Chapter 2

Integral Extensions

2.1 Integral Elements

2.1.1 Definitions and Comments

Let R be a subring of the ring S, and let $\alpha \in S$. We say that α is *integral* over R if α is a root of a *monic* polynomial with coefficients in R. If R is a field and S an extension field of R, then α is integral over R iff α is algebraic over R, so we are generalizing a familiar notion. If α is a complex number that is integral over $\mathbb{Z}$, then α is said to be an *algebraic integer* For example, if d is any integer, then $\sqrt{d}$ is an algebraic integer, because it is a root of $x^2 - d$. Notice that $2/3$ is a root of the polynomial $f(x) = 3x - 2$, but f is not monic, so we cannot conclude that $2/3$ is an algebraic integer. In a first course in algebraic number theory, one proves that a rational number that is an algebraic integer must belong to $\mathbb{Z}$, so $2/3$ is not an algebraic integer.

There are several conditions equivalent to integrality of α over R, and a key step is the following result, sometimes called the *determinant trick*.

2.1.2 Lemma

Let R, S and α be as above, and recall that a module is *faithful* if its annihilator is 0. Let M be a finitely generated R-module that is faithful as an $R[\alpha]$-module. Let I be an ideal of R such that $\alpha M \subseteq IM$. Then α is a root of a monic polynomial with coefficients in I.

Proof. let $x_1, \ldots, x_n$ generate M over R. Then $\alpha x_i \in IM$, so we may write $\alpha x_i = \sum_{j=1}^{n} c_{ij} x_j$ with $c_{ij} \in I$. Thus

$$\sum_{j=1}^{n} (\delta_{ij}\alpha - c_{ij}) x_j = 0, \ 1 \leq i \leq n.$$

In matrix form, we have $Ax = 0$, where A is a matrix with entries $\alpha - c_{ii}$ on the main diagonal, and $-c_{ij}$ elsewhere. Multiplying on the left by the adjoint matrix, we get $\Delta x_i = 0$ for all i, where Δ is the determinant of A. But then Δ annihilates all of M, so $\Delta = 0$. Expanding the determinant yields the desired monic polynomial. ♣

2.1.3 Remark

If $\alpha M \subseteq IM$, then in particular, α *stabilizes* M, in other words, $\alpha M \subseteq M$.

2.1.4 Theorem

Let R be a subring of S, with $\alpha \in S$. The following conditions are equivalent:
(1) α is integral over R;
(2) $R[\alpha]$ is a finitely generated R-module;
(3) $R[\alpha]$ is contained in a subring R' of S that is a finitely generated R-module;
(4) There is a faithful $R[\alpha]$-module M that is finitely generated as an R-module.

Proof.
(1) implies (2): If α is a root of a monic polynomial over R of degree n, then α^n and all higher powers of α can be expressed as linear combinations of lower powers of α. Thus $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ generate $R[\alpha]$ over R.

(2) implies (3): Take $R' = R[\alpha]$.

(3) implies (4): Take $M = R'$. If $y \in R[\alpha]$ and $yM = 0$, then $y = y1 = 0$.

(4) implies (1): Apply (2.1.2) with $I = R$. ♣

We are going to prove a transitivity property for integral extensions, and the following result will be helpful.

2.1.5 Lemma

Let R be a subring of S, with $\alpha_1, \ldots, \alpha_n \in S$. If α_1 is integral over R, α_2 is integral over $R[\alpha_1], \ldots$, and α_n is integral over $R[\alpha_1, \ldots, \alpha_{n-1}]$, then $R[\alpha_1, \ldots, \alpha_n]$ is a finitely generated R-module.

Proof. The $n = 1$ case follows from (2.1.4), part (2). Going from $n-1$ to n amounts to proving that if A, B and C are rings, with C a finitely generated B-module and B a finitely generated A-module, then C is a finitely generated A-module. This follows by a brief computation:

$$C = \sum_{j=1}^{r} By_j,\ B = \sum_{k=1}^{s} Ax_k,\ \text{so } C = \sum_{j=1}^{r}\sum_{k=1}^{s} Ay_j x_k.\ \clubsuit$$

2.1.6 Transitivity of Integral Extensions

Let A, B and C be subrings of R. If C is integral over B, that is, every element of C is integral over B, and B is integral over A, then C is integral over A.

Proof. Let $x \in C$, with $x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0$. Then x is integral over $A[b_0, \ldots, b_{n-1}]$. Each b_i is integral over A, hence over $A[b_0, \ldots, b_{i-1}]$. By (2.1.5), $A[b_0, \ldots, b_{n-1}, x]$ is a finitely generated A-module. By (2.1.4), part (3), x is integral over A. ♣

2.1.7 Definitions and Comments

If R is a subring of S, the *integral closure* of R in S is the set R_c of elements of S that are integral over R. Note that $R \subseteq R_c$ because each $a \in R$ is a root of $x - a$. We say that R is *integrally closed* in S if $R_c = R$. If we simply say that R is *integrally closed* without reference to S, we assume that R is an integral domain with fraction field K, and R is integrally closed in K.

If the elements x and y of S are integral over R, then just as in the proof of (2.1.6), it follows from (2.1.5) that $R[x, y]$ is a finitely generated R-module. Since $x + y, x - y$ and xy belong to this module, they are integral over R by (2.1.4), part (3). The important conclusion is that

$$R_c \text{ is a subring of } S \text{ containing } R.$$

If we take the integral closure of the integral closure, we get nothing new.

2.1.8 Proposition

The integral closure R_c of R in S is integrally closed in S.

Proof. By definition, $R_c \subseteq (R_c)_c$. Thus let $x \in (R_c)_c$, so that x is integral over R_c. As in the proof of (2.1.6), x is integral over R. Thus $x \in R_c$. ♣

We can identify a large class of integrally closed rings.

2.1.9 Proposition

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

Proof. Let x belong to the fraction field K of R. Write $x = a/b$ where $a, b \in R$ and a and b are relatively prime. If x is integral over R, there is an equation of the form

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_1(a/b) + a_0 = 0$$

with $a_i \in R$. Multiplying by b^n, we have $a^n + bc = 0$, with $c \in R$. Thus b divides a^n, which cannot happen for relatively prime a and b unless b has no prime factors at all, in other words, b is a unit. But then $x = ab^{-1} \in R$. ♣

A domain that is an integral extension of a field must be a field, as the next result shows.

2.1.10 Proposition

Let R be a subring of the integral domain S, with S integral over R. Then R is a field if and only if S is a field.

Proof. Assume that S is a field, and let a be a nonzero element of R. Since $a^{-1} \in S$, there is an equation of the form

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \cdots + c_1 a^{-1} + c_0 = 0$$

with $c_i \in R$. Multiply the equation by a^{n-1} to get

$$a^{-1} = -(c_{n-1} + \cdots + c_1 a^{n-2} + c_0 a^{n-1}) \in R.$$

Now assume that R is a field, and let b be a nonzero element of S. By (2.1.4) part (2), $R[b]$ is a finite-dimensional vector space over R. Let f be the R-linear transformation on this vector space given by multiplication by b, in other words, $f(z) = bz,\ z \in R[b]$. Since $R[b]$ is a subring of S, it is an integral domain. Thus if $bz = 0$ (with $b \neq 0$ by choice of b), we have $z = 0$ and f is injective. But any linear transformation on a finite-dimensional vector space is injective iff it is surjective. Therefore if $b \in S$ and $b \neq 0$, there is an element $c \in R[b] \subseteq S$ such that $bc = 1$. Consequently, S is a field. ♣

2.1.11 Preview

Let S be integral over the subring R. We will analyze in great detail the relation between prime ideals of R and those of S. Suppose that Q is a prime ideal of S, and let $P = Q \cap R$. (We say that Q *lies over* P.) Then P is a prime ideal of R, because it is the preimage of Q under the inclusion map from R into S. The map $a + P \to a + Q$ is a well-defined injection of R/P into S/Q, because $P = Q \cap R$. Thus we can regard R/P as a subring of S/Q. Moreover, S/Q is integral over R/P. To see this, let $b + Q \in S/Q$. Then b satisfies an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

with $a_i \in R$. But $b + Q$ satisfies the same equation with a_i replaced by $a_i + P$ for all i, proving integrality of S/Q over R/P. We can now invoke (2.1.10) to prove the following result.

2.1.12 Proposition

Let S be integral over the subring R, and let Q be a prime ideal of S, lying over the prime ideal $P = Q \cap R$ of R. Then P is a maximal ideal of R if and only if Q is a maximal ideal of S.

Proof. By (2.1.10), R/P is a field iff S/Q is a field. ♣

2.1.13 Remarks

Some results discussed in (2.1.11) work for arbitrary ideals, not necessarily prime. If R is a subring of S and J is an ideal of S, then $I = J \cap R$ is an ideal of R. As in (2.1.11), R/I can be regarded as a subring of S/J, and if S is integral over R, then S/J is integral over R/I. Similarly, if S is integral over R and T is a multiplicative subset of R, then S_T is integral over R_T. To prove this, let $\alpha/t \in S_T$, with $\alpha \in S, t \in T$. Then there is an equation of the form $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$, with $c_i \in R$. Thus

$$(\frac{\alpha}{t})^n + (\frac{c_{n-1}}{t})(\frac{\alpha}{t})^{n-1} + \cdots + (\frac{c_1}{t^{n-1}})\frac{\alpha}{t} + \frac{c_0}{t^n} = 0$$

with $c_{n-j}/t^j \in R_T$.

2.2 Integrality and Localization

Results that hold for maximal ideals can sometimes be extended to prime ideals by the technique of localization. A good illustration follows.

2.2.1 Proposition

Let S be integral over the subring R, and let P_1 and P_2 be prime ideals of S that lie over the prime ideal P of R, that is, $P_1 \cap R = P_2 \cap R = P$. If $P_1 \subseteq P_2$, then $P_1 = P_2$.

Proof. If P is maximal, then by (2.1.12), so are P_1 and P_2, and the result follows. In the general case, we localize with respect to P. Let $T = R \backslash P$, a multiplicative subset of $R \subseteq S$. The prime ideals P_i , $i = 1, 2$, do not meet T, because if $x \in T \cap P_i$, then $x \in R \cap P_i = P$, contradicting the definition of T. By the basic correspondence between prime ideals in a ring and prime ideals in its localization, it suffices to show that $P_1 S_T = P_2 S_T$. We claim that

$$PR_T \subseteq (P_1 S_T) \cap R_T \subset R_T.$$

The first inclusion holds because $P \subseteq P_1$ and $R_T \subseteq S_T$. The second inclusion is proper, for otherwise $R_T \subseteq P_1 S_T$ and therefore $1 \in P_1 S_T$, contradicting the fact that $P_1 S_T$ is a prime ideal.

But PR_T is a maximal ideal of R_T, so by the above claim,

$$(P_1 S_T) \cap R_T = PR_T, \text{ and similarly } (P_2 S_T) \cap R_T = PR_T.$$

Thus $P_1 S_T$ and $P_2 S_T$ lie over PR_T. By (2.1.13), S_T is integral over R_T. As at the beginning of the proof, $P_1 S_T$ and $P_2 S_T$ are maximal by (2.1.12), hence $P_1 S_T = P_2 S_T$. ♣

If S/R is an integral extension, then prime ideals of R can be lifted to prime ideals of S, as the next result demonstrates. Theorem 2.2.2 is also a good example of localization technique.

2.2.2 Lying Over Theorem

If S is integral over R and P is a prime ideal of R, there is a prime ideal Q of S such that $Q \cap R = P$.

Proof. First assume that R is a local ring with unique maximal ideal P. If Q is any maximal ideal of S, then $Q \cap R$ is maximal by (2.1.12), so $Q \cap R$ must be P. In general, let T be the multiplicative set $R \setminus P$. We have the following commutative diagram.

$$\begin{array}{ccc} R & \longrightarrow & S \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ R_T & \longrightarrow & S_T \end{array}$$

The horizontal maps are inclusions, and the vertical maps are canonical ($f(r) = r/1$ and $g(s) = s/1$). Recall that S_T is integral over R_T by (2.1.13). If Q' is any maximal ideal of S_T, then as at the beginning of the proof, $Q' \cap R_T$ must be the unique maximal ideal

of R_T, namely PR_T. By commutativity of the diagram, $f^{-1}(Q' \cap R_T) = g^{-1}(Q') \cap R$. (Note that if $r \in R$, then $f(r) \in Q' \cap R_T$ iff $g(r) \in Q'$.) If $Q = g^{-1}(Q')$, we have $f^{-1}(PR_T) = Q \cap R$. By the basic localization correspondence [cf.(2.2.1)], $f^{-1}(PR_T) = P$, and the result follows. ♣

2.2.3 Going Up Theorem

Let S be integral over R, and suppose we have a chain of prime ideals $P_1 \subseteq \cdots \subseteq P_n$ of R, and a chain of prime ideals $Q_1 \subseteq \cdots \subseteq Q_m$ of S, where $m < n$. If Q_i lies over P_i for $i = 1, \ldots, m$, then there are prime ideals $Q_{m+1}, \ldots, Q_n$ of S such that $Q_m \subseteq Q_{m+1} \subseteq \cdots \subseteq Q_n$ and Q_i lies over P_i for every $i = 1, \ldots, n$.

Proof. By induction, it suffices to consider the case $n = 2, m = 1$. Thus assume $P_1 \subseteq P_2$ and $Q_1 \cap R = P_1$. By (2.1.11), S/Q_1 is integral over R/P_1. Since P_2/P_1 is a prime ideal of R/P_1, we may apply the lying over theorem (2.2.2) to produce a prime ideal Q_2/Q_1 of S/Q_1 such that

$$(Q_2/Q_1) \cap R/P_1 = P_2/P_1,$$

where Q_2 is a prime ideal of S and $Q_1 \subseteq Q_2$. We claim that $Q_2 \cap R = P_2$, which gives the desired extension of the Q-chain. To verify this, let $x_2 \in Q_2 \cap R$. By (2.1.11), we have an embedding of R/P_1 into S/Q_1, so $x_2 + P_1 = x_2 + Q_1 \in (Q_2/Q_1) \cap R/P_1 = P_2/P_1$. Thus $x_2 + P_1 = y_2 + P_1$ for some $y_2 \in P_2$, so $x_2 - y_2 \in P_1 \subseteq P_2$. Consequently, $x_2 \in P_2$. Conversely, if $x_2 \in P_2$ then $x_2 + P_1 \in Q_2/Q_1$, hence $x_2 + P_1 = y_2 + Q_1$ for some $y_2 \in Q_2$. But as above, $x_2 + P_1 = x_2 + Q_1$, so $x_2 - y_2 \in Q_1$, and therefore $x_2 \in Q_2$. ♣

It is a standard result of field theory that an embedding of a field F in an algebraically closed field can be extended to an algebraic extension of F. There is an analogous result for ring extensions.

2.2.4 Theorem

Let S be integral over R, and let f be a ring homomorphism from R into an algebraically closed field C. Then f can be extended to a ring homomorphism $g : S \to C$.

Proof. Let P be the kernel of f. Since f maps into a field, P is a prime ideal of R. By (2.2.2), there is a prime ideal Q of S such that $Q \cap R = P$. By the factor theorem, f induces an injective ring homomorphism $\overline{f} : R/P \to C$, which extends in the natural way to the fraction field K of R/P. Let L be the fraction field of S/Q. By (2.1.11), S/Q is integral over R/P, hence L is an algebraic extension of K. Since C is algebraically closed, $\overline{f}$ extends to a monomorphism $\overline{g} : L \to C$. If $p : S \to S/Q$ is the canonical epimorphism and $g = \overline{g} \circ p$, then g is the desired extension of f, because $\overline{g}$ extends $\overline{f}$ and $\overline{f} \circ p|_R = f$. ♣

In the next section, we will prove the companion result to (2.2.3), the going down theorem. There will be extra hypotheses, including the assumption that R is integrally closed. So it will be useful to get some practice with the idea of integral closure.

2.2.5 Lemma

Let R be a subring of S, and denote by $\overline{R}$ the integral closure of R in S. If T is a multiplicative subset of R, then $(\overline{R})_T$ is the integral closure of R_T in S_T.

Proof. Since $\overline{R}$ is integral over R, it follows from (2.1.13) that $(\overline{R})_T$ is integral over R_T. If $\alpha/t \in S_T$ ($\alpha \in S, t \in T$) and α/t is integral over R_T, we must show that $\alpha/t \in (\overline{R})_T$. There is an equation of the form

$$(\frac{\alpha}{t})^n + (\frac{a_1}{t_1})(\frac{\alpha}{t})^{n-1} + \cdots + \frac{a_n}{t_n} = 0$$

with $a_i \in R$ and $t_i, t \in T$. Let $t_0 = \prod_{i=1}^n t_i$, and multiply the equation by $(tt_0)^n$ to conclude that $t_0\alpha$ is integral over R. Therefore $t_0\alpha \in \overline{R}$, so $\alpha/t = t_0\alpha/t_0t \in (\overline{R})_T$. ♣

2.2.6 Corollary

If T is a multiplicative subset of the integrally closed domain R, then R_T is integrally closed.

Proof. Apply (2.2.5) with $\overline{R} = R$ and $S = K$, the fraction field of R (and of R_T). Then R_T is the integral closure of R_T in S_T. But $S_T = K$, so R_T is integrally closed. ♣

Additional results on localization and integral closure will be developed in the exercises. The following result will be useful. (The same result was proved in (1.5.1), but a slightly different proof is given here.)

2.2.7 Proposition

The following conditions are equivalent, for an arbitrary R-module M.
(1) $M = 0$;
(2) $M_P = 0$ for all prime ideals P of R;
(3) $M_P = 0$ for all maximal ideals P of R.

Proof. It is immediate that (1) $\Rightarrow$ (2) $\Rightarrow$ (3). To prove that (3) $\Rightarrow$ (1), let $m \in M$. If P is a maximal ideal of R, then $m/1$ is 0 in M_P, so there exists $r_P \in R \setminus P$ such that $r_P m = 0$ in M. Let $I(m)$ be the ideal generated by the r_P. Then $I(m)$ cannot be contained in any maximal ideal $\mathcal{M}$, because $r_{\mathcal{M}} \notin \mathcal{M}$ by construction. Thus $I(m)$ must be R, and in particular, $1 \in I(m)$. Thus 1 can be written as a finite sum $\sum_P a_P r_P$ where P is a maximal ideal of R and $a_P \in R$. Consequently,

$$m = 1m = \sum_P a_P r_P m = 0. \ \clubsuit$$

2.3 Going Down

We will prove a companion result to the going up theorem (2.2.3), but additional hypotheses will be needed and the analysis is more complicated.

2.3.1 Lemma

Let S be integral over the subring R, with I an ideal of R. Then $\sqrt{IS}$ is the set of all $s \in S$ satisfying an equation of integral dependence $s^m + r_{m-1}s^{m-1} + \cdots + r_1 s + r_0 = 0$ with the $r_i \in I$.

Proof. If s satisfies such an equation, then $s^m \in IS$, so $s \in \sqrt{IS}$. Conversely, let $s^n \in IS,\ n \geq 1$, so that $s^n = \sum_{i=1}^{k} r_i s_i$ for some $r_i \in I$ and $s_i \in S$. Then $S_1 = R[s_1, \ldots, s_k]$ is a subring of S, and is also a finitely generated R-module by (2.1.5). Now

$$s^n S_1 = \sum_{i=1}^{k} r_i s_i S_1 \subseteq \sum_{i=1}^{k} r_i S_1 \subseteq IS_1.$$

Moreover, S_1 is a faithful $R[s^n]$-module, because an element that annihilates S_1 annihilates 1 and is therefore 0. By (2.1.2), s^n, hence s, satisfies an equation of integral dependence with coefficients in I. ♣

2.3.2 Lemma

Let R be an integral domain with fraction field K, and assume that R is integrally closed. Let f and g be monic polynomials in $K[x]$. If $fg \in R[x]$, then both f and g are in $R[x]$.

Proof. In a splitting field containing K, we have $f(x) = \prod_i (x - a_i)$ and $g(x) = \prod_j (x - b_j)$. Since the a_i and b_j are roots of the monic polynomial $fg \in R[x]$, they are integral over R. The coefficients of f and g are in K and are symmetric polynomials in the roots, hence are integral over R as well. But R is integrally closed, and the result follows. ♣

2.3.3 Proposition

Let S be integral over the subring R, where R is an integrally closed domain. Assume that no nonzero element of R is a zero-divisor of S. (This is automatic if S itself is an integral domain.) If $s \in S$, define a homomorphism $h_s : R[x] \to S$ by $h_s(f) = f(s)$; thus h_s is just evaluation at s. Then the kernel I of h_s is a principal ideal generated by a monic polynomial.

Proof. If K is the fraction field of R, then $IK[x]$ is an ideal of the PID $K[x]$, and $IK[x] \neq 0$ because s is integral over R. (If this is unclear, see the argument in Step 1 below.) Thus $IK[x]$ is generated by a monic polynomial f.

Step 1: $f \in R[x]$.

By hypothesis, s is integral over R, so there is a monic polynomial $h \in R[x]$ such that $h(s) = 0$. Then $h \in I \subseteq IK[x]$, hence h is a multiple of f, say $h = fg$, with g monic in $K[x]$. Since R is integrally closed, we may invoke (2.3.2) to conclude that f and g belong to $R[x]$.

Step 2: $f \in I$.

Since $f \in IK[x]$, we may clear denominators to produce a nonzero element $r \in R$ such that $rf \in IR[x] = I$. By definition of I we have $rf(s) = 0$, and by hypothesis, r is not a zero-divisor of S. Therefore $f(s) = 0$, so $f \in I$.

Step 3: f generates I.

Let $q \in I \subseteq IK[x]$. Since f generates $IK[x]$, we can take a common denominator and

write $q = q_1 f/r_1$ with $0 \neq r_1 \in R$ and $q_1 \in R[x]$. Thus $r_1 q = q_1 f$, and if we pass to residue classes in the polynomial ring $(R/Rr_1)[x]$, we have $\overline{q_1}\,\overline{f} = 0$. Since $\overline{f}$ is monic, the leading coefficient of $\overline{q_1}$ must be 0, which means that $\overline{q_1}$ itself must be 0. Consequently, r_1 divides every coefficient of q_1, so $q_1/r_1 \in R[x]$. Thus f divides q in $R[x]$. ♣

2.3.4 Going Down Theorem

Let the integral domain S be integral over the integrally closed domain R. Suppose we have a chain of prime ideals $P_1 \subseteq \cdots \subseteq P_n$ of R and a chain of prime ideals $Q_m \subseteq \cdots \subseteq Q_n$ of S, with $1 < m \leq n$. If Q_i lies over P_i for $i = m, \ldots, n$, then there are prime ideals $Q_1, \ldots, Q_{m-1}$ such that $Q_1 \subseteq \cdots \subseteq Q_m$ and Q_i lies over P_i for every $i = 1, \ldots, n$.

Proof. By induction, it suffices to consider $n = m = 2$. Let T be the subset of S consisting of all products $rt,\ r \in R \setminus P_1,\ t \in S \setminus Q_2$. In checking that T is a multiplicative set, we must make sure that it does not contain 0. If $rt = 0$ for some $r \notin P_1$ (hence $r \neq 0$) and $t \notin Q_2$, then the hypothesis that r is not a zero-divisor of S gives $t = 0$, which is a contradiction (because $0 \in Q_2$). Note that $R \setminus P_1 \subseteq T$ (take $t = 1$), and $S \setminus Q_2 \subseteq T$ (take $r = 1$).

First we prove the theorem under the assumption that $T \cap P_1 S = \emptyset$. Now $P_1 S_T$ is a proper ideal of S_T, else 1 would belong to $T \cap P_1 S$. Therefore $P_1 S_T$ is contained in a maximal ideal $\mathcal{M}$. By basic localization theory, $\mathcal{M}$ corresponds to a prime ideal Q_1 of S that is disjoint from T. Explicitly, $s \in Q_1$ iff $s/1 \in \mathcal{M}$. We refer to Q_1 as the *contraction* of $\mathcal{M}$ to S; it is the preimage of $\mathcal{M}$ under the canonical map $s \to s/1$. With the aid of the note at the end of the last paragraph, we have $(R \setminus P_1) \cap Q_1 = (S \setminus Q_2) \cap Q_1 = \emptyset$. Thus $Q_1 \cap R \subseteq P_1$ and $Q_1 = Q_1 \cap S \subseteq Q_2$. We must show that $P_1 \subseteq Q_1 \cap R$. We do this by taking the contraction of both sides of the inclusion $P_1 S_T \subseteq \mathcal{M}$. Since the contraction of $P_1 S_T$ to S is $P_1 S$, we have $P_1 S \subseteq Q_1$, so $P_1 \subseteq (P_1 S) \cap R \subseteq Q_1 \cap R$, as desired.

Finally, we show that $T \cap P_1 S$ is empty. If not, then by definition of T, $T \cap P_1 S$ contains an element rt with $r \in R \setminus P_1$ and $t \in S \setminus Q_2$. We apply (2.3.1), with $I = P_1$ and s replaced by rt, to produce a monic polynomial $f(x) = x^m + r_{m-1}x^{m-1} + \cdots + r_1 x + r_0$ with coefficients in P_1 such that $f(rt) = 0$. Define

$$v(x) = r^m x^m + r_{m-1} r^{m-1} x^{m-1} + \cdots + r_1 r x + r_0.$$

Then $v(x) \in R[x]$ and $v(t) = 0$. By (2.3.3), there is a monic polynomial $g \in R[x]$ that generates the kernel of the evaluation map $h_t : R[x] \to S$. Therefore $v = ug$ for some $u \in R[x]$. Passing to residue classes in the polynomial ring $(R/P_1)[x]$, we have $\overline{v} = \overline{u}\ \overline{g}$. Since $r_i \in P_1$ for all $i = 0, \ldots, m-1$, we have $\overline{v} = \overline{r}^m x^m$. Since R/P_1 is an integral domain and g, hence $\overline{g}$, is monic, we must have $\overline{g} = x^j$ for some j with $0 \leq j \leq m$. (Note that $r \notin P_1$, so $\overline{v}$ is not the zero polynomial.) Consequently,

$$g(x) = x^j + a_{j-1}x^{j-1} + \cdots + a_1 x + a_0$$

with $a_i \in P_1, i = 0, \ldots, j-1$. But $g \in \ker h_t$, so $g(t) = 0$. By (2.3.1), t belongs to the radical of $P_1 S$, so for some positive integer l, we have $t^l \in P_1 S \subseteq P_2 S \subseteq Q_2 S = Q_2$, so $t \in Q_2$. This contradicts our choice of t (recall that $t \in S \setminus Q_2$). ♣