MA 3G6 - PRIMARY DECOMPOSITION

DIANE MACLAGAN

Motivation

We recall/introduce the following three facts.

1. Any positive integer has a unique prime factorization $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ where the p_i are prime and $m_i \in \mathbb{N}$. This means that every ideal in $\mathbb{Z}$ can be written uniquely as the intersection of ideals generated by prime powers.
2. If R is a UFD, then every $f \in R$ can be written uniquely as a product of powers of irreducible elements. Thus every principal ideal can be written uniquely as the intersection of ideals generated by powers of irreducible elements.
3. (not examinable in 2017)

   Definition 1. Let I be an ideal in $K[x_1, \dots, x_n]$. The variety $X = V(I) \subseteq K^n$ is *irreducible* if we cannot write $X = X_1 \cup X_2$ where $X_i \subsetneq X$ for $i = 1, 2$, and each X_i has the form $V(I_i)$ for some ideal $I_i \subset K[x_1, \dots, x_n]$.

   Proposition 2. *Let K be algebraically closed. Every variety in K^n can be written as the union of a finite number of irreducible varieties.*

   Proof. If X is not irreducible, then we can write it as $X = X_1 \cup X_2$ with X_1, X_2 proper subvarieties. Either each X_i is irreducible, or we can rewrite it as $X_i = X_{i1} \cup X_{i2}$ with X_{ij} a proper subvariety of X_i. Repeat this procedure. Either this terminates with a X written as a finite number of irreducible varieties, or we get an infinite string of varieties $X \supsetneq X_i \supsetneq X_{ij} \supsetneq X_{ijk} \supsetneq \dots$. Write X^k for the variety in this list whose label has k indices. Then $I(X) \subseteq I(X^1) \subseteq I(X^2) \subseteq I(X^3) \dots$. Since $K[x_1, \dots, x_n]$ is Noetherian, this must stabilize with $I(X^k) = I(X^N)$ for all $k \geq N$ for some fixed N. But then $V(I(X^k)) = V(I(X^N))$ for $k \geq N$, which is a contradiction, as if we write $X^k = V(I^k)$, then $I(X^k) = \sqrt{I^k}$, and $V(\sqrt{I^k}) = V(I^k) = X^k$. $\square$

(Challenge: you do not need to assume that K is algebraically closed here).

This decomposition is again unique (exercise: prove this!).

The goal of this topic is to generalize these examples to more general rings.

Definitions

Definition 3. Let Q be a proper ideal in a ring R. Then Q is *primary* (or "a primary ideal") if whenever $fg \in Q$, either $f \in Q$ or $g^m \in Q$ for some $m > 0$.

Example 4. Let $I = \langle 27 \rangle \subset \mathbb{Z}$. Then I is primary, as if $ab \in I$, then 27 divides ab, so either 27 divides a, or 3 divides b, and so 27 divides b^3. The ideal $\langle 12 \rangle \subset \mathbb{Z}$ is not primary, however, as $(3)(4) \in \langle 12 \rangle$, but 3 is not divisible by 12, and no power of 4 is divisible by 12.

In general, an ideal $\langle n \rangle \subset \mathbb{Z}$ is primary if and only if n is (up to sign) a power of a prime. (Check this!)

Remark 5. If Q is primary, then $P = \sqrt{Q}$ is prime. Indeed, if $fg \in P$, then $(fg)^m = f^m g^m \in Q$ for some $m > 0$, so either $f^m \in Q$ (and thus $f \in \sqrt{Q} = P$), or some power $(g^m)^l = g^{ml}$ is in Q, so $g \in \sqrt{Q} = P$.

Definition 6. We say that Q is P-primary for a prime P if Q is primary and $P = \sqrt{Q}$.

Example 7. The ideal $\langle 27 \rangle \subset \mathbb{Z}$ is $\langle 3 \rangle$-primary. The ideal $\langle x^2 - 2x + 1 \rangle \subseteq \mathbb{C}[x]$ is $\langle x - 1 \rangle$-primary.

Warning: In $\mathbb{Z}$ the condition $\sqrt{Q} = P$ is prime suffices to ensure that Q is primary, but this is not true in general. For example consider the ideal $Q = \langle x^2, xy \rangle \subset \mathbb{C}[x, y]$. Then $\sqrt{Q} = \langle x \rangle$, which is prime, but Q is not primary, as $xy \in Q$, $x \notin Q$, and no power of y is in Q. Note that this also shows that the order of f and g in the definition matters (or more precisely, that we need to consider both orders); $y \notin Q$, but $x^2 \in Q$ is not enough to show that Q is primary.

Main theorem

For the rest of these notes we assume that R is Noetherian.

Definition 8. Let I be a proper ideal in a Noetherian ring R. A *primary decomposition* of I is an expression

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_r$$

where each Q_i is primary.

The decomposition is *irredundant* if for all $1 \leq i \leq r$ we have $I \subsetneq \cap_{j \neq i} Q_j$.

The decomposition is *minimal* if there is no decomposition with fewer terms (i.e. r is as small as possible. Minimal decompositions are automatically irredundant.

Example 9. Let $I = \langle x^2, xy, x^2z^2, yz^2 \rangle$. Then $I = \langle x^2, y \rangle \cap \langle x, z^2 \rangle$ is a primary decomposition. You will show that these ideals are primary in HW5, and also justify that the intersection of these two ideals is I. The containment $I \subset \langle x^2, y \rangle \cup \langle x, z^2 \rangle$ is straightforward. The ideals $\sqrt{\langle x^2, y \rangle}$ and $\sqrt{\langle x, z^2 \rangle}$ are prime, as the quotients by them are polynomial rings, so domains.

This decomposition is irredundant, as neither term can be removed. It is also minimal, as I is not primary ($xy \in I$, $x \notin I$, and no power of y is in I).

By contrast, $\langle 9 \rangle = \langle 3 \rangle \cap \langle 9 \rangle \subset \mathbb{Z}$ is not an irredundant primary decomposition, as we do not need the ideal $\langle 3 \rangle$ in this decomposition.

Exercise 10. Consider the following intersections in $\mathbb{C}[x, y]$. Are they (irredundant? minimal?) primary decompositions?

(1) $\langle x^2 \rangle \cap \langle y^3 \rangle \cap \langle x, y \rangle$.
(2) $\langle x^2, xy^2, y^3 \rangle \cap \langle x^3, y \rangle$

The main theorem about primary decompositions is the following.

Theorem 11. *Let I be a proper ideal in a Noetherian ring R. Then I has a primary decomposition.*

Our proof will detour via the concept of irreducible ideals.

Definition 12. An ideal $I \subseteq R$ is irreducible if it cannot be written as the intersection of two strictly larger ideals: if $I = J \cap K$ with J, K ideals of R then $I = J$ or $I = K$.

Lemma 13. *Irreducible ideals in a Noetherian ring are primary.*

Proof. Suppose that I is an irreducible ideal with $fg \in I$. Consider the chain of ideals $J_k = (I : g^k) := \{h \in R : hg^k \in I\}$ for $k \geq 1$. Note that $J_i \subseteq J_{i+1}$ for $i \geq 1$, so $J_1 \subseteq J_2 \subseteq \dots$ is an ascending chain of ideals. Since R is Noetherian, there is N for which $J_k = J_N$ for $k \geq N$. We claim that $I = (I + \langle g^N \rangle) \cap (I + \langle f \rangle)$. Indeed, if $h \in (I + \langle g^N \rangle) \cap (I + \langle f \rangle)$ then $gh \in I$ (since $h \in I + \langle f \rangle$, and $fg \in I$). Since $h \in I + \langle g^N \rangle$, we have $h = i + jg^N$ for some $i \in I$, $j \in R$, so $gh = gi + jg^{N+1}$. This means that $jg^{N+1} \in I$, so $j \in J_{N+1} = J_N$. But this means that $jg^N \in I$, so $h \in I$. This shows that $(I + \langle g^N \rangle) \cap (I + \langle h \rangle) \subseteq I$. The opposite inclusion is immediate, so we have equality. Since I is irreducible, we must have $I + \langle g^N \rangle = I$, or $I + \langle f \rangle = I$, and thus $f \in I$ or $g^N \in I$. We thus conclude that I is primary. $\square$

Proof of Theorem 11. It suffices by Lemma 13 to show that every ideal $I \subseteq R$ has an irreducible decomposition, so can be written as the intersection of a finite number of irreducible ideals. This follows by "Noetherian induction". Let $\mathcal{S}$ be the set of proper ideals in R that do not have an irreducible decomposition. We want to show that $\mathcal{S}$ is empty. If $\mathcal{S} \neq \emptyset$, then it has a maximal element $I \in \mathcal{S}$ (since R is Noetherian, so there is no infinite ascending chain of ideals in R, so in particular no infinite ascending chain of ideals in $\mathcal{S}$). Since I is not irreducible, we can write $I = J \cap K$ where J, K are proper ideals with $I \subsetneq J$, $I \subsetneq K$. But then $J, K \notin \mathcal{S}$, so $J = \cap_{i=1}^r Q_i$ and$K = \cap_{j=1}^s Q'_j$ with Q_i, Q'_j irreducible, and so $I = \cap_{i=1}^r Q_i \cap \cap_{j=1}^s Q'_j$ is an irreducible decomposition for I, which contradicts that $I \in \mathcal{S}$. From this contradiction we conclude that $\mathcal{S}$ is empty as required. $\square$

Uniqueness?

Primary decomposition generalizes the notion of prime factorization for integers. In that case we have uniqueness. We now discuss the extent to which this is true in our setting.

We first note that we need some assumptions to get uniqueness; $\langle 27 \rangle = \langle 3 \rangle \cap \langle 27 \rangle$ are two different primary decompositions.

Given any primary decomposition $I = \cap_{i=1}^s Q_i$ we can obtain an *irredundant* primary decomposition by iteratively removing Q_j if $I = \cap_{i \neq j} Q_i$. Thus every proper ideal in a Noetherian ring has an irredundant primary decomposition.

We also have the following lemma:

Lemma 14. *If Q_1, Q_2 are primary ideals in R with $\sqrt{Q_1} = \sqrt{Q_2} = P$, then $Q_1 \cap Q_2$ is P-primary.*

Proof. Suppose $fg \in Q_1 \cap Q_2$. Then either $f \in Q_1 \cap Q_2$, or, without loss of generality, $f \notin Q_1$, so there is $m > 0$ with $g^m \in Q_1$, and thus $g \in \sqrt{Q_1} = P$. Since $\sqrt{Q_2} = P$, in this case there is $l > 0$ with $g^l \in Q_2$, so $g^{\max m,l} \in Q_1 \cap Q_2$. Thus $Q_1 \cap Q_2$ is primary. We have $Q_1 \cap Q_2 \subseteq Q_1$, so $\sqrt{Q_1 \cap Q_2} \subseteq P$. If $f \in P$, then there are m, l with $f^m \in Q_1$, and $f^l \in Q_2$. Then $f^{\max(m,l)} \in Q_1 \cap Q_2$, so $f \in \sqrt{Q_1 \cap Q_2}$, and thus $\sqrt{Q_1 \cap Q_2} = P$. $\square$

This means that given a primary decomposition $I = \cap_{i=1}^s Q_i$ for an ideal I, we can modify it by removing some terms and replacing others by their intersections to get one with the following two properties:

(1) The decomposition is irredundant, and
(2) If $i \neq j$, we have $\sqrt{Q_i} \neq \sqrt{Q_j}$.

These decompositions are still not always unique, but they are closer to unique, as we next see.

Associated primes

Recall: The annihilator $\operatorname{ann}(M)$ of an element m of an R-module M is $\operatorname{ann}(m) = \{r \in R : rm = 0_M\}$.

Definition 15. Let M be an R-module. An ideal P is an associated prime of M if P is prime, and $P = \operatorname{ann}(m)$ for some $m \in M$. We write $\operatorname{Ass}(M)$ for the set of associated primes of M.

Example 16. Let $R = \mathbb{C}[x]$, and $M = \mathbb{C}[x]/\langle x^2 \rangle$. Then $\langle x \rangle$ is an associated prime of M, since $\langle x \rangle = \operatorname{ann}(x + \langle x^2 \rangle)$. The annihilator of $1 + \langle x^2 \rangle$ is $\langle x^2 \rangle$, which is not prime.

Lemma 17. *If R is a Noetherian ring, and $M \neq 0$,then* $\operatorname{Ass}(M) \neq \emptyset$.

Proof. Let $\mathcal{S} = \{\operatorname{ann}(m) : m \in M, m \neq 0\}$. Then $\mathcal{S}$ is nonempty, since there is a nonzero element of M, and every element of $\mathcal{S}$ is a proper ideal, as $1 \notin \operatorname{ann}(m)$ if $m \neq 0$. Thus $\mathcal{S}$ is a nonempty collection of proper ideals in the Noetherian ring R, so it has a maximal element $I = \operatorname{ann}(m')$. We claim that I is prime. Indeed, if $fg \in I$, then $fgm' = 0_M$. If $gm' = 0_M$, then $g \in I$. If $gm' \neq 0_M$, then $f \in \operatorname{ann}(gm')$. Now for any $m \in M$ we have $\operatorname{ann}(m) \subseteq \operatorname{ann}(gm)$, as if $hm = 0_M$, then $h(gm) = g(hm) = g0_M = 0_M$. Thus since $I = \operatorname{ann}(m')$ is a maximal element of $\mathcal{S}$, we have $\operatorname{ann}(m') = \operatorname{ann}(gm')$. Thus if $gm' \neq 0_M$, we have $f \in \operatorname{ann}(m') = I$. So either $g \in I$ or $f \in I$, and so I is prime. We then conclude that $I \in \operatorname{Ass}(M)$, so $\operatorname{Ass}(M) \neq \emptyset$. $\square$

Proposition 18. *If Q is a P-primary ideal in a Noetherian ring R, then* $\operatorname{Ass}(R/Q) = \{P\}$.

Proof. We have $\sqrt{Q} = P$. If $r \in R \setminus Q$, and $s \in R$ with $rs \in Q$, then $s^m \in Q$ for some $m > 0$, so $s \in P$. Thus for any $m = r + Q \in R/Q$ we have $\operatorname{ann}(m) \subseteq P$. Since $Q \subseteq \operatorname{ann}(m)$, we have $P = \sqrt{Q} \subseteq \sqrt{\operatorname{ann}(m)} \subseteq \sqrt{P} - P$, so $\sqrt{\operatorname{ann}(m)} = P$. Thus if $\operatorname{ann}(m)$ is prime, it equals P. As we know that $\operatorname{Ass}(R/Q)$ is nonempty by Lemma 17, we conclude that $\operatorname{Ass}(R/Q) = \{P\}$. $\square$

We now discuss the connection of associated primes to primary decomposition.

This needs the following definition (recall that we have already seen the direct product of rings).

Definition 19. If $M_1, \dots, M_s$ are R-modules, then $\oplus_{i=1}^s M_i$ is the R-module with elements $\{(m_1, \dots, m_s) : m_i \in M_i\}$ with addition coordinate-wise, and $r(m_1, \dots, m_s) = (rm_1, \dots, rm_s)$.

Example 20. For any ring R, the free module R^s is the direct sum of s copies of R.

Lemma 21. *If $\phi\colon M \to N$ is an injection of R-modules, then* $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N)$.

Proof. If $P = \mathrm{ann}(m)$ for some element $m \in M$, then $P = \mathrm{ann}(\phi(m))$. □

Example 22. Consider the group homomorphism $\phi(\mathbb{Z}/2\mathbb{Z}) \to \mathbb{Z}/6\mathbb{Z}$ given by $\phi(1) = 3$. This is a $\mathbb{Z}$-module homomorphism. We have $\mathrm{Ass}(\mathbb{Z}/2\mathbb{Z}) = \{\langle 2 \rangle\}$ (by Proposition 18), and $\mathrm{Ass}(\mathbb{Z}/6\mathbb{Z}) = \{\langle 2 \rangle, \langle 3 \rangle\}$.

Lemma 23. *If $M = \oplus_{i=1}^s M_i$ is a direct sum of R-modules, then* $\mathrm{Ass}(M) = \cup_{i=1}^s \mathrm{Ass}(M_i)$.

Proof. From the injective homomorphism $\phi_i\colon M_i \to M$ given by $\phi_i(m) = (0_{M_1}, \dots, m, \dots, 0_{M_s})$, we get $\mathrm{Ass}(M_i) \subseteq \mathrm{Ass}(M)$. Suppose $P = \mathrm{ann}((m_1, \dots, m_s)) \in \mathrm{Ass}(M)$, but $P \notin \mathrm{Ass}(M_i)$ for any $1 \leq i \leq s$. For all $r \in P$ we have $rm_s = 0_{M_s}$, so since $P \neq \mathrm{ann}(m_s)$ there is $r' \in \mathrm{ann}(m_s) \setminus P$. By induction we know that since $P \notin \mathrm{Ass}(M_i)$ for $1 \leq i \leq s-1$ we have $P \notin \mathrm{Ass}(\oplus_{i=1}^{s-1} M_i)$, so since $P \subseteq \mathrm{ann}((m_1, \dots, m_{s-1}))$ there is $r'' \in R$ with $r'' \in \mathrm{ann}((m_1, \dots, m_{s-1})) \setminus P$. But then $r'r''(m_1, \dots, m_s) = 0$, so $r'r'' \in P$, but $r', r'' \notin P$. This is a contradiction, since P is prime, so we conclude that $P \in \mathrm{Ass}(M_i)$ for some i, and so $Ass(M) = \cup_{i=1}^s \mathrm{Ass}(M_i)$. □

Theorem 24. *Let R be a Noetherian ring, and let $I = Q_1 \cap \cdots \cap Q_s$ be a primary decomposition, where Q_i is P_i-primary. Then $\mathrm{Ass}(R/I) \subseteq \{P_1, \dots, P_s\}$. If the decomposition is irredundant, then we have equality.*

Proof. Each R/Q_i is an R-module, so we can form the direct sum $M = \oplus_{i=1}^s R/Q_i$. Consider the R-module homomorphism $\phi\colon R/I \to M$ given by $\phi(r+I) = (r+Q_1, \dots, r+Q_s)$. To see that this is well defined, note that if $I \subseteq Q_i$ for each i, so if $r + I = r' + I$, then $r - r' \in I \subseteq Q_i$, so $r + Q_i = r' + Q_i$ for each i.

If $\phi(r + I) = 0_M$, then $r \in Q_i$ for all i, so $r \in \cap_{i=1}^s Q_i = I$, so $r + I = 0 + I$, and so ϕ is injective. Thus by Lemma 21 we have $\mathrm{Ass}(R/I) \subseteq \mathrm{Ass}(M)$. By Lemma 23 we have $\mathrm{Ass}(M) = \cup_{i=1}^s \mathrm{Ass}(R/Q_i) = \{P_1, \dots, P_s\}$, so $\mathrm{Ass}(R/I) \subseteq \{P_1, \dots, P_s\}$.

If the decomposition is irredundant, then for all $1 \leq i \leq s$, we have $I \neq \cap_{j\neq i} Q_j$. Consider $\phi(\cap_{j\neq i} Q_j + I)$. Since ϕ is injective, this is nonzero. However the image in each R/Q_j coordinate is zero for $j \neq i$, so we may consider ϕ restricted to $\cap_{j\neq i} Q_j + I$ as a homomorphism to R/Q_i. This is still injective, so $\mathrm{Ass}(\cap_{j\neq i} Q_j + I) \subseteq \mathrm{Ass}(R/Q_i) = \{P_i\}$. Since $\cap_{j\neq i} Q_j + I$ is a submodule of R/I (so there is an injective map $\cap_{j\neq i} Q_j + I \to R/I$), we have $P_i \in \mathrm{Ass}(R/I)$. Thus $\mathrm{Ass}(R/I) = \{P_1, \ldots, P_s\}$. $\square$

Important consequences: This shows that the primes occuring as $\sqrt{Q_i}$ in an irredundant primary decomposition $I = \cap_{i=1}^s Q_i$ are determined (so do not depend on the choice of decomposition. It also shows that $\mathrm{Ass}(R/I)$ is a finite set when R is Noetherian.

Definition 25. If $I = \cap_{i=1}^s Q_i$ is an irredundant primary decomposition with $P_i = \sqrt{Q_i} \neq P_j$ for $i \neq j$, then Q_i is called the primary component of I corresponding to P_i.

Definition 26. Let I be an ideal of R, and fix $f \in R$. The set

$$(I : f) = \{r \in R : rf \in I\}$$

is an ideal of R (check!). The saturation of I by f is

$$(I : f^\infty) = \{r \in R : \text{ there is } m > 0 \text{ such that } rf^m \in I\}.$$

Exercise 27. (1) $(I : f^\infty) = \cup_{m\geq 1}(I : f^m)$.
(2) We have $(I : f^m) \subseteq (I : f^{m+1})$ for any I, f and $m > 0$.
(3) If R is Noetherian, then $(I : f^\infty) = (I : f^N)$ for some $N > 0$.
(4) $(I \cap J : f) = (I : f) \cap (J : f)$.

Definition 28. An associated prime P of an R-module M is *minimal* if there is no $P' \subsetneq P$ with $P' \in \mathrm{Ass}(M)$.

Example 29. Let $I = \langle x^2, xy\rangle \subseteq \mathbb{C}[x, y]$. Then $I = \langle x\rangle \cap \langle x^2, y\rangle$ is an irredundant primary decomposition for I, so the associated primes are $\langle x\rangle$ and $\langle x^2, y\rangle$. The ideal $\langle x\rangle$ is a minimal associated prime, but $\langle x, y\rangle$ is not.

Proposition 30. *Let P be a minimal associated prime of an ideal I in a Noetherian ring R. Then the P-primary component of I does not depend on the choice of primary decomposition.*

Proof. Let $I = \cap_{i=1}^s Q_i$ be an irredundant primary decomposition, with $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$, and $\sqrt{Q_s} = P$. (We checked that this exists in the uniqueness section). Since $\cap_{i=1}^{s-1} Q_i \neq I$, there is $f \in \cap_{i=1}^{s-1} Q_i \setminus Q_s$. We may assume that $f \notin P$, as if $\cap_{i=1}^s Q_i \subseteq P$, then $Q_i \subset P$ for some i with $1 \leq i \leq s-1$, (using that if $J_1 \cap J_2 \subset P$ for a prime ideal

P, then $J_1 \subset P$ or $J_2 \subset P$) and so $P_i = \sqrt{Q_i} \subset P$, which would contradict either the minimality of P, or the hypothesis that $P_i \neq P_j$ for $i \neq j$. Then $(I : f^\infty) = \cap_{i=1}^s (Q_i : f^\infty)$ by the exercise. If $f \in Q_i$ then $(Q_i : f^\infty) = R$ (as $1f^1 \in Q_i$). Thus $(I : f^\infty) = (Q_s : f^\infty)$. If $g \in (Q_s : f^\infty)$, then $gf^m \in Q_s$ for some $m > 0$, so since Q_s is primary we have $g \in Q_s$ or $(f^m)^l = f^{ml} \in Q_s$ for some $l > 0$. Since $f \notin P = \sqrt{Q_s}$, we have $f^{ml} \notin Q_s$ for any m, l, so $g \in Q_s$, and thus $(Q_s : f^\infty) = Q_s$. Thus $(I : f^\infty) = Q_s$, so Q_s does not depend on the choice of primary decomposition. □

Proposition 30 generalizes the fact that the powers of primes showing up in a prime factorization are determined.

Important: The assumption that P is minimal is *essential* in Proposition 30. Consider the ideal $I = \langle x^3, x^2y^2 \rangle \subseteq \mathbb{C}[x,y]$. Then $I = \langle x^2 \rangle \cap \langle x^3, y^2 \rangle$ and $I = \langle x^2 \rangle \cap \langle x^3, x^2y^2, y^5 \rangle$ are both irredundant primary decompositions. The ideal I has one minimal associated prime ($\langle x \rangle$), which has (as required) the same primary component in both decompositions. Both ideals $\langle x^3, y^2 \rangle$ and $\langle x^3, x^2y^2, y^5 \rangle$ are $\langle x, y \rangle$-primary.

Summary

We showed that in a Noetherian ring every proper ideal I has an irredundant primary decomposition $I = \cap_{i=1}^s$ with the property that $i \neq j$ means that $\sqrt{Q_i} \neq \sqrt{Q_j}$. Such decompositions are minimal, as every associated prime occurs exactly one as $\sqrt{Q_i}$. The primary components Q_i that are P_i primary for a minimal associated prime P_i do not depend on the primary decomposition, but the primary components for non-minimal primes can be different in different minimal primary decompositions.