Chapter 0

Ring Theory Background

We collect here some useful results that might not be covered in a basic graduate algebra course.

0.1 Prime Avoidance

Let $P_1, P_2, \ldots, P_s,\ s \geq 2$, be ideals in a ring R, with P_1 and P_2 not necessarily prime, but $P_3, \ldots, P_s$ prime (if $s \geq 3$). Let I be any ideal of R. The idea is that if we can avoid the P_j individually, in other words, for each j we can find an element in I but not in P_j, then we can avoid all the P_j simultaneously, that is, we can find a single element in I that is in none of the P_j. We will state and prove the contrapositive.

0.1.1 Prime Avoidance Lemma

With I and the P_i as above, if $I \subseteq \cup_{i=1}^{s} P_i$, then for some i we have $I \subseteq P_i$.

Proof. Suppose the result is false. We may assume that I is not contained in the union of any collection of $s-1$ of the P_i's. (If so, we can simply replace s by $s-1$.) Thus for each i we can find an element $a_i \in I$ with $a_i \notin P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_s$. By hypothesis, I is contained in the union of all the P's, so $a_i \in P_i$. First assume $s = 2$, with $I \not\subseteq P_1$ and $I \not\subseteq P_2$. Then $a_1 \in P_1,\ a_2 \notin P_1$, so $a_1 + a_2 \notin P_1$. Similarly, $a_1 \notin P_2,\ a_2 \in P_2$, so $a_1 + a_2 \notin P_2$. Thus $a_1 + a_2 \notin I \subseteq P_1 \cup P_2$, contradicting $a_1, a_2 \in I$. Note that P_1 and P_2 need not be prime for this argument to work. Now assume $s > 2$, and observe that $a_1 a_2 \cdots a_{s-1} \in P_1 \cap \cdots \cap P_{s-1}$, but $a_s \notin P_1 \cup \cdots \cup P_{s-1}$. Let $a = (a_1 \cdots a_{s-1}) + a_s$, which does not belong to $P_1 \cup \cdots \cup P_{s-1}$, else a_s would belong to this set. Now for all $i = 1, \ldots, s-1$ we have $a_i \notin P_s$, hence $a_1 \cdots a_{s-1} \notin P_s$ because P_s is prime. But $a_s \in P_s$, so a cannot be in P_s. Thus $a \in I$ and $a \notin P_1 \cup \cdots \cup P_s$, contradicting the hypothesis. ♣

It may appear that we only used the primeness of P_s, but after the preliminary reduction (see the beginning of the proof), it may very well happen that one of the other P_i's now occupies the slot that previously housed P_s.

0.2 Jacobson Radicals, Local Rings, and Other Miscellaneous Results

0.2.1 Lemma

Let $J(R)$ be the Jacobson radical of the ring R, that is, the intersection of all maximal ideals of R. Then $a \in J(R)$ iff $1 + ax$ is a unit for every $x \in R$.

Proof. Assume $a \in J(R)$. If $1 + ax$ is not a unit, then it generates a proper ideal, hence $1 + ax$ belongs to some maximal ideal $\mathcal{M}$. But then $a \in \mathcal{M}$, hence $ax \in \mathcal{M}$, and therefore $1 \in \mathcal{M}$, a contradiction. Conversely, if a fails to belong to a maximal ideal $\mathcal{M}$, then $\mathcal{M} + Ra = R$. Thus for some $b \in \mathcal{M}$ and $y \in R$ we have $b + ay = 1$. If $x = -y$, then $1 + ax = b \in \mathcal{M}$, so $1 + ax$ cannot be a unit (else $1 \in \mathcal{M}$). ♣

0.2.2 Lemma

Let $\mathcal{M}$ be a maximal ideal of the ring R. Then R is a *local ring* (a ring with a unique maximal ideal, necessarily $\mathcal{M}$) if and only if every element of $1 + \mathcal{M}$ is a unit.

Proof. Suppose R is a local ring, and let $a \in \mathcal{M}$. If $1 + a$ is not a unit, then it must belong to $\mathcal{M}$, which is the ideal of nonunits. But then $1 \in \mathcal{M}$, a contradiction. Conversely, assume that every element of $1+\mathcal{M}$ is a unit. We claim that $\mathcal{M} \subseteq J(R)$, hence $\mathcal{M} = J(R)$. If $a \in \mathcal{M}$, then $ax \in \mathcal{M}$ for every $x \in R$, so $1+ax$ is a unit. By (0.2.1), $a \in J(R)$, proving the claim. If $\mathcal{N}$ is another maximal ideal, then $\mathcal{M} = J(R) \subseteq \mathcal{M} \cap \mathcal{N}$. Thus $\mathcal{M} \subseteq \mathcal{N}$, and since both ideals are maximal, they must be equal. Therefore R is a local ring. ♣

0.2.3 Lemma

Let S be any subset of R, and let I be the ideal generated by S. Then $I = R$ iff for every maximal ideal $\mathcal{M}$, there is an element $x \in S \setminus \mathcal{M}$.

Proof. We have $I \subset R$ iff I, equivalently S, is contained in some maximal ideal $\mathcal{M}$. In other words, $I \subset R$ iff $\exists \mathcal{M}$ such that $\forall x \in S$ we have $x \in \mathcal{M}$. The contrapositive says that $I = R$ iff $\forall \mathcal{M}\ \exists x \in S$ such that $x \notin \mathcal{M}$. ♣

0.2.4 Lemma

Let I and J be ideals of the ring R. Then $I + J = R$ iff $\sqrt{I} + \sqrt{J} = R$.

Proof. The "only if" part holds because any ideal is contained in its radical. Thus assume that $1 = a + b$ with $a^m \in I$ and $b^n \in J$. Then

$$1 = (a+b)^{m+n} = \sum_{i+j=m+n} \binom{m+n}{i} a^i b^j.$$

Now if $i + j = m + n$, then either $i \geq m$ or $j \geq n$. Thus every term in the sum belongs either to I or to J, hence to $I + J$. Consequently, $1 \in I + J$. ♣

0.3 Nakayama's Lemma

First, we give an example of the *determinant trick*; see (2.1.2) for another illustration.

0.3.1 Theorem

Let M be a finitely generated R-module, and I an ideal of R such that $IM = M$. Then there exists $a \in I$ such that $(1 + a)M = 0$.

Proof. Let $x_1, \dots, x_n$ generate M. Since $IM = M$, we have equations of the form $x_i = \sum_{j=1}^{n} a_{ij}x_j$, with $a_{ij} \in I$. The equations may be written as $\sum_{j=1}^{n}(\delta_{ij} - a_{ij})x_j = 0$. If I_n is the n by n identity matrix, we have $(I_n - A)x = 0$, where $A = (a_{ij})$ and x is a column vector whose coefficients are the x_i. Premultiplying by the adjoint of $(I_n - A)$, we obtain $\Delta x = 0$, where Δ is the determinant of $(I_n - A)$. Thus $\Delta x_i = 0$ for all i, hence $\Delta M = 0$. But if we look at the determinant of $I_n - A$, we see that it is of the form $1 + a$ for some element $a \in I$. ♣

Here is a generalization of a familiar property of linear transformations on finite-dimensional vector spaces.

0.3.2 Theorem

If M is a finitely generated R-module and $f : M \to M$ is a surjective homomorphism, then f is an isomorphism.

Proof. We can make M into an $R[X]$-module via $Xx = f(x)$, $x \in M$. (Thus $X^2x = f(f(x))$, etc.) Let $I = (X)$; we claim that $IM = M$. For if $m \in M$, then by the hypothesis that f is surjective, $m = f(x)$ for some $x \in M$, and therefore $Xx = f(x) = m$. But $X \in I$, so $m \in IM$. By (0.3.1), there exists $g = g(X) \in I$ such that $(1 + g)M = 0$. But by definition of I, g must be of the form $Xh(X)$ with $h(X) \in R[X]$. Thus $(1+g)M = [1 + Xh(X)]M = 0$.

We can now prove that f is injective. Suppose that $x \in M$ and $f(x) = 0$. Then

$$0 = [1 + Xh(X)]x = [1 + h(X)X]x = x + h(X)f(x) = x + 0 = x. \ \clubsuit$$

In (0.3.2), we cannot replace "surjective" by "injective". For example, let $f(x) = nx$ on the integers. If $n \geq 2$, then f is injective but not surjective.

The next result is usually referred to as Nakayama's lemma. Sometimes, Akizuki and Krull are given some credit, and as a result, a popular abbreviation for the lemma is NAK.

0.3.3 NAK

(a) If M is a finitely generated R-module, I an ideal of R contained in the Jacobson radical $J(R)$, and $IM = M$, then $M = 0$.

(b) If N is a submodule of the finitely generated R-module M, I an ideal of R contained in the Jacobson radical $J(R)$, and $M = N + IM$, then $M = N$.

Proof.
(a) By (0.3.1), $(1+a)M = 0$ for some $a \in I$. Since $I \subseteq J(R)$, $1+a$ is a unit by (0.2.1). Multiplying the equation $(1+a)M = 0$ by the inverse of $1+a$, we get $M = 0$.
(b) By hypothesis, $M/N = I(M/N)$, and the result follows from (a). ♣

Here is an application of NAK.

0.3.4 Proposition

Let R be a local ring with maximal ideal J. Let M be a finitely generated R-module, and let $V = M/JM$. Then
(i) V is a finite-dimensional vector space over the *residue field* $k = R/J$.
(ii) If $\{x_1 + JM, \ldots, x_n + JM\}$ is a basis for V over k, then $\{x_1, \ldots, x_n\}$ is a minimal set of generators for M.
(iii) Any two minimal generating sets for M have the same cardinality.

Proof.
(i) Since J annihilates M/JM, V is a k-module, that is, a vector space over k. Since M is finitely generated over R, V is a finite-dimensional vector space over k.
(ii) Let $N = \sum_{i=1}^{n} Rx_i$. Since the $x_i + JM$ generate $V = M/JM$, we have $M = N + JM$. By NAK, $M = N$, so the x_i generate M. If a proper subset of the x_i were to generate M, then the corresponding subset of the $x_i + JM$ would generate V, contradicting the assumption that V is n-dimensional.
(iii) A generating set S for M with more than n elements determines a spanning set for V, which must contain a basis with exactly n elements. By (ii), S cannot be minimal. ♣

0.4 Localization

Let S be a subset of the ring R, and assume that S is *multiplicative*, in other words, $0 \notin S$, $1 \in S$, and if a and b belong to S, so does ab. In the case of interest to us, S will be the complement of a prime ideal. We would like to divide elements of R by elements of S to form the *localized ring* $S^{-1}R$, also called the *ring of fractions* of R by S. There is no difficulty when R is an integral domain, because in this case all division takes place in the fraction field of R. We will sketch the general construction for arbitrary rings R. For full details, see TBGY, Section 2.8.

0.4.1 Construction of the Localized Ring

If S is a multiplicative subset of the ring R, we define an equivalence relation on $R \times S$ by $(a,b) \sim (c,d)$ iff for some $s \in S$ we have $s(ad - bc) = 0$. If $a \in R$ and $b \in S$, we define the fraction a/b as the equivalence class of (a,b). We make the set of fractions into a ring in a natural way. The sum of a/b and c/d is defined as $(ad+bc)/bd$, and the product of a/b and c/d is defined as ac/bd. The additive identity is $0/1$, which coincides with $0/s$ for every $s \in S$. The additive inverse of a/b is $-(a/b) = (-a)/b$. The multiplicative identity is $1/1$, which coincides with s/s for every $s \in S$. To summarize:

$S^{-1}R$ is a ring. If R is an integral domain, so is $S^{-1}R$. If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is a field, the *fraction field* of R.

There is a natural ring homomorphism $h : R \to S^{-1}R$ given by $h(a) = a/1$. If S has no zero-divisors, then h is a monomorphism, so R can be embedded in $S^{-1}R$. In particular, a ring R can be embedded in its *full ring of fractions* $S^{-1}R$, where S consists of all non-divisors of 0 in R. An integral domain can be embedded in its fraction field.

Our goal is to study the relation between prime ideals of R and prime ideals of $S^{-1}R$.

0.4.2 Lemma

If X is any subset of R, define $S^{-1}X = \{x/s : x \in X, s \in S\}$. If I is an ideal of R, then $S^{-1}I$ is an ideal of $S^{-1}R$. If J is another ideal of R, then
(i) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;
(ii) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;
(iii) $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$;
(iv) $S^{-1}I$ is a proper ideal iff $S \cap I = \emptyset$.

Proof. The definitions of addition and multiplication in $S^{-1}R$ imply that $S^{-1}I$ is an ideal, and that in (i), (ii) and (iii), the left side is contained in the right side. The reverse inclusions in (i) and (ii) follow from

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

To prove (iii), let $a/s = b/t$, where $a \in I,\ b \in J,\ s, t \in S$. There exists $u \in S$ such that $u(at - bs) = 0$. Then $a/s = uat/ust = ubs/ust \in S^{-1}(I \cap J)$.

Finally, if $s \in S \cap I$, then $1/1 = s/s \in S^{-1}I$, so $S^{-1}I = S^{-1}R$. Conversely, if $S^{-1}I = S^{-1}R$, then $1/1 = a/s$ for some $a \in I,\ s \in S$. There exists $t \in S$ such that $t(s - a) = 0$, so $at = st \in S \cap I$. ♣

Ideals in $S^{-1}R$ must be of a special form.

0.4.3 Lemma

Let h be the natural homomorphism from R to $S^{-1}R$ [see (0.4.1)]. If J is an ideal of $S^{-1}R$ and $I = h^{-1}(J)$, then I is an ideal of R and $S^{-1}I = J$.

Proof. I is an ideal by the basic properties of preimages of sets. Let $a/s \in S^{-1}I$, with $a \in I$ and $s \in S$. Then $a/1 = h(a) \in J$, so $a/s = (a/1)(1/s) \in J$. Conversely, let $a/s \in J$, with $a \in R, s \in S$. Then $h(a) = a/1 = (a/s)(s/1) \in J$, so $a \in I$ and $a/s \in S^{-1}I$. ♣

Prime ideals yield sharper results.

0.4.4 Lemma

If I is any ideal of R, then $I \subseteq h^{-1}(S^{-1}I)$. There will be equality if I is prime and disjoint from S.

Proof. If $a \in I$, then $h(a) = a/1 \in S^{-1}I$. Thus assume that I is prime and disjoint from S, and let $a \in h^{-1}(S^{-1}I)$. Then $h(a) = a/1 \in S^{-1}I$, so $a/1 = b/s$ for some $b \in I, s \in S$. There exists $t \in S$ such that $t(as - b) = 0$. Thus $ast = bt \in I$, with $st \notin I$ because $S \cap I = \emptyset$. Since I is prime, we have $a \in I$. ♣

0.4.5 Lemma

If I is a prime ideal of R disjoint from S, then $S^{-1}I$ is a prime ideal of $S^{-1}R$.

Proof. By part (iv) of (0.4.2), $S^{-1}I$ is a proper ideal. Let $(a/s)(b/t) = ab/st \in S^{-1}I$, with $a, b \in R, s, t \in S$. Then $ab/st = c/u$ for some $c \in I, u \in S$. There exists $v \in S$ such that $v(abu - cst) = 0$. Thus $abuv = cstv \in I$, and $uv \notin I$ because $S \cap I = \emptyset$. Since I is prime, $ab \in I$, hence $a \in I$ or $b \in I$. Therefore either a/s or b/t belongs to $S^{-1}I$. ♣

The sequence of lemmas can be assembled to give a precise conclusion.

0.4.6 Theorem

There is a one-to-one correspondence between prime ideals P of R that are disjoint from S and prime ideals Q of $S^{-1}R$, given by

$$P \to S^{-1}P \text{ and } Q \to h^{-1}(Q).$$

Proof. By (0.4.3), $S^{-1}(h^{-1}(Q)) = Q$, and by (0.4.4), $h^{-1}(S^{-1}P) = P$. By (0.4.5), $S^{-1}P$ is a prime ideal, and $h^{-1}(Q)$ is a prime ideal by the basic properties of preimages of sets. If $h^{-1}(Q)$ meets S, then by (0.4.2) part (iv), $Q = S^{-1}(h^{-1}(Q)) = S^{-1}R$, a contradiction. Thus the maps $P \to S^{-1}P$ and $Q \to h^{-1}(Q)$ are inverses of each other, and the result follows. ♣

0.4.7 Definitions and Comments

If P is a prime ideal of R, then $S = R \setminus P$ is a multiplicative set. In this case, we write R_P for $S^{-1}R$, and call it the *localization* of R at P. We are going to show that R_P is a local ring, that is, a ring with a unique maximal ideal. First, we give some conditions equivalent to the definition of a local ring.

0.4.8 Proposition

For a ring R, the following conditions are equivalent.

(i) R is a local ring;
(ii) There is a proper ideal I of R that contains all nonunits of R;
(iii) The set of nonunits of R is an ideal.

Proof.
(i) implies (ii): If a is a nonunit, then (a) is a proper ideal, hence is contained in the unique maximal ideal I.
(ii) implies (iii): If a and b are nonunits, so are $a + b$ and ra. If not, then I contains a unit, so $I = R$, contradicting the hypothesis.
(iii) implies (i): If I is the ideal of nonunits, then I is maximal, because any larger ideal J would have to contain a unit, so $J = R$. If H is any proper ideal, then H cannot contain a unit, so $H \subseteq I$. Therefore I is the unique maximal ideal. ♣

0.4.9 Theorem

R_P is a local ring.

Proof. Let Q be a maximal ideal of R_P. Then Q is prime, so by (0.4.6), $Q = S^{-1}I$ for some prime ideal I of R that is disjoint from $S = R \setminus P$. In other words, $I \subseteq P$. Consequently, $Q = S^{-1}I \subseteq S^{-1}P$. If $S^{-1}P = R_P = S^{-1}R$, then by (0.4.2) part (iv), P is not disjoint from $S = R \setminus P$, which is impossible. Therefore $S^{-1}P$ is a proper ideal containing every maximal ideal, so it must be the unique maximal ideal. ♣

0.4.10 Remark

It is convenient to write the ideal $S^{-1}I$ as IR_P. There is no ambiguity, because the product of an element of I and an arbitrary element of R belongs to I.

0.4.11 Localization of Modules

If M is an R-module and S a multiplicative subset of R, we can essentially repeat the construction of (0.4.1) to form the localization of M by S, and thereby divide elements of M by elements of S. If $x, y \in M$ and $s, t \in S$, we call (x, s) and (y, t) equivalent if for some $u \in S$, we have $u(tx - sy) = 0$. The equivalence class of (x, s) is denoted by x/s, and addition is defined by

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}.$$

If $a/s \in S^{-1}R$ and $x/t \in S^{-1}M$, we define

$$\frac{a}{s}\frac{x}{t} = \frac{ax}{st}.$$

In this way, $S^{-1}M$ becomes an $S^{-1}R$-module. Exactly as in (0.4.2), if M and N are submodules of an R-module L, then

$$S^{-1}(M + N) = S^{-1}M + S^{-1}N \text{ and } S^{-1}(M \cap N) = (S^{-1}M) \cap (S^{-1}N).$$