid (bc)$ for some $c, b \in R$, implies $a \mid b$ or $a \mid c$.

Prime elements are irreducible; if p is prime and $p = ab$ for some $a, b \in R$, then $p \mid ab$ and so $p \mid a$ or $p \mid b$. If $p \mid a$, then $pc = a$ and so $p = ab = pcb$ implying $1 = bc$. Likewise, if $p \mid b$, then a is a unit. However, as well will see in our first theorem, irreducible elements are quite common-place while primes are rare.

We say that an ideal I of R is *finitely generated* if there exist a subset $\{a_1, a_2, \ldots, a_n\}$ of I such that

$$a \in I \implies \exists\, r_1, r_2, \ldots, r_n \in R \text{ such that } a = \Sigma_{i=1}^{n} r_i a_i.$$

In this case we write

$$I = (a_1, a_2, \ldots, a_n).$$

Conversely, given $a_1, a_2, \ldots, a_n \in R$ we can define an ideal I by asserting

$$a \in I \Leftrightarrow \exists\, r_1, r_2, \ldots, r_n \in R \text{ such that } a = \Sigma_{i=1}^{n} r_i a_i,$$

in which case $I = (a_1, a_2, \ldots, a_n)$. Note that for nonzero elements a, b in a domain R, $a \mid b$ if and only if $(b) \subseteq (a)$.

Definition . An integral domain R is called *noetherian* if every ideal is finitely generated.

Proposition 1. *The following are equivalent on an integral domain R:*

(a) *R is noetherian.*
(b) *If $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ are ideals of R, then there is an index m such that $n \geq m$ implies $I_m = I_n$.*
(c) *Any nonempty collection of ideals has a maximal member.*
(d) *A submodule of a finitely generated R-module is itself finitely generated.*

Proof. $(a) \rightarrow (b)$. Given such a chain of ideals, set $I = \cup_n I_n$. Since the ideals $I_1, I_2, \ldots$ form a chain, I is again an ideal (check this!). But I is finitely generated, so there exists a finite generating set $a_1, \ldots, a_n$. For each i, there is an index m_i such that $a_i \in I_{m_i}$. Let

$$m = max\{m_1, m_2, \ldots, m_n\}.$$

Then each $a_j \in I_m$ and so $I = I_m$.

$(b) \rightarrow (c)$. Let $\mathcal{I}$ be any nonempty collection of ideals. Choose $I_1 \in \mathcal{I}$. If I_1 is not maximal among all ideals in $\mathcal{I}$, choose $I_2 \in \mathcal{I}$ that properly contains I_1. Proceeding like this, in order that (b) is not violated, this process must stop, and it terminates in selecting an ideal that is not smaller than any other ideal of $\mathcal{I}$.

$(c) \rightarrow (a)$. Given an ideal I, let $\mathcal{I}$ be the set of all finitely generated ideals J such that $J \subseteq I$. $\mathcal{I}$ has a maximal member J, and if $J \neq I$ there is an element $a \in I \setminus J$ so that $J \subseteq J + (a) \subseteq I$, in contradiction to (c).

$(d) \rightarrow (a)$. R is generated by 1 and so is every submodule of R; i.e., every ideal of R, must be finitely generated.

$(a) \rightarrow (d)$. We know that every ideal of R is finitely generated. We induct on n to show that every submodule of a direct sum of n copies of R, which I'll write as $F = \oplus_n R$, is finitely generated. The induction is easy since if K is a submodule of F and $\pi : F \rightarrow R$ is the projection map onto the first component (i.e., $\pi(r_1, r_2, \ldots, r_n) = r_1$), then we have an exact sequence

$$0 \rightarrow H \rightarrow K \xrightarrow{f} I \rightarrow 0,$$

where f is the restriction of π to K. Since $H \leq \oplus_{n-1} R$, and $I \leq R$, by induction H and I are finitely generated. Therefore, if $x_1, x_2, \ldots, x_n$ are such that $f(x_1), f(x_2), \ldots, f(x_n)$ generate I, and $y_1, y_2, \ldots, y_m$ generate $H = Kernel\ f$, then check that $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m$ generate K. $\square$

Theorem 2. *Suppose every chain of principal ideals of R stabilizes. Then, any nonzero nonunit in R is a product of irreducible elements.*

Proof. Suppose some nonzero, nonunit in R is not a product of irreducible elements. Let $\mathcal{I}$ be the collection of all principal ideals $\{(a) \mid a \text{ is not a product of irreducible elements}\}$. Any chain in $\mathcal{I}$;

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots ,$$

must stabilize (by hypothesis) meaning that for some index m, $(a_j) = (a_m)$ for all $j \geq m$. Therefore, $\mathcal{I}$ contains a maximal element, call it (a).

We cannot have a irreducible by the description of $\mathcal{I}$, so there exist element $b, c \in R$, both non-units, such that $a = bc$. But then (a) is properly contained in both (b) and (c), and so by the choice of (a), both b and c are products of irreducible elements. But $a = bc$ so a is a product of irreducible elements. This contradiction shows that $\mathcal{I}$ must be nonempty. □

Definition . A domain R is called a *unique factorization domain*, or UFD for short, if every nonzero, nonunit can be (uniquely) factored into a product of primes of R.

The uniqueness is provided for free (Mathematicians speak of "paying a price" for a particular hypothesis) for if

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

with p_i, q_j primes, then p_1 divides $q_1 q_2 \cdots q_m$, and so by the obvious (correct) extrapolation, p_1 divides some q_j, which after re-indexing we assume to be q_1. Since q_1 is irreducible, $p_1 = u_1 q_1$ for some unit u_1. After cancelling we obtain

$$p_2 p_3 \cdots p_n = u_1 q_2 q_3 \cdots q_m,$$

and by induction we obtain $n = m$, and after re-indexing, $p_i = u_i q_i$ for some unit $u_i \in R$.

Uniqueness is not assured, in general, for factorizations into irreducibles.

Proposition 3. *The following are equivalent for an integral domain R:*

(a) *R is a UFD.*
(b) (i) *Every non-zero, nonunit of R can be factored into a product of irreducible elements, and*
    (ii) *If $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$ occurs with a_i and b_j irreducible elements, then $n = m$ and after re-indexing $a_i = u_i b_i$ for some units $u_i \in R$.*

Proof. By the remarks after the definition of UFD, it is sufficient to show, under either (a) or (b), that irreducible elements are prime. Assuming (a), any irreducible element r is a product of primes, and so by the definition of irreducible, r must be a single prime. Assuming (b), suppose that an irreducible element s divides a product rt. Say $st' = rt$.

Factoring t', t and r into products of irreducibles, we find by the uniqueness in part (b), that s must be one of the irreducibles factors (up to unit multiple) of either r or t. That is, $s \mid r$ or $s \mid t$. □

A word of caution here: By Theorem 2 and its converse (Exercise 6.), R is a UFD if and only if every proper chain of principal ideals is finite. However, UFD's need not be noetherian or even seem noetherian-like.

Example 4. It is an exercise at the end of the section that when R is a UFD, then so is $R[x]$. Repeating, so is $(R[x])[y] = R[x, y]$, and so is $R[x_1 1, x_2, \dots, x_n]$ for any number of indeterminates $x_1, x_2, \dots, x_n$. By $R[x_1, x_2, \dots]$ we mean the polynomials with coefficients in R that involve only finitely many of the x_j's, so it follows that $R[x_1, x_2, \dots]$ is a UFD as well. The ideal $(x_1, x_2, \dots)$ is obviously not finitely generated.

As a corollary to our theorem, we can deduce the Fundamental Theorem of Arithmetic, as it relates to domains.

The classical approach to studying rings is to view them through their ideals (this is due to Dedekind).

Definitions . Let P and M be ideals of the integral domain R, with $P, M \neq R$.

- P is said to be a *prime* ideal, if for any $r, s \in R$, $rs \in P$ implies $r \in P$ or $s \in P$.
- M is said to be a *maximal* ideal, if for any ideal J containing M, either $J = M$ or $J = R$.

There is an arithmetic that we can perform on ideals. Given ideals I and J, define the addition of the two ideals as

$$I + J = \{a + b \mid a \in I, b \in J\},$$

and the multiplication as

$$IJ = \{x \in R \mid \exists\, n \in \mathbb{Z}^+,\ a_i \in I, b_i \in J, \text{for } i = 1, 2, \dots, n$$
$$\text{such that } x = \Sigma_{i=1}^{n} a_i b_i\}.$$

Certainly IJ contains ab where $a \in I$ and $b \in J$ but the set $\{ab \mid a \in I, b \in J\}$ is not usually closed under $+$ and will not be an ideal in those cases. Later we will consider multiplicative ideal theory.

We will make several observations:

Observation: An ideal $P \neq R$ is prime if and only if for any ideals I, J of R with $IJ \subseteq P$, either $I \subseteq P$ or $J \subseteq P$.

Proof. If P is prime and the ideals I, J are given, with $IJ \subseteq P$ while J and I are both not contained in P, then let $a \in J \setminus P$ and $b \in I \setminus P$. Then $ab \in P$ but $a, b \notin P$, a contradiction. Conversely, if $ab \in P$, then $(a)(b) = (ab) \subseteq P$ implies $a \in (a) \subseteq P$ or $b \in (b) \subseteq P$, so the ideal-theoretic property leads to the elemental property. □

Observation: An ideal $M \neq R$ is maximal if and only if for any $r \in R \setminus M$, $M + (r) = R$.

Proof. If M is maximal and $r \in R \setminus M$, then $M + (r)$ is an ideal properly containing M. Hence $M + (r) = R$. Conversely, if M satisfies $M + (r) = R$ for any $r \in R \setminus M$, and J is an ideal containing M, then either $J = M$, or there exists $r \in J \setminus M$. In the latter case, $R = M + (r) \subseteq J \subseteq R$, and so $J = R$. □

Observation: Maximal ideals are prime.

Proof. If $rs \in M$ and $r \notin M$, then $M + (r) = R$ and so $m + ar = 1$ for some $m \in M$ and $a \in R$. Then, $s = sm + sar \in M$. □

Observation: Every ideal I unequal to R is contained in some maximal ideal M.

Proof. Consider the set $\mathcal{M}$ of all ideals J such that $I \subseteq J$ and $J \neq R$. Then $I \in \mathcal{M}$ so $\mathcal{M}$ is nonempty. If $\{J_\alpha\}_{\alpha<\lambda}$ is a chain of elements from $\mathcal{M}$ (i.e., $\alpha < \beta \Leftrightarrow J_\alpha \leq J_\beta$), then set $J = \cup_{\alpha<\lambda} J_\alpha$. It is easy to see that $J \in \mathcal{M}$. Therefore, by Zorn's Lemma, $\mathcal{M}$ contains a maximal element M. If J is an ideal that contains M and $J \neq R$, then $J \in \mathcal{M}$ and so J must be equal to M by the choice of M. Thus, M is a maximal ideal of R. □

The following are easy exercises:
Show: P is prime if and only if R/P is an integral domain.
Show: M is maximal if and only R/M is a field.
Show: Finite integral domains are fields, so if P is a prime ideal such that R/P is finite, then M is a maximal ideal.

Definition . An integral domain R is called a *principal ideal domain*, or PID for short, if every ideal is principal (i.e., generated by a single element).

Theorem 5. *Any PID is a UFD.*

Proof. Let R be a PID. Since, obviously R is noetherian, any nonzero, nonunit can be factored into a product of irreducible elements by Theorem 2. It remains to show that any irreducible element in a PID is prime.

Let a be an irreducible element, and suppose $a \mid bc$ for some $b, c \in R$. Since a is not a unit, $(a) \neq R$ and so (a) is contained in a maximal ideal M. Write $M = (d)$. Then $a \in (d)$ implies $a = de$ for some $e \in R$, but because a is irreducible, e must be a unit. That is, $(a) = (d) = M$. Since maximal ideals are prime, $bc \in (a)$ implies $c \in (a)$ (i.e., $a \mid c$) or $b \in (a)$ (i.e., $a \mid b$). □

EXERCISES of SECTION 1:

1. Show that if F is a field, then $R = F[x]$ is a PID. Hint: use the degree function $deg : F[x] \to \mathbb{N}$ and the division algorithm in $F[x]$ to show that if $f(x) \neq 0$ is an ideal of smallest degree in an ideal $I \neq 0$, that $I = (f(x))$.
2. Suppose $\alpha \in \mathbb{C}$ is the root to a monic polynomial $f(x) \in \mathbb{Z}[x]$, and put $R = \mathbb{Z}[\alpha]$; the collection of all polynomials in $\mathbb{Z}$ evaluated at α.
   (a) Show that R is an integral domain that is finitely generated over $\mathbb{Z}$.
   (b) Argue that the quotient field of R is $\mathbb{Q}[\alpha]$, and that for any $\beta \in R$, there exists an integer $k \neq 0$ such that $k\beta^{-1} \in R$.
   (c) Using (b), argue that any nonzero ideal of R contains an integer, and so R/I is finite.
   (d) Using (c) conclude that R is a noetherian domain such that every non-zero prime ideal is maximal.
3. Let R be a UFD with quotient field Q, and let $f(x) \in R[x]$.
   (a) Show that there is an element $r \in R$ and a polynomial $g(x) \in R[x]$, such that $f(x) = rg(x)$ and the gcd of the coefficients of $g(x)$ is 1. (r is called the *content of* f and we write $c(f) = r$).
   (b) Show that if $f(x) = g(x)h(x)$ with $g(x), h(x) \in Q[x]$, then there exists polynomials $g_1(x), h_1(x) \in R[x]$ each having content 1, and elements $0 \neq a, a_1, b, b_1 \in R$ such that a, a_1 and b, b_1 are coprime pairs, and $ag(x) = a_1 g_1(x)$ and $bh(x) = b_1 h_1(x)$. Thus, $abf(x) = a_1 b_1 g_1(x) h_1(x)$.
   (c) With the notation of part (b), show that $ab = 1$.
   (d) Conclude that $f(x) \in R[x]$ is irreducible in $R[x]$ if and only if $f(x)$ is irreducible in $Q[x]$.
4. Let R be a UFD. Using Problem 3. show that $R[x]$ is a UFD.

5. The intersection of all maximal ideals of R is called the *Jacobson radical* of R. Suppose $J = \cap_{M\ max} M$.
   (a) Show that $a \in J$ if and only if for every $r \in R$, $1 + ra$ is a unit. Hint: $\Rightarrow$ $ra \in J$ for every $r \in R$, and so $1 + ra$ must be a unit. $\Leftarrow$ $a \notin M$ for some M implies $M + (a) = R$ and $1 - ra \in M$ for some $r \in R$.
   (b) Deduce a version of Nakayama's Lemma: If K is a finitely generated module, that is, $K = Rx_1 + Rx_2 + \cdots + Rx_n$, such that $JK = K$, then $K = 0$. Hint: Assume n is the minimal number of generators required to generate K; write $x_1 = a_1x_1 + \cdots a_nx_n \in JK = K$ with $a_j \in J$ for all j. Invert $1 - a_1$.
   (c) Prove **Nakayama's Lemma:** Let B be a finitely generated module, and let A be a submodule such that $B = A + JB$. Then $B = A$. Hint: $K = B/A$ is finitely generated and satisfies $K = JK$.
6. The *Hilbert Basis Theorem* asserts that if R is noetherian, then so is $R[x]$. Assuming R is a noetherian domain, show that $R[x]$ is noetherian. Hint: If J is an ideal in $R[x]$, let I_n be the ideal of elements that occur as coefficients of x^n in some polynomial in J. Observe that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. Use this to pick generators for J.

2. Integral Closure

When we study domains, a primary tool is the *integral closure* of the domain, and to use it we need to develop it. If we just wish to characterize Dedekind domains, we can be satisfied with a simpler description of the integrally closed property, one that is readily usable. So, we need to balance the two objectives. (That is, the definitions we consider now will be towards a more general perspective in order to accommodate the homework, rather than the definition of integral closure given in class for the purpose of proving our Dedekind domains theorem).

Definitions . An element $t \in Q$ will be said to be *integral over* R if there is a finitely generated (as an R-module) over-ring S of R inside Q which contains t. Given a domain R, an over-ring S of R in the quotient field Q is said to be *integral over* R, if every $t \in S$ is integral over R. If every element in Q that is integral over R belongs to R, then we say that R is *integrally closed*.

Proposition 6. *The following are equivalent for an integral domain R and an element t in a field F containing R:*

(1) *t is integral over R.*
(2) *$R[t]$ is a (module) finitely generated over-ring of R.*
(3) *There is a polynomial $f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$ such that $f(t) = 0$.*

Proof. (2) $\rightarrow$ (1) is obvious. (3) $\rightarrow$ (2) is easy because $t^n = -\Sigma_{j=1}^{n-1} r_j t^j$ implying that $R[t]$ is a ring that is generated as an R-module by $1, t, \ldots, t^{n-1}$.

(1) $\rightarrow$ (3). Let S be a subring of F containing R and t such that $S = Rt_1 + Rt_2 + \cdots + Rt_n$. For each i there exists $r_{ij} \in R$ with j running from 1 to n, such that

$$t \cdot t_i = \Sigma_{j=1}^{n} r_{ij} t_j.$$

Let A be the $n \times n$ matrix whose i, j^{th} entry is r_{ij}. Then, we can rephrase the above equation as the matrix equation

$$AX = tX,$$

where X is the n-tuple $(t_1, t_2, \ldots, t_n)$ (actually, stand X up to multiply). Or, in the other familiar form

$$(A - tI)X = 0,$$

where I is the $n \times n$ identity matrix.

If we let x be an indeterminate, then the determinant of $A - xI$ (computed using cofactor expansion for example), is a monic polynomial of degree n, for which t is a root. This works the same way it always has in undergraduate linear algebra. Therefore, t is a root to $det(A - xI)$, which as you may recall, is equal to $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. □

Here is the definition given in class describing integrally closed.

Corollary 7. *The noetherian domain R is integrally closed if and only if whenever S is an over-ring of R, $S^{-1} = \emptyset$.*

Proof. This is due to the fact that $S^{-1} \neq 0$ (i.e., S is a fractional over-ring) if and only if S is finitely generated:

$0 \neq t \in S^{-1} \Rightarrow tS \subseteq R \Rightarrow S \cong tS$ is a (finitely generated) ideal of R,

and

$$S \text{ finitely generated over } R \Rightarrow S = Rt_1 + \ldots + Rt_n$$
$$\text{for some } t_j \in Q \Rightarrow rS \subseteq R \text{ for some } 0 \neq r \in R$$

(clear the denominators of the t_j's). □

Some well-known examples of integrally closed domains are the rings we have just finished studying.

Example 8. If R is a UFD, then R is integrally closed.

Proof. Suppose $t = r/s \in Q$ is integral over R. We can assume that r/s is in lowest form so that the $gcd(r, s) = 1$ (r, s do not share a prime factor). By the proposition above, t is a root to some $x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$, and so plugging in t and clearing the powers of s from the denominators we have

$$r^n + r_{n-1}sr^{n-1} + \cdots + s^{n-1}r_1r + s^nr_0 = 0.$$

But then

$$s(r_{n-1}r^{n-1} + \cdots + s^{n-2}r_1r + s^{n-1}r_0) = -r^n,$$

and so any prime factor of s must divide r as well. By design, s does not share any primes with r, so s must be a unit, implying $t \in R$. □

A way to create examples of integrally closed domains is to take the widely-understood domain $\mathbb{Z}$, and a field containing $\mathbb{Z}$, and compute the "integral closure" of $\mathbb{Z}$ inside the field.

Example 9. Let F be any field containing $\mathbb{Z}$. The collection of all elements $\alpha \in F$ such that α is a root to some monic polynomial in $\mathbb{Z}[x]$ is integrally closed, and is called the *integral closure of* $\mathbb{Z}$ in F.

Proof. Let R be the collection of all the α's just described. As in the proof of the proposition, $\alpha \in R$ if and only if the ring $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group. If $\alpha, \beta \in R$, then $\alpha\beta$, and $\alpha + \beta$ both belong to $S = \mathbb{Z}[\alpha, \beta] = (\mathbb{Z}[\alpha])[\beta]$.

Something in S looks like

$$f_0(\alpha) + f_1(\alpha)\beta + \cdots + f_k(\alpha)\beta^k$$

for some $f_j(x) \in \mathbb{Z}[x]$. But $\alpha, \beta \in R$ implies that there exists integers n and m such that any $f(\alpha)$ can be generated by $1, \alpha, \ldots, \alpha^{n-1}$ over $\mathbb{Z}$, and any $g(\beta)$ by $1, \beta, \ldots, \beta^{m-1}$ over $\mathbb{Z}$. It follows that any element in S can be generated by

$$1, \alpha^i\beta^j,\ i < n,\ j < m.$$

For example, for $j > m$, one can write $\beta^j = \Sigma_{i=0}^m \ell_{ij}\beta^i$, so that

$$f_0(\alpha) + f_1(\alpha)\beta + \cdots + f_k(\alpha)\beta^k = \Sigma_{i_1=0}^m f_{i_1}(\alpha)\beta^{i_1} +$$

$$\Sigma_{j=m+1}^k [f_j(\alpha)\Sigma_{i=0}^m \ell_{ij}\beta^i].$$

Likewise we can express each $f_i(\alpha)$ exclusively in terms of $1, \alpha, \ldots, \alpha^n$ using integer coefficients. Thus, S is finitely generated and so R is a subring of F.

If $\gamma \in F$ is integral over R, then γ is a root to some $x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$. But $\mathbb{Z}[r_j]$ is finitely generated for each j, from which it follows as above that

$$\mathbb{Z}[r_1, r_2, \ldots, r_{n-1}]$$

is finitely generated over $\mathbb{Z}$ as well. Hence

$$\mathbb{Z}[r_1, r_2, \ldots, r_{n-1}, \gamma]$$

is finitely generated over $\mathbb{Z}$ too and so $\gamma \in R$ to begin with. That is, R is integrally closed. □

Recall that an element α of a field F containing $\mathbb{Z}$ is called *algebraic over* $\mathbb{Z}$ if there exists

$$0 \neq f(x) \in \mathbb{Z}[x] \text{ such that } f(\alpha) = 0.$$

In this case, the *minimal polynomial for* α *over* $\mathbb{Z}$ is the monic polynomial of smallest positive degree in $\mathbb{Q}[x]$ having α as a root. Note, if

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

has α as a root, with $a_n \neq 0$, then so does

$$g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

where $b_j = a_j/a_n$. While there are infinitely many choices for $f(x)$, recall that the monic $g(x)$ is unique provided we are considering the polynomials of smallest degree. Furthermore, it is an easy exercise using long division to show that

$$h(x) \in \mathbb{Q}[x] \text{ with } h(\alpha) = 0 \iff g(x) \mid h(x) \text{ in } \mathbb{Q}[x].$$

Example 10. Let α be in a field F containing $\mathbb{Z}$. The following are equivalent:

(1) α is integral over $\mathbb{Z}$.
(2) α is algebraic over $\mathbb{Z}$ and the monic minimal polynomial for α is in $\mathbb{Z}[x]$.
(3) α is algebraic but is not the root of some polynomial in $\mathbb{Z}[x]$ with leading coefficient greater than 1 while the coefficients are relatively prime.

Proof. (1) $\rightarrow$ (2) is a proof given in class (essentially). Let $g(x) \in \mathbb{Z}[x]$ be the monic polynomial of smallest degree having α as a root (α integral) and let $f(x) \in \mathbb{Q}[x]$ be the monic polynomial of smallest degree having α as a root (clearly, α is algebraic over $\mathbb{Z}$). Performing long division, we can factor $g(x) = f(x)h(x)$ for some monic polynomial $h(x) \in \mathbb{Q}[x]$.

There are positive integers m and n such that $nf(x), mh(x) \in \mathbb{Z}[x]$, and the gcd's of the coefficients of $nf(x)$ and also of $mh(x)$ are both 1 (for example, choose only the smallest n that will make $nf(x) \in \mathbb{Z}[x]$). Then $mng(x) = (nf(x))(mh(x))$. Suppose there is a prime p dividing n. Considering the polynomials "mod p", we obtain

$$0 = \overline{mng(x)} = \overline{nf(x)} \cdot \overline{mh(x)}.$$

(What we mean is that the coefficients of the polynomials are reduced modulo p, which is signified by the bar over the polynomials; formally, we have a ring epimorphism from $\mathbb{Z}[x] \to \mathbb{Z}[x]/p\mathbb{Z}[x]$ given by $y(x) \mapsto y(x) + p\mathbb{Z}[x]$, and the isomorphism $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$ affords the reduction of the coefficients).

But $\mathbb{Z}_p[x]$ is an integral domain, and $\overline{nf(x)} \cdot \overline{mh(x)} = 0$ implies either $\overline{nf(x)} = 0$ or $\overline{mh(x)} = 0$. Neither is possible since the coefficients of $nf(x)$ and of $mh(x)$ are relatively prime. Therefore, $m = 1$ and $g(x) = f(x) \in \mathbb{Z}[x]$.

(2) $\to$ (3). For the moment just assume that α is algebraic. If $f(x) \in \mathbb{Q}[x]$ is the monic polynomial of least degree with α as a root, then for some integer n, $nf(x)$ has the gcd of its coefficients equal to 1. Conversely, if $f_0(x)$ is a polynomial of least degree in $\mathbb{Z}[x]$ with the gcd of its coefficients equal to 1 and α as a root, then $f_0(x)/a \in \mathbb{Q}[x]$ is the monic polynomial for α of least degree where a is the coefficient of the highest power of x in $f_0(x)$. It follows that, under the full force of (2), a has to be 1. Thus, every polynomial in $\mathbb{Z}[x]$ with the gcd of its coefficients equal to 1 and having α as a root must be monic.

(3) $\to$ (1). Again, if $f(x) \in \mathbb{Q}[x]$ is the monic irreducible polynomial for α, and $f(x) \notin \mathbb{Z}[x]$, then we could multiply by an $n > 1$ to obtain a polynomial $nf(x) \in \mathbb{Z}[x]$ such that the gcd of the coefficients is 1. We conclude that $f(x) \in \mathbb{Z}[x]$ and α is integral over $\mathbb{Z}$. □

For example, the following algebraic elements are roots to the given polynomials:

$$\alpha = \sqrt{2+\sqrt{3}} \quad \Longleftrightarrow \quad f(x) = x^4 - 4x^2 + 1,$$

$$\beta = \sqrt[3]{2+3\sqrt{5}} \quad \Longleftrightarrow \quad g(x) = x^6 - 4x^3 - 41,$$

$$\gamma = \sqrt{2+\sqrt{3/5}} \quad \Longleftrightarrow \quad h(x) = 5x^4 - 20x^2 + 17,$$

$$\delta = (\sqrt{2}+\sqrt{3})/(\sqrt{1+\sqrt{2}}) \quad \Longleftrightarrow \quad k(x) = x^8 - 60x^6 + 134x^4 + 60x^2 + 1.$$

From this data and the previous example we find that α, β, δ are integral over $\mathbb{Z}$ while γ is not. To see how to obtain the polynomials,

let us consider obtaining $k(x)$ for δ. Square both sides and eliminate the denominator:

$$\delta^2(1+2+2\sqrt{2}) = 2+3+2\sqrt{6};$$

(legally) remove the square-root on the $\sqrt{6}$ term:

$$(\delta^2(3+2\sqrt{2})-5)^2 = 4(6) = 24;$$

or;

$$(\delta^4(3+2\sqrt{2})^2 - 2(5)\delta^2(3+2\sqrt{2}) + 25 = 24;$$

or;

$$(\delta^4(9+8+12\sqrt{2}) - 20\delta^2\sqrt{2} = -1+30\delta^2;$$

isolate the remaining square-root;

$$\sqrt{2}(12\delta^4 - 20\delta^2) = -1+30\delta^2-17\delta^4;$$

square both sides;

$$2(144\delta^8+400\delta^4-480\delta^6) = 1+900\delta^4+(17)^2\delta^8-1020\delta^6-60\delta^2+34x^4;$$

and since $17^2 = 288+1 = 2(144)+1$, when we replace δ with x, we obtain

$$k(x) = x^8 - 60x^6 + 134x^4 - 60x^2 + 1.$$

3. Localizations and Over-rings of R

Definition . If P is a prime ideal in an integral domain R, then

$$R_P = \{\frac{r}{s} \mid r \in R,\ s \in R \setminus P\},$$

is an over-ring of R (inside Q), called the *localization of R at P.*

More generally, if $\mathcal{S}$ is a nonempty *multiplicatively closed* subset of R that does not contain 0; that is, $\mathcal{S} \neq \emptyset$, $0 \notin \mathcal{S}$ and for every $s_1, s_2 \in \mathcal{S}$, $s_1 s_2 \in \mathcal{S}$, then one can form a *localization*, $\mathcal{S}^{-1}(R)$, where

$$\mathcal{S}^{-1}(R) = \{\frac{r}{s} \mid s \in \mathcal{S},\ r \in R\}.$$

Using the principal that $\mathcal{S}$ is multiplicatively closed, we see immediately that $\mathcal{S}^{-1}(R)$ is an over-ring of R (regard $r \in R$ as $\frac{sr}{s}$ where $s \in \mathcal{S}$).

In the case of the localization of R at a prime P, $\mathcal{S}$ is taken to be $R \setminus P$. In one instance below we form a localization that is not at a prime ideal so we must consider the broader notion of localization, $\mathcal{S}^{-1}(R)$ (though it is no harder).

Proposition 11. *Let $\mathcal{S}$ be a multiplicatively closed subset of R.*

(a) *J is an ideal of $\mathcal{S}^{-1}(R)$ if and only if $J = \mathcal{S}^{-1}(I) = \{\frac{a}{s} \mid s \in \mathcal{S},\ a \in I\}$, for some ideal I of R.*

(b) *P' is a prime ideal of $\mathcal{S}^{-1}(R)$ if and only if $P' = \mathcal{S}^{-1}(P) = \{\frac{a}{s} \mid s \in \mathcal{S},\ a \in P\}$, for some prime ideal P of R such that $P \cap \mathcal{S} = \emptyset$.*

Proof. (a). Given an ideal J of $\mathcal{S}^{-1}(R)$, we will consider $I = R \cap J$. If $b \in J$, then $sb \in R \cap J = I$ for some $s \in \mathcal{S}$, so that $b = \frac{sb}{s} \in \mathcal{S}^{-1}(I)$. On the other hand, $I \subseteq J$ implies that $\mathcal{S}^{-1}(R)I = \mathcal{S}^{-1}(I) \subseteq J$. Therefore, $J = \mathcal{S}^{-1}(I)$. Conversely, $\mathcal{S}^{-1}(I) = \mathcal{S}^{-1}(R)I$ is an ideal of $\mathcal{S}^{-1}(R)$ when I is an ideal of R, so the proof of (a) is complete.

(b). From (a) we note that $P' = \mathcal{S}^{-1}(P)$ where $P = P' \cap R$. With this notation, we will show that

$$P' \text{ is prime in } \mathcal{S}^{-1}(R) \iff P \text{ is prime in } R \text{ with } P \cap \mathcal{S} = \emptyset.$$

If P' is prime in $\mathcal{S}^{-1}(R)$, then for any r_1, r_2 in R (in particular), $r_1 r_2 \in P'$ implies $r_1 r_2 \in P' \cap R = P$. We are given that $r_1 \in P'$ (hence $r_1 \in P' \cap R = P$) or $r_2 \in P'$ (hence $r_2 \in P' \cap R = P$), and because $1 \notin P'$, $1 \notin P$ so P is prime.

Conversely, if $P = P' \cap R$ is a prime ideal of R with $P \cap \mathcal{S} = \emptyset$, then first of all, $1 \notin P'$, so $P' \neq \mathcal{S}^{-1}(R)$. If $\frac{r_1}{s_1}\frac{r_2}{s_2} \in P' = \mathcal{S}^{-1}(P)$ for some $r_1, r_2 \in R$ and $s_1, s_2 \in \mathcal{S}$, then, multiplying by $s_1 s_2$, $r_1 r_2 \in P' \cap R = P$, implies $r_1 \in P \subseteq P'$ or $r_2 \in P \subseteq P'$. Hence $\frac{r_1}{s_1} \in P' = \mathcal{S}^{-1}(P)$ or $\frac{r_1}{s_1} \in P'$. □

Do you wonder which domains have the property that every overring S of R in Q must be a localization? This is what commutative ring theorists do, and the next section provides a partial answer.

4. Dedekind Domains

Characterization of Dedekind Domains The following are equivalent for an integral domain R that is not a field.

(1) R is Dedekind (i.e., every proper ideal is a product of prime ideals).
(2) Every nonzero ideal is invertible.
(3) R is noetherian, every nonzero prime ideal is maximal, and R is integrally closed.
(4) R is noetherian and for every maximal ideal M of R, R_M is a local PID.

Proof. (1) → (2). Observe that a product of ideals $I_1 I_2 \cdots I_n$ is invertible if and only if each I_j is invertible. Therefore, it is sufficient to show that every nonzero prime ideal is invertible. Let P be a nonzero prime ideal of R. Given $0 \neq a \in P$, by (1), we can write $Ra = P_1 P_2 \cdots P_n$. By the preceding remark, each P_j is invertible.

Since $P_1P_2\cdots P_n = Ra \subseteq P$ and P is prime, P contains one of the invertible primes P_j (for some j). In order to show that P is invertible, it is sufficient to show that P_j is maximal. Therefore, we have reduced the problem to showing that every invertible prime ideal is maximal, so without loss of generality, let P be an invertible prime (in other words, forget all the previous uses of letters).

In order to show that P is maximal we must show that if $r \in R \setminus P$, then $P + Rr = R$. Suppose that $P + Rr \neq R$. Then, by (1), $P + Rr = P_1P_2\cdots P_n$ for some prime ideals $P_1, P_2, \ldots, P_n$. Since $r \notin P$, $r^2 \notin P$ as well and we can write $P + Rr^2 = Q_1Q_2\cdots Q_m$ for some prime ideals $Q_1, Q_2, \ldots, Q_m$. Each P_j contains $P_1P_2\cdots P_n$ and therefore must contain P. Likewise, Q_i contains P for all i. Hence, we can factor modulo P:

$$(P + Rr)/P = \bar{P}_1\bar{P}_2\cdots\bar{P}_n,$$

and

$$(P + Rr^2)/P = \bar{Q}_1\bar{Q}_2\cdots\bar{Q}_m,$$

where $\bar{P}_j = P_j/P$, $\bar{R} = R/P$, and $\bar{Q}_i = Q_i/P$. Furthermore,

$$((P + Rr)/P)^2 = (P + Rr^2)/P,$$

so that

$$\bar{P}_1^2\bar{P}_2^2\cdots\bar{P}_n^2 = \bar{Q}_1\bar{Q}_2\cdots\bar{Q}_m.$$

Each $\bar{P}_j$ and $\bar{Q}_i$ is a prime ideal in the integral domain R/P; for instance, $\bar{R}/\bar{P}_j = (R/P)/(P_j/P) = R/P_j$ is an integral domain. Additionally, each $\bar{P}_j$ and $\bar{Q}_i$ is invertible because $(P + Rr)/P$ and $(P + Rr^2)/P$ are principal ideals of $\bar{R}$ (the general element in $(P + Rr^2)/P$ for example is the coset $sr^2 + P$ for some $s \in R$).

We can prove by induction on m that $2n = m$ and after re-indexing, $\bar{Q}_{2i-1} = \bar{Q}_{2i} = \bar{P}_i$ for $i = 1, 2, \ldots n$. We will show how reduction of the index works. Among each $\bar{P}_i$ and $\bar{Q}_j$, choose one that is minimal with respect to containment. If it is a $\bar{P}_i$, then reorder so that $i = 1$. Then $\bar{P}_1$ contains $\bar{Q}_1\bar{Q}_2\cdots\bar{Q}_m$ and hence must contain some $\bar{Q}_j$ since $\bar{P}_1$ is a prime ideal. Reorder so that $j = 1$, then cancel

$$\bar{P}_1\bar{P}_2^2\cdots\bar{P}_n^2 = \bar{Q}_2\cdots\bar{Q}_m.$$

If the original minimal prime was chosen as some $\bar{Q}_j$, reorder so that $j = 1$, and as before $\bar{Q}_1$, must contain some $\bar{P}_i$, which we take to be $\bar{P}_1$. Again, we cancel to obtain

$$\bar{P}_1\bar{P}_2^2\cdots\bar{P}_n^2 = \bar{Q}_2\cdots\bar{Q}_m.$$

In either case, induction applies (or, we can just repeat the argument as many times as necessary).

From $\bar{Q}_{2i-1} = \bar{Q}_{2i} = \bar{P}_i$ for $i = 1, 2, \ldots n$, we see that $Q_{2i-1} = Q_{2i} = P_i$ for $i = 1, 2, \ldots n$. Therefore,

$$(P + Rr)^2 = P_1^2 P_2^2 \cdots P_n^2 = Q_1 Q_2 \cdots Q_m = P + Rr^2.$$

So, $P \subseteq P + Rr^2 = P^2 + Rr^2 + Pr$. Given $p \in P$, write $p = p_2 + sr^2 + p_1 r$, so that $sr^2 = p - p_2 - p_1 r \in P$. Since r^2 does not belong to the prime ideal P, $s \in P$ and so $P \subseteq P + Pr^2 + Pr = P^2 + Pr = P(P + Rr)$. But since P is invertible, $R = P^{-1}P \subseteq P^{-1}P(P + Rr) = P + Rr \subseteq R$. This contradiction, shows that indeed $P + Rr = R$ (from the start) and therefore P is maximal as claimed.

(2) $\rightarrow$ (3). For any proper ideal I,

$$I^{-1}I = R \iff \Sigma_{i=1}^n b_i a_i = 1 \text{ for some } b_i \in I^{-1},\ a_i \in I.$$

Under (2), I is invertible, and so $a = \Sigma_{i=1}^n (ab_i)a_i$ for any $a \in I$, and since $ab_i \in I$ for all i, I is generated by $a_1, a_2, \ldots, a_n$. I.e., R is noetherian.

If P is a nonzero prime ideal, then P is contained in a maximal ideal M. Since M is invertible, $M^{-1}P \subseteq R$, and $M(M^{-1}P) \subseteq P$. Since P is prime, either $M^{-1}P \subseteq P$ or $M \subseteq P$. If the former were to hold, $M^{-1}P \subseteq P$, then P invertible implies $M^{-1} = M^{-1}PP^{-1} \subseteq PP^{-1} = R$. But forming inverses is order reversing and $M \subseteq R$ (so $M^{-1} \supseteq R$). Taken together, we have $M^{-1} = R$, from which $MM^{-1} = M$; a contradiction. Therefore, the latter case holds; $P = M$.

Suppose S is a fractional over-ring of R in the quotient field Q; $R \subseteq S$ implies $S^{-1} \subseteq R$ is an ideal and by (2), $(S^{-1})^{-1}S^{-1} = R$. But S is a ring, and $(S^{-1})^{-1}S^{-1} = R$ is an S-module, so $S \cdot R \subseteq R$, and $S = R$.

(3) $\rightarrow$ (4). Recall that $R_M = \{\frac{r}{s} \mid r, s \in R,\ s \notin M\}$. By Proposition 11, the ideals of $S = R_M$ are *extended*; i.e., the ideals of S must be of the form $I \cdot R_M = \{\frac{r}{s} \mid r \in I,\ s \in R \setminus M\}$ for some ideal I of R. Furthermore, the prime ideals of $S = R_M$ are of the form $P \cdot R_M$ where P is a prime ideal contained in M. Therefore, from (3), every ideal of S is finitely generated (since the ideals of R are finitely generated), with 0 and $N = M \cdot R_M$ as the only prime ideals of S.

We will first show that the maximal ideal of S is principal. By homework problem number 2 from the current set, it suffices to show that N is invertible (relative to S). But, in a manner applied earlier, $N^{-1} = \{t \in Q \mid tN \subseteq S\}$, contains S, and so $N \subseteq N^{-1}N \subseteq S$. If $N^{-1}N = N$, then $N^{-1}N^{-1}N = N^{-1}N = N$, implying that $N^{-1}N^{-1} = N^{-1}$; i.e., $T = N^{-1}$ is a fractional over-ring of S. But, we claim that S is integrally closed; a property inherited from R.

If $S[t]$ is an over-ring of S, then there exists an equation $t^n + s_{n-1}t^{n-1} + \cdots + s_0 = 0$ where $s_j \in S$ and $n \geq 1$. Let $r \in R \setminus M$ be such that $rs_j \in R$

for all j. Then $r^n(t^n + s_{n-1}t^{n-1} + \cdots + s_0) = (rt)^n + rs_{n-1}(rt)^{n-1} + \cdots + r^n s_0 = 0$, implying that rt is integral over R. Therefore, $rt = a \in R$ and consequently $t = ar^{-1} \in S$. Therefore, S is integrally closed by Proposition 6, and so $N^{-1} = S$.

We will show in this paragraph that N^{-1} is in fact unequal to S. Fix $0 \neq y \in N$ and consider the cyclic S-module

$$C = \langle \frac{1}{y} + S \rangle$$

inside Q/S. Observe that $C \neq 0$, because N does not contain a unit of S. The collection $\mathcal{I}$ of all ideals I of S such that $I = \{s \in S \mid s(\frac{t}{y} + S) = 0\}$, for some fixed $t \in S$ such that $\frac{t}{y} \notin S$. Since S is noetherian, unions of chained ideals of S stabilize and so $\mathcal{I}$ contains maximal members. Let P be maximal in $\mathcal{I}$, say $P = ann_S\, x + S$ for some $x = \frac{t}{y} \in Q \setminus S$ where $t \in S$, and suppose $rs \in P$, for some $r, s \in S$ with $r \notin P$. Then, $r(x + S) \neq 0$ but $(P + (s))(rx + S) = 0$. This implies $P = P + (s)$ and so $s \in P$ and P is prime. But $P \neq 0$ since $0 \neq Sy \in \mathcal{I}$, therefore $P = N$. That is, there exists an element $q = \frac{t}{y} \in Q \setminus S$ such that $Nq \in S$ and so $q \in N^{-1} \setminus S$.

Therefore, $N^{-1}N = S$ is the only possibility, and since S is local, by homework problem 2, N must be principal. Write $N = (b)$ for some $b \in S$. Now, S is a noetherian domain with principal maximal ideal $N = (b)$ and N and 0 are the only primes. We need to show that S is a PID.

Our first claim is that $\cap_{k=1}^{\infty} N^k = 0$. If we set $I = \cap_{k=1}^{\infty} N^k$ then clearly $bI = I$: check that if $a = bc$, then $a \in (b^n)$ if and only if $c \in (b^{n-1})$; so $a \in (b^n)$ for all n if and only if $c \in (b^n)$ for all n. Thus, $\frac{1}{b}I = I$, and I is an ideal in $S[\frac{1}{b}] = Q$. To see that $S[\frac{1}{b}] = Q$ observe that $S[\frac{1}{b}]$ is a localization of S using the set $\{b^j\}_{j=1}^{\infty}$, and by Proposition 11, $S[\frac{1}{b}]$ has no prime ideals save 0; consequently, $S[\frac{1}{b}]$ must be a field; and consequently, the field Q. But having I a module over Q can only happen when $I = 0$. Thus, $\cap_{k=1}^{\infty} N^k = 0$.

Let J be a proper ideal of S. Then $J \subseteq N$. Since $\cap_k (b^k) = 0$, there is a least positive integer such that $J \subseteq (b^k)$ but J is not contained in (b^{k+1}). If $a \in J \setminus (b^{k+1})$, write $a = ub^k$ where $u \in R$. Then, obviously, $u \notin (b)$, implying that u is a unit (since S is local with maximal ideal (b)). Therefore, $J = (b^k)$ and S is a PID.

(4) $\rightarrow$ (1). Let P be a prime ideal of R that is contained in a maximal ideal M, $P \neq M$. Then, from Proposition 11, $P \cdot R_M$ is a prime ideal in the ring R_M. But, R_M is a local PID so the only prime ideals are 0

and $M \cdot R_M$. Also,

$$r \in M \setminus P \implies r \in (M \cdot R_M) \setminus (P \cdot R_M) \ (check!)$$

and so P must be zero. Hence any nonzero prime ideal of R is maximal.

By the Primary Decomposition Theorem (to follow), every ideal $I \neq 0$ has a (reduced) primary decomposition:

$$I = I_1 \cap I_2 \cap \cdots \cap I_n,$$

where the I_j's are primary ideals associated with distinct primes (maximal ideals) M_j's. When the radicals, $M_1, M_2, \ldots, M_n$ are coprime in pairs (i.e., $M_i + M_j = R$ for all $i \neq j$), the intersection can be replaced by the product:

$$I = I_1 \cdot I_2 \cdots I_n \ \text{(see Corollary 11 below)}.$$

Once we show that the primary ideal I_j must be equal to $M_j^{n_j}$ for some positive integer n_j, the proof will be complete.

Let J be any nonzero primary ideal and let $M = rad(J)$. Note that M is a maximal ideal. Since R_M is a local PID, $J \cdot R_M = M^n \cdot R_M$ for some positive integer n. We claim that $J = M^n$. Note, that M^n too is primary by Proposition 14.

We claim that because J is primary,

$$J = R \cap (J \cdot R_M),$$

where $M = rad(J)$. Once this has been established we can show too that $M^n = R \cap (M^n \cdot R_M)$, since M^n is primary with radical M as well. This leads to

$$J = R \cap (J \cdot R_M) = R \cap (M^n \cdot R_M) = M^n,$$

as desired.

Clearly, $J \subseteq R \cap (J \cdot R_M)$. Suppose $a \in R \cap (J \cdot R_M) \setminus J$. Then, for some $r \in R \setminus M$, $ra \in J$. But J is primary and $a \notin J$ implies $r^m \in J$ for some $m \geq 1$. However, $r \notin M$ implies $r^m \notin M$ for any m since M is prime; a contradiction. Therefore, a primary ideal must be M^n for some maximal ideal M and integer n, completing the proof. □

Dedekind domains have ample structure with which we can discover the wonders of ring theory. Many of the assertions that were made during the course of the proof no longer hold once we leave the structure of Dedekind domains.

Example 12. Let $R = F[x, y]$ where F is a field. The quotient field Q of R is then $F(x, y) = \{ f(x, y)/g(x, y) \mid f(x, y), g(x, y) \in R,\ g(x, y) \neq 0\}$. The ideal generated by x and y, $M = (x, y)$, is maximal. But if $q(x, y) \in M^{-1}$, then $q(x, y) \cdot x \in R$ implies $q(x, y) = \frac{h(x,y)}{x}$ (recall

that R is a UFD). But then $q(x,y)\cdot y \in R$, implies $x|h(x,y)$ so that $q(x,y)\in R$. That is,

$$M^{-1} = R,$$

unlike the case when the domain is noetherian such that every nonzero prime ideal is maximal.

A class of domains receiving the most attention these days is the class of Prüfer domains. A domain is called Prüfer if every finitely generated ideal is invertible. There are numerous examples of non-noetherian Prüfer domains. Also, it can be shown that a maximal ideal M of a Prüfer domain is infinitely generated if and only if $M^2 = M$, and there are many example of such rings.

Example 13. The following conditions are equivalent for an integral domain R:

(1) R is Prüfer.
(2) For all ideals I, J, K of R, $I(J\cap K) = (IJ)\cap(IK)$.
(3) For all ideals I, J, K of R, $I\cap(J+K) = (I\cap J)+(I\cap K)$.
(4) Every over-ring S of R in Q is Prüfer.
(5) For every prime ideal P of R, R/P is Prüfer.

It can be shown for a Dedekind domain R, that every over-ring S of R in Q is of the form

$$S = \cap_{M\in\mathcal{M}} R_M,$$

where $\mathcal{M}$ is a collection of maximal ideals of R, and S is like-wise Dedekind.

EXERCISES of SECTION 3:

1. A domain R is called a *divisorial* domain if every proper ideal I satisfies $(I^{-1})^{-1} = I$.
   (i) Show that Dedekind domains are divisorial.
   (ii) If R is divisorial and M is a maximal ideal of R, show that $M^{-1}/R \cong R/M$.
2. (i) Show that a PID is Dedekind.
   (ii) Show that if every maximal ideal in a Dedekind domain R is principal, then R is a PID.
   (iii) Find Dedekind domain that is not a PID. Hint: consider $\mathbb{Z}[\sqrt{-5}]$.

5. Primary Decompositions of Ideals

We have seen that any ideal in a PID is a product of primary ideals (i.e., powers of a prime ideal). In order to establish this for more general domains, we need to weaken the definition of primary.

Definition . An ideal I of an integral domain R is called *primary*, if $I \neq R$ and whenever $rs \in I$ with $r \notin I$, there is an $n \geq 1$ such that $s^n \in I$.

Definition . The *radical of an ideal* I, $rad(I)$, is the ideal consisting of the elements $r \in R$ such that $r^n \in I$ for some $n \geq 1$.

Sometimes $rad(I)$ is called the *nilradical* of I, and sometimes it is written as $\sqrt{I}$.

Proposition 14. *Given an ideal $I \neq R$ of the noetherian domain R, one can say the following:*

(i) *The radical of I, $rad(I)$, is the intersection of all prime ideals containing I.*
(ii) *There is an $n \geq 1$ such that $rad(I)^n \subseteq I$.*
(iii) *If I is primary, then $rad(I)$ is prime.*
(iv) *If $rad(I)$ is a maximal ideal, I is primary.*

Item (i) prompts the phrase, *prime radical*, for $rad(I)$.

Proof. (i). Let $J = \cap\{P \mid I \subseteq P\}$ (P will always represent a prime unless otherwise indicated). If $r \in rad(I)$, then $r^n \in I$ for some $n \geq 1$. But then, for any $P \supseteq I$, $r^n \in P$ and since P is prime, $r \in P$. I.e., $rad(I) \subseteq J$. Conversely, if $r \in J$, but $r^n \notin I$ for any n, then consider the situation with the multiplicatively closed set $\mathcal{S} = \{r^n\}_{n=1}^{\infty}$. We have $\mathcal{S} \cap I = 0$ and so $\mathcal{S}^{-1}(I)$ is a proper ideal of $\mathcal{S}^{-1}(R)$. However, there are no primes in $\mathcal{S}^{-1}(R)$ containing $\mathcal{S}^{-1}(I)$ since r belongs to every P containing I; a contradiction. Thus, $r^n \in I$ for some n and $J \subseteq rad(I)$.

(ii). Since R is noetherian, $rad(I)$ is finitely generated; say $rad(I)$ is generated by $r_1, r_2, \ldots, r_k$. For each j there exists an n_j such that $r_j^{n_j} \in I$. Set $n = \Sigma_j n_j$. Given $r = \Sigma_j a_j r_j \in rad(I)$, we will convince ourselves that $r^n \in R$ by considering the case of two r_j's:

$$r^n = (a_1r_1+a_2r_2)^n = \Sigma_{i=0}^{n} c_{n,i}(a_1r_1)^i(a_2r_2)^{n-i} = \Sigma_{i=0}^{n} c_{n,i}(a_1^i a_2^{n-i})[r_1^i r_2^{n-i}],$$

where $c_{n,i}$ is the (integral) number of combinations of n things taken i at a time without regard to order. Observe that when $i < n_1$, $n-i > n_2$ and so $r_2^{n-i} \in I$ and when $i \geq n_1$, $r_1^i \in I$. Thus

$$r^n \in I.$$

That is, $rad(I)^n \subseteq I$. The case when $k > 2$ is analogous, one must use the multinomial expansion formula rather than the binomial expansion formula.

(iii). Suppose $rs \in rad(I)$ for some $r, s \in R$ with $r \notin rad(I)$. By the definition of $rad(I)$, there is an $n \geq 1$ such that $r^n s^n = (rs)^n \in I$. But

I is primary, and $r^n \notin I$ (since $r \notin rad(I)$), implies that some power of s^n, $s^{mn} \in I$. That is, $s \in rad(I)$. Therefore, $rad(I)$ is prime.

(iv). Let I be an ideal such that $rad(I) = M$ is maximal and suppose that $ab \in I$, with $a \notin I$. By (ii), there is an $n \geq 1$ such that $M^n \subseteq I$, so if we show that $b \in M$, then we will have $b^n \in I$. Suppose $b \notin M$. Then $M + (b) = R$. Consider

$$(M + (b))^n = M^n + bM^{n-1} + \cdots b^{n-1}M + (b^n) = R.$$

If we multiply this by a we obtain

$$aM^n + (ab)M^{n-1} + \cdots + (ab^{n-1})M + (ab^n) = aR.$$

But the left-hand-side is contained in I while the right-hand-side is not; a contradiction. Thus, $b \in M$ and so $b^n \in I$ as required for a primary ideal. □

Corollary 15. *If J is a primary ideal in a noetherian domain and $P = rad(J)$, then for some positive integer n, $P^n \subseteq J$.*

Example 16. Let $R = F[x, y]$ where F is a field, and observe that $M = (x, y)$ is a maximal ideal of R. Then each of the ideals given below is primary with radical M:

$$(x^2, y),\ (x^2, y^2),\ (x^2, y^3),\ (x^3, y^3),\ \ldots$$

Observe that a power of M is primary but does not appear in this list. Check for M or $M^2 = (x^2, xy, y^2)$ for example.

Given any module B, we can consider the *annihilator ideal* associated with an element $b \in B$

$$ann_R\, b = \{r \in R \mid rb = 0\}.$$

Of course $ann_R\, b$ may be 0 or may be R, but for certain modules B, $ann_R\, b$ will always be a proper ideal when $b \neq 0$. For example, when $B = R/I$ for a proper ideal I of R. Then, for any $0 \neq b \in B = R/I$, $ann_R\, b$ is a proper ideal, properly containing I.

Let us restrict ourselves to torsion (or bounded modules B), and assume that for any $b \in B$ there exists an $0 \neq r \in R$ such that $rb = 0$. The *associated primes* of B are the prime ideals P of R such that

$$P = ann_R\, b,$$

for some $b \in B$. With $\mathcal{A} = \{J \mid J = ann_R\, b \text{ for some } 0 \neq b \in B\}$, the maximal elements in $\mathcal{A}$ are associated primes of B.

To see this, let P be a maximal element in $\mathcal{A}$ and write $P = ann_R\, b$ for some $b \in B$. If $rs \in P$ but $r \notin P$, then $rb \neq 0$, but

$$(P + (s)) \cdot rb \subseteq Pb = 0.$$

Thus, $(s) \subseteq P$, and P is prime.

Proposition 17. *Let I be a proper ideal of the noetherian domain R. Then R/I has a single associated prime P if and only if I is primary with radical P.*

Proof. Assume that I is primary with radical P, and let P' be an associated prime of the (bounded) module R/I ($a \cdot R/I = 0$ for some (any) nonzero $a \in I$). Say $P' = ann_R\ r + I$ for some $r \in R \setminus I$, and observe that $I \subseteq P'$. Suppose there exists an $a \in P' \setminus P$. Then $ar \in I$ and $r \notin I$ implies $a^n \in I \subseteq P$ for some n, and because P is prime $a \in P$; i.e., $P' \subseteq P$. But I contains a power of its radical P, so $P^m \subseteq I \subseteq P'$ implies $P = P'$.

Conversely, suppose R/I has the lone associate prime P. Note that $P \supseteq I$. Suppose $rs \in I$ with $r \notin I$. Then $b = r + I \neq 0$ and the annihilator of b is contained in a maximal element in the set of all annihilators of R/I. I.e., $P(r+I) = 0$ and also $(P+(s))(r+I) = 0$. To complete the proof it is enough to show that every prime P' containing I, contains P (for then $P = rad(I)$ by Proposition 14, and by Corollary 15, $s^n \in P^n \subseteq I$ as needed).

Suppose there exists an $a \in P \setminus P'$. Since $I \subseteq P'$, $a \notin I$ and so $a + I \neq 0$. But then P is the unique maximal annihilator, and so $Pa \subseteq I \subseteq P'$. In particular, $a^2 \in P'$; a contradiction. Thus $P \subseteq P'$ and the proof is complete. □

There are a lot of different proofs of the result that every ideal has a *primary decomposition*, that is, for any proper ideal I, there exist primary ideals $I_1, I_2, \ldots, I_n$ such that

$$I = I_1 \cap I_2 \cap \cdots \cap I_n.$$

We opt for the direct approach, though this is not the traditional approach.

An ideal J that is different from R is called *irreducible*, if $J = J' \cap J'$ for some ideals J', J", implies one of J' of J" must be J (sound familiar?). An intersection $I = J_1 \cap J_2 \cap \cdots \cap J_n$ is called *irredundant* if for no proper subset U of $\{1, 2, \ldots, n\}$ is $I = \cap_{j \in U} J_j$. So J is irreducible if J is not the irredundant intersection of two ideals J' and J''.

Theorem 18. *Let I be a proper ideal in a noetherian domain R. Then, there exists primary ideals $I_1, I_2, \ldots, I_k$ such that*

$$I = I_1 \cap I_2 \cap \cdots \cap I_k.$$

Proof. We claim that any proper ideal I can be expressed as

$$I = I_1 \cap I_2 \cap \cdots \cap I_k,$$

where the ideals $I_1, I_2, \ldots, I_n$ are irreducible. Perhaps you can do this yourselves? While this is straightforward, we can shorten the process by using a slight technique.

If some proper ideal is not a finite intersection of irreducible ideals, then let $\mathcal{I}$ be the nonempty collection of all such ideals. Since R is noetherian, $\mathcal{I}$ contains a maximal member, call it J, by Proposition 1. Every ideal properly containing J must be an intersection of irreducibles.

If J is irreducible, then J is an intersection of irreducibles. Otherwise, $J = J_1 \cap J_2$ with J_1, J_2 both properly containing J. But then J_1, J_2 are intersections of irreducibles, and so is $J = J_1 \cap J_2$; a contradiction. Therefore $\mathcal{I}$ is empty.

It remains to show that irreducible ideals are primary. Let J be an irreducible ideal and consider R/J. If R/J has two associated prime, P_1 and P_2, then there exist elements $r_1, r_2 \in R$ such that $P_i = ann_R\, r_i + J$. Note that this last condition implies that for $J_i = Rr_i + J$, $J_i/J \cong R/P_i$ for $i = 1, 2$. Since J_1, J_2 properly contain J, $J_1 \cap J_2 = J$ is impossible. Let $x \in J_1 \cap J_2$ but $x \notin J$. The element $x + J_1$ corresponds to a nonzero element $r + P_1$ in R/P_1. But $P_2(x + J) = 0$ implies that P_2 annihilates $r + P_1$ and so $P_2 r \subseteq P_1$. This is impossible because $r \notin P_1$ and P_2 and P_1 are distinct primes. Thus, R/J has only 1 associated prime and by Proposition 17, J is primary. □

Corollary 19. *If $I_1, I_2, \ldots, I_n$ are primary ideals whose radicals are the distinct maximal ideals $M_1, M_2, \ldots, M_n$, then*

$$I_1 \cap I_2 \cap \cdots \cap I_n = I_1 \cdot I_2 \cdots I_n.$$

Proof. Each of the primary ideals I_j contains a power of their radical M_j by Corollary 8, so there exists a $k \geq 1$ such that $M_j^k \subseteq I_j$ for all j. Note that

$$M_i^k + \Pi_{j \neq i} M_j^k = R$$

for all i. To see this observe that if M is a maximal ideal containing $M_i^k + \Pi_{j \neq i} M_j^k$ then M contains M_i and M contains some M_j with $j \neq i$ (since M is prime), which is impossible. It follows that for any i,

$$I_i + \Pi_{j \neq i} I_j = R.$$

We have $I_1 I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$, and we can go the other way by induction on n. The inductive step is handled by multiplying both sides of the above equation by $I_1 \cap I_2 \cap \cdots \cap I_n$:

$$I_1 \cap I_2 \cap \cdots \cap I_n = [I_i \cap \cap_{j \neq i} I_j](I_i + \Pi_{j \neq i} I_j) =$$

$$[I_i \cap (\Pi_{j \neq i} I_j)](I_i + \Pi_{j \neq i} I_j) = [I_i \cap (\Pi_{j \neq i} I_j)] I_i + [I_i \cap (\Pi_{j \neq i} I_j)] \Pi_{j \neq i} I_j$$

$$\subseteq I_1 I_2 \cdots I_n.$$

□