Miscellenous Notes

Nawal Kishor Hazarika

Contents

1 Primary Decomoposition

Remark 1.1 We will show that the quotient of a primary ideal is primary. Let P be a primary ideal containing I in the ring A. Now for $\overline{xy} \in \overline{P}$, we have $xy - p \in I$ for some $p \in P$. Thus $xy - p \in P$ i.e., $xy \in P$. Hence $x \in P$ or $y^n \in P$. This implies $\overline{x} \in \overline{P}$ or $\overline{y} \in r(\overline{P})$.

Remark 1.2 If radical of an ideal is prime, it does not imply that the ideal is primary.

Remark 1.3 If an ideal is power of a prime, it does not mean the ideal is primary.

Proposition 1.4. *If the radical $\mathfrak{r}(I)$ is maximal for some ideal I. Then I is primary.*

Proof. Let us consider the quotient ring $R = A/\mathfrak{m}$ where $\mathfrak{m} = \mathfrak{r}(I)$. Now the image of $\mathfrak{m}$ in the quotient ring is the set of all nilpotent elements i.e., the nilradical of R. Which is nothing but the intersection of prime ideals in R. But the prime ideals of R are in 1-1 correspondence with the ideal of A containing I. If for some prime ideal P of A is such that $I \subseteq P$ and $\mathfrak{m}/I \subseteq P/I$, then we must have $\mathfrak{m} \subseteq P$. Otherwise say $x \in \mathfrak{m}$, $x \notin P$. But $\overline{x} \in P/I$ implies $x + I = y + I$ for some $y \in P$. Which implies $x - y \in I \subseteq P$ i.e., $(x - y) + y = x \in P$. The only proper ideal of A containing $\mathfrak{m}$ is the ideal itslef. Thus there is only one prime ideal in the ring R and hence only one maximal ideal. Therefore each element of R is eithe a unit or a nilpotent element. Hence the zero-divisors are nilpotent. □

Lemma 1.5. *Let $\mathfrak{q}$ be a $\mathfrak{p}$ primary ideal.*

i) if $x \in \mathfrak{q}$, $(\mathfrak{q} : x) = (1)$

ii) if $x \notin \mathfrak{q}$ then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.

iii) if $x \notin \mathfrak{p}$, $(\mathfrak{q} : x) = (1)$.

Proof. i) Clear.

ii) Let $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$. The fact that $x \notin \mathfrak{q}$ implies $y^m \in \mathfrak{q}$ i.e., $y \in \mathfrak{p}$. Thus $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$ and $\mathfrak{p} = \sqrt{\mathfrak{q}} \subseteq \sqrt{(\mathfrak{q} : x)} \subseteq \mathfrak{p}$.

Also for $ab \in (\mathfrak{q} : x)$ let $b \notin \sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$. To show $a \in (\mathfrak{q} : x)$. Now $abx \in \mathfrak{q}$ with $b \notin \mathfrak{p}$. Thus $ax \in \mathfrak{q}$ i.e., $a \in (\mathfrak{q} : x)$.

iii) For any $y \in (\mathfrak{q} : x)$, $xy \in \mathfrak{q}$ implies $y \in \mathfrak{q}$. Since $x^n \notin \mathfrak{q}$ for any $n \geq 0$.

□

Definition 1.6 A **primary decomoposition** of an ideal I in A is **an** expression of I as finite intersection of primary ideals i.e.,

$$I = \cap_{i=1}^{n} \mathfrak{q}_i.$$

If (i) the $r(\mathfrak{q}_i)$ are distinct and (ii) $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$, the primary decomoposition is said to be **minimal or reduced.** □

Remark 1.7 Every ideal in a Noetherian ring has a primary decomoposition.

1.1 The 1st Uniquness Theorem

Theorem 1.8 (1st uniquness theorem)**.** *Let I be a decompossible ideal in A and $I = \cap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomoposition. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)(1 \leq i \leq n)$. Then the $\mathfrak{p}_i$ are precisely the prime ideals contained in the set $\{r(I : x) \mid x \in A\}$.*

Proof. For any x, we have $(I : x) = (\cap \mathfrak{q}_i : x) = \cap(\mathfrak{q}_i : x)$. Thus $r(I : x) = \cap_{i=1}^n r(\mathfrak{q}_i : x)$. By 1.5 We have $r(\mathfrak{q}_i : x) = 1$ if $x \in \mathfrak{q}_i$, and $r(\mathfrak{q}_i : x) = \mathfrak{p}_i$ if $x \notin \mathfrak{q}_i$. Hene $r(I : x) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$. Moreover if $r(I : x)$ is prime, we must have $r(I : x) = \mathfrak{p}_j$ for some j. Thus the prime ideals of the set $\{r(I : x) \mid x \in A\}$ are the primes occuring in the minimal decomoposition of I.

Conversely, there exists $x_i \notin \mathfrak{q}_i, x_i \in \cap_{j \neq i} \mathfrak{q}_j$ because $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$. And by 1.5 we have $r(I : x_I) = \mathfrak{p}_i$. ☐

Definition 1.9 If $I = \cap_{i=1}^n \mathfrak{q}_i$ is a minimal primary decomoposition with $r(\mathfrak{q}_i) = \mathfrak{p}_i$, the ideals $\mathfrak{p}_i$ are said to *belong* to or to be *associated* with $\mathfrak{a}$.

The minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ are said to be the minimal or isolated prime ideals belonging to $\mathfrak{a}$. The other prime ideals are called embedded. ☐

Definition 1.10 Ass(I) is the set of all prime ideals of the form $r(I : x)$ for some $x \in A$. ☐

Example $\mathfrak{a} = (x^2, xy)$ in $k[x, y]$ has minimal primary decomoposition $\mathfrak{a} = (x) \cap (x, y)^2 = \mathfrak{q}_1 \cap \mathfrak{q}_2^2$. Here $pf_1 = (x)$ is minimal and $\mathfrak{p}_2 = (x, y)$ is embedded.

Definition 1.11 An ideal is said to be decomoposible if it has a primary decomoposition. ☐

Proposition 1.12 (Minimal Prime Ideals)**.** *Let $\mathfrak{a}$ be a decomoposible ideal. Then any prime ideal containing $\mathfrak{a}$ contains a minimal element associated/belonging to $\mathfrak{a}$. Thus the minimal prime ideals of $\mathfrak{a}$ are precisely the minimal elements in the set of prime ideals containing $\mathfrak{a}$.*

Proof. If $\mathfrak{p} \supseteq I = \cap \mathfrak{q}_i$, then $r(\mathfrak{p}) = \mathfrak{p} \supseteq \cap \mathfrak{p}_i$. Therefore $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i. If $\mathfrak{p}_i$ is a minimal element of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ we are done. Otherwise it will contain a minimal element belonging to $\mathfrak{a}$. ☐

Proposition 1.13. *Let $\mathfrak{a}$ be a decomoposible ideal with minimal primary decomoposition $\mathfrak{a} = \cap \mathfrak{q}_i$ with $r(\mathfrak{q}_i) = \mathfrak{p}_i$. Then*

$$\cup \mathfrak{p}_i = \{x \in A \mid (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

In particular if the zero ideal is decomoposible, the set D of zero-divisors of A is union of all the prime ideals belonging to 0.

Proof. If $\mathfrak{a}$ is decomoposible in A, then (0) is decomoposible in the quotient ring $A/\mathfrak{a}$ such that $0 = \cap \overline{\mathfrak{q}}_i$ and $\overline{\mathfrak{q}}_i$ is primary.

In particular let us assume that the zero ideal is decomoposible such that $0 = \cap \mathfrak{q}_i$. Again D is equal to $\cup_{x \neq 0} r(0 : x)$. Also $r(0 : x) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \subseteq \mathfrak{p}_j$. Thus $D \subseteq \cup_{i=1}^n \mathfrak{p}_j$. Again each $\mathfrak{p}_j$ is of the form $r(0 : x)$ for some $x \in A$. Therefore $\cup_{i=1}^n \mathfrak{p}_j \subseteq D \subseteq \cup_{i=1}^n \mathfrak{p}_j$. ☐

Remark 1.14

$$D\text{=\{set of all zero-divisors of A\}}=\bigcup \text{\{all prime ideals belonging to 0\}},$$

and

$$\mathfrak{N}=\{\text{nilpotent elements of A}\}=\bigcap\{\text{all minimal prime ideals belonging to } 0\}.$$

1.2 Primary Ideals and Localization

Proposition 1.15. *If I is an ideal in A, S a multiplicative subset of A then $I^{ec} = \cup_{s\in S}(I : s)$.*

Proof. Let $x \in I^{ec}$ i.e., $x \in (S^{-1}I)^c$. Thus $x/1 = a/s$ for some $a \in S$ i.e., $t.(a - sx) = 0$ for some $t \in S$. Hence $sxt = at \in I$ and $x \in (I : st)$. Therefore we have

$$I^{ec} \subseteq \cup_{s\in S}(I : s).$$

Also for $x \in \cup_{s\in S}(I : s)$, $xs \in I$ for some $s \in S$. This gives us $xs/s = x/1 \in I^e$ and $x \in I^{ec}$. □

Proposition 1.16. $S^{-1}r(I) = r(S^{-1}I)$.

Proof. If $x/s \in r(S^{-1}I)$, $(x/s)^m \in S^{-1}I$ i.e., $x^m/s^m = y/t$ for $y \in I$. Therefore $u(x^m t - s^m y) \in I$ for some $u \in S$. Now $x^m tu \in I$ will imply $(xtu)^m \in I$ and $xtu \in r(I)$. Thus $x/s \in S^{-1}r(I)$.

Conversely for $x/s \in S^{-1}r(I)$, $x^m \in I$ and $x^m/s^m \in S^{-1}I$. Therefore we have $x/s \in r(S^{-1}I)$. □

Proposition 1.17. *Let S be a multiplicatively closed set of A and $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.*

i) if $S \cap \mathfrak{p} \neq \phi$, $S^{-1}\mathfrak{q} = S^{-1}A$.

ii) if $S \cap \mathfrak{p} = \phi$, $S^{-1}\mathfrak{q}$ is a $S^{-1}\mathfrak{p}$-primary ideal and its contraction in A is $\mathfrak{q}$.

Proof. i) Let $s \in S \cap \mathfrak{p}$, then $s^n \in S \cap \mathfrak{q}$. Therefore we have a unit $\frac{s^n}{1} \in S^{-1}\mathfrak{q}$.

ii) Let $S \cap \mathfrak{p} = \phi$, then $s \in S$ and $as \in \mathfrak{q}$ implies $a \in \mathfrak{q}$. Thus $\mathfrak{q}^{ec} = \cup_{s\in S}(\mathfrak{q} : s) = \mathfrak{q}$ by 1.15 i.e., the contraction is $\mathfrak{q}$.

Again $r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$ by 1.16.

All it remains to show that $S^{-1}\mathfrak{q}$ is primary. For $\frac{x}{s}\frac{y}{t} \in S^{-1}\mathfrak{q}$ let $y/t \notin S^{-1}\mathfrak{p}$ i.e., $y \notin \mathfrak{p}$. Now $u(xyr - zst) \in \mathfrak{q}$ for some $z \in \mathfrak{q}$. Again $xyru \in \mathfrak{q}$ with $y \notin \mathfrak{p}$, implieds $xru \in \mathfrak{q}$. But $ru \notin \mathfrak{p}(S \cap \mathfrak{p} = \phi)$ and we will have $x \in \mathfrak{q}$, since $\mathfrak{q}$ is primary. Therefore $\frac{x}{s} \in S^{-1}\mathfrak{p}$.

□

Remark 1.18 The contraction of an ideal $S^{-1}I$ in A is denoted by $S(I)$.

Proposition 1.19. *Let S be a multiplicatively closed subset of A and $\mathfrak{a}$ is a decomoposible ideal. Let $I = \cap\mathfrak{q}_i$ be a minimal primary decomoposition of $\mathfrak{a}$. Let $r(\mathfrak{q}_i) = \mathfrak{p}_i$ and S meets $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$ but not $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Then $S^{-1}\mathfrak{a} = \cap_{i=1}^m S^{-1}\mathfrak{q}_i$ and $S(\mathfrak{a}) = \cap_{i=1}^m \mathfrak{q}_i$ are minimal primary decomoposition.*

Proof. We have $S^{-1}\mathfrak{a} = S^{-1}(\cap_n \mathfrak{q}_i) = \cap_n S^{-1}(\mathfrak{q}_i) = \cap_m S^{-1}\mathfrak{q}_i$, where $S^{-1}\mathfrak{q}_i$ are $S^{-1}\mathfrak{p}_i$ primary. Since each $\mathfrak{p}_i$ are distinct, each $S^{-1}\mathfrak{p}_i$ are also distinct.

Using contraction we get $S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = (\cap_m S^{-1}\mathfrak{q}_i)^c = \cap_m (S^{-1}\mathfrak{q}_i)^c = \cap\mathfrak{q}_i$ by 1.17. □

1.3 The 2nd Uniquness Theorem

Definition 1.20 A set Σ of prime ideals belonging to an ideal I is said to be isolated if the elements are minimal prime ideals belonging to I. $\square$

Remark 1.21 For an isolated set Σ of prime ideals belonging to I. The set $A \setminus \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$ is multiplicatively closed. Clearly $1 \in S$ and for any $x, y \in S$ if $xy \in \cup\mathfrak{p}$, then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$. Which is a contraction to the fact that $x, y \in S$.

Also for any prime ideal $\mathfrak{p}$ belonging to I if we have $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}_1 \cap S = \phi$. Otherwise $\mathfrak{p} \notin \Sigma$ implies $\mathfrak{p} \nsubseteq \cup_{\mathfrak{p}'\in\Sigma}\mathfrak{p}'$. Thus $\mathfrak{p} \cap S \neq \phi$.

2 Abstract Algebra

2.1 Conjugacy classes in A_n and S_n

Lemma 2.1. *Let G acts transtiviely on a set A, H a normal subgroup of G. If the orbits of A under the action of H are $\{\mathcal{O}_i \mid 1 \leq i \leq r\}$ then G permutes $\mathcal{O}_i$'s.*

Proof. Let $x \in \mathcal{O}_1$ and $gx \in \mathcal{O}_2$. We have to show that $gO_1 = O_2$. For any $u \in O_1$, there exists $h \in H$ such that $hx = u$. Therefore we have $gu = g(hx) = (h'g)u = h'y$, since H is normal in G. Thus $gO_1 \subseteq O_2$. Similarly for any $v \in O_2$, there exists h_1 such that $h_1 y = v$ i.e., $h_1(gx) = v$ and $g(h_1'x) = v$. Therefore $O_2 \subseteq gO_1$. This proves the lemma. $\square$

Lemma 2.2. *The action of G on $\{O_1, \ldots, O_n\}$ is transtive and the orbits of A under the action of H have the same cardinality.*

Proof. For any O_i, O_j, let $x_i \in O_i, x_j \in O_j$. Since the action of G on A is transtive we have $gx_i = x_j$ for some $g \in G$. Thus $gO_i = O_j$ by the previous lemma. This implies that $|O_i| = |O_j|$. $\square$

Remark 2.3 If $a \in A$, by Orbit-Stabilizer theorem

$$|O_1| = \frac{|H|}{|H_a|} = \frac{|H|}{|H \cap G_a|}.$$

Again $|G : HG_a| = \frac{|G|/|G_a|}{|HG_a|/|G_a|}$. Now $|G| = |G_a||A|$ and $\frac{G_a}{H\cap G_a} \equiv \frac{HG_a}{H}$ implies $|G/G_a| = |A|$ and $\frac{|HG_a|}{|G_a|} = \frac{|H|}{|H\cap G_a|}$. Combining all the facts we get

$$|G : HG_a| = \frac{|A|}{|O_1|} = r.$$

Remark 2.4 For $G = S_n$ and $H = A_n$, if K is a conjugacy class contained in H and $x \in K$ we will have $r = |G : HG_a|$. Here r is the number of conjugacy classes of x when acted by A_n. Now $A_n \subseteq HG_a \subseteq G$ implies $2 = |G : H| = |G : HG_a||HG_a : H| = r.k$, where $|G : HG_a| = r, |HG_a : H| = k$. Thus $r = 1, k = 2$ or $r = 2, k = 1$.

Remark 2.5 If G_a contains some odd cycle then we must have $H \nsubseteq HG_a$ and hence $k = 2, r = 1$ i.e., the conjugacy class of x is the same when we consider the action of A_n. On the other hand $r = 1$ implies $k = 2$ and therefore there must exist some $\sigma \in G \setminus H$ contained in G_a. Clearly σ must be an odd cycle.

Proposition 2.6. *For $\sigma \in A_n$, conjugacy class of x in S_n does not split in A_n if and only if it commutes with some odd cycle.*

Proof. The proof is precisely the remark mentioned above. □

Remark 2.7 $\sigma \in S_n$ does not commute with any odd permutation if and only if the cycle type of it consists of distinct odd integers.

Proof. Let us assume that σ does not commute with any odd cycle and $\sigma = \sigma_1\sigma_2 \ldots \sigma_r$ be its cycle decomoposition. We claim that σ commutes with σ_i's, since

$$\sigma\sigma_1(x) = \begin{cases} \sigma(y), & \text{if } x \in \sigma_1 \text{ and } \sigma_1(x) = y, \\ \sigma(x), & \text{else.} \end{cases}$$

Again

$$\sigma_1\sigma(x) = \begin{cases} \sigma(y), & \text{if } x \in \sigma_1, \\ \sigma(x), & \text{else.} \end{cases}$$

Because $x \in \sigma_1$, $\sigma(\sigma_1(x)) = \sigma(y)$. Again $x \notin \sigma_1$ implies $\sigma(x) \notin \sigma_1$ and hence $\sigma_1\sigma(x) = \sigma(x)$. Thus each cycle σ_i must be even i.e., of odd length. If there are two disjoint odd cycles of same odd length k such that $\sigma_i = (a_1a_2 \ldots a_k)$ and $\sigma_j = (b_1b_2 \ldots b_k)$, we can consider the odd permutation $\tau = (a_1b_1)(a_2b_2)\ldots(a_kb_k)$. Therefore $\sigma\tau = \tau\sigma$ and hence all the cycles must of distinct length.

Conversely let us assume that the cycle type of σ consists of distinct odd integers. . . . □

2.2 Simple Groups of Order 168

For a simple group of order 168, the number n_7 of sylow-7 subgroups must divide 24. $n_7 = 1 + 7k \mid 24$ and the fact that $n_7 \neq 1$ implies $n_7 = 8$. Therefore there are $8 \times 6 = 48$ elements of order 7 in G. If P_7 is a sylow-7 subgroup of G, $|G : N_G(P_7)| = 7$ i.e., $N_G(P_7) = 21$.

There exists some $x \in N_G(P_7) = N$ such that $o(x) = 7$. Again $|cl_N(x)| = \frac{|N|}{|C_N(x)|}$ i.e., $|cl_n(x)| = \frac{21}{7} = 3$ or $|cl_N(x)| = \frac{21}{21} = 1$. The second case can not occur since $C_N(x) = N$ implies there exists some element y of order 3 that commutes with all the elements of N. Thus $N \subseteq N_G(P_3)$, where $P_3 = \langle y\rangle$ and $n_3 = |G : N_G(P_3)| \leq 8$. This together with $n_3 = 1 + 3k \mid 56$ gives us $n_3 = 1, 4, 7$.

Lemma 2.8. *For a simple group G, if it has a subgroup of index $n \geq 3$ then $|G| \mid \frac{n!}{2}$.*

By this lemma we can discard the cases $n_3 = 4$ and $n_3 = 7$. Moreover $n_3 \neq 1$ as the group is simple. This leads us to the conclusion that $|C_N(x)| = 7$ and $|cl_N(x)| = 3$. Since there are six elements of order 7, we have two conjugacy classes-$cl(x), cl(y)$ in the subgroup N. For any other element u of order 7, there exists $g \in G$ such that $gP_7g^{-1} = \langle u\rangle$. Therfore by the same argument there are two conjugacy classes in $\langle u\rangle$ out of which three elements of order 7 are conjugate to x and rest three are conjugate to y. Summarizing all these facts we have the following proposition.

Proposition 2.9. *In a simple group of order 168, the number of conjugacy classes of elements of order 7 is precisely two.*

$$\begin{aligned}(kn)(hn')(kn)^{-1} &= k(nh)(n'n^{-1}k^{-1})\\ &= k(hn_1)(n'n^{-1}k^{-1}), \text{ since } hN = Nh\\ &= kh(n_1n'n^{-1}k^{-1})\\ &= kh(k^{-1}k)n_1(k^{-1}k)n'(k^{-1}k)n^{-1}k^{-1}\\ &= (khk^{-1})(kn_1k^{-1})(kn'k^{-1})(kn^{-1}k^{-1})\\ &= h_2n_2n_3n_4 \in HN.\end{aligned}$$

2.3 Gauss' Lemma

Theorem 2.10 (Gauss Lemma). *If R is a UFD and $F = frac(R)$, a polynomial $f(x) \in R[x]$ is irreducible in $R[x]$ if it irreducible in $F[x]$ and gcd of its coefficients is 1.*

Proof. □

Definition 2.11 A polynomial, f is said to be primitive if its content, $c(f)$ i.e. the gcd of the coefficients is 1. □

Proposition 2.12. *Content of product of two polynomials is product of the contents.*

Proof. Any polynomil f can be written as a product of a non zero scalar and a primitive polynomial, $f = c(f) \times \frac{f}{c(f)}$. We will prove the statement for primitive polynomials.

Let $f(x) = a_0 + a_1x + a_2x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + b_2x + \cdots + b_nx^n$ with $a_mb_n \neq 0$. Let us assume that p is a prime divisor of fg. The fact that $c(f) = c(g) = 1$ implies that there are least r, s such that $p \nmid a_r, p \nmid a_s$. Thus p divides a_i and b_j for $0 \leq i \leq r-1, 0 \leq j \leq s-1$. Since p divides each of the coefficients of $h(x)$, $p \mid \sum_{i+j=r+s} a_ib_j$ i.e

$$p \mid a_0b_{r+s} + a_1b_{r+s-1} + a_2b_{r+s-2} + \cdots + a_rb_s + \cdots + a_{s+r}b_0.$$

Hence we must have $p \mid a_rb_s$, a contraction to our choices of r and s. Therefore we have $c(h) = 1$. □

Lemma 2.13 (**Gauss Lemma**). *A primitive polynomial in $R[x]$ is irreducible if and only if it its irreducible in $F[x]$, where R is a UFD and F its field of fractions.*

Proof. Let us assume that f is a primitive irreducible polynomial in $R[x]$ and if possible $f(x)$ is reducible in $F[x]$ such that $f(x) = g(x)h(x)$ with $g, h \in F[x]$. We can write $g(x) = \frac{a}{b}G(x)$ and $h(x) = \frac{c}{d}H(x)$ with $a, b, c, d \in R^{\times}$ and G, H are primitive. Then $f(x) = \frac{u}{v}G(x)H(x)$ and $(u, v) = 1$. Thus together with the fact that $v.c(f) = uc(G)c(H)$ give us $u = v$ and $f(x) = G(x)H(x)$. Which is a clear contraction to the irreducibility of f in $R[x]$.

Converse is trivial. □

Theorem 2.14. *For an integral domain R, $R[x]$ is a UFD if and only if $F[x]$ is a UFD, where $F = frac(R)$.*

Corollary 2.15. *A polynomial ring over a UFD is again a UFD.*

3 818

3.1 Spec and Two Definitions of Affine Space — Ravi Vakil

When considered as an element of $Spec(A)$, a prime ideal $\mathfrak{p}$ of A will be denoted as $[\mathfrak{p}]$. Elements of A are functions on $spec(A)$ such that $a([\mathfrak{p}]) = a(mod\ \mathfrak{p})$. An element that lies on $\mathfrak{p}$ has value 0 or a function vansishing at the point $[\mathfrak{p}]$.

Ravi Vakil's definition of an affine space.

Definition 3.1 We define $\mathbb{A}^n(k) = Spec(k[x_1, x_2, \ldots, x_n])$={The set of prime ideals of $k[x_1, \ldots, x_n]$} with Zariski topology. $\square$

Definition 3.2 For $f \in \mathbb{C}[x_1, \ldots, x_n]$ and $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$,

$$Z(f) = \{\mathfrak{p} \mid f([\mathfrak{p}]) = 0\} = \{\mathfrak{p} \mid f \in \mathfrak{p}\} \text{ and } Z(I) = \{\mathfrak{p} \mid I \subseteq \mathfrak{p}\}.$$

But on the other hand we have $V(f) = \{P \in \mathbb{C}^n \mid f(P) = 0\}$. $\square$

Definition 3.3 If $T \subseteq \mathbb{A}^n(k)$ then $I(T) = \{f \in k[X_1, X_2, \ldots, X_n] \mid f(p) = 0 \text{ for all } p \in T\}$. But for $S \subseteq \mathbb{A}^n_k(\mathbb{A}^n(k)$ with the Zariski topology) we have $I(S) = \{f \in k[X_1, X_2, \ldots, X_n] \mid f([\mathfrak{p}]) = 0 \text{ for all } [\mathfrak{p}] \in S\} = \{f \in k[X_1, X_2, \ldots, X_n] \mid f \in \mathfrak{p} \text{ for all } [\mathfrak{p}] \in S\}$. Thus

$$I(S) = \bigcap_{\mathfrak{p} \in S} \mathfrak{p}.$$

$\square$

Example $\mathfrak{a}^2(\mathbb{C})$={prime ideals of $\mathbb{C}[x, y]$}. Thus we have each point (a, b) of $\mathbb{C}^2$ corresponding to $(x - a, x - b)$ and one bonus point $[0]$. (0) is contained in every prime ideal hence $[0]$ is close to each point $[\mathfrak{p}]$.

When we talk about affine variety V, it corresponds to a prime ideal $\mathfrak{p}$ such that $V(\mathfrak{p}) = V$. But with spec when we refer to an affine variety we mean something like $\text{Spec}(k[V]) = \text{Spec}\,(k[X_1, X_2, \ldots, X_n]/I(V))$. Here the prime ideals are those which contain $I(V)$.

3.2 Basis for Zariski Topology on $k[V]$

For some affine variety V, the open sets in $Spec(k[V])$ are

$$D(f) = \text{Spec}(k[V]) \smallsetminus Z(f).$$

Thus $D(f) = \{\mathfrak{p} \mid f \notin \mathfrak{p}\}$ i.e., the points where f doesn't vanish. Now the prime ideals that do not contain f are precisely those prime ideals that do not intersect the multiplicative set $S = \{1, f, f^2, \ldots\}$. More precisely these are the prime ideals that we get after localizing $k[V]$ at the multiplicative set S. Therefore we can have $D(f) = \text{Spec}(S^{-1}k[V]) = \text{Spec}(k[V]_f)$, the spectrum of the localization of the coordinate ring with respect to the multiplicative set $\{1, f, f^2, f^3, \ldots\}$.

Now the elements of $(k[V])_f$ are the functions which are defined as long as their denominators are nonzero, on $D(f)$ precisely this case occurs .

Definition 3.4 The residue field of $\mathfrak{p}$ is $\frac{k[V]_{\mathfrak{p}}}{\mathfrak{p}k[V]_{\mathfrak{p}}}$. □

Remark 3.5 The prime ideals of $(k[V])_{\mathfrak{p}}$ are precisely those which contain $\mathfrak{p}$.

3.3 Irreducible Subsets of $\mathbb{A}^2_{\mathbb{C}}$

Example By Gauss' Lemma $y - x^2$ is irreducible in $\mathbb{C}[x, y]$, since $y - x^2 \in (\mathbb{C}[x])[y]$ is irreducible and its content is $gcd(1, -x^2) = 1$. Similarly $y^2 + x^3 + x$ in $(\mathbb{C}[x])(y)$ is irreducible by Eisenstein's criterion.

Remark 3.6 We claim that the irreducible subsets of $\mathbb{A}^2_{\mathbb{C}}$ correspond to the ideals $(0), (x - a, y - b), (f(x))$ for some irreducible polynomial $f(x) \in \mathbb{C}[x, y]$. If $\mathfrak{P}$ is a prime ideal which is not principal, then we have $f, g \in \mathfrak{P}$ such that they don't share irreducible factors. By the Euclidean algorithm in $\mathbb{C}(x)[y]$ we have $1 = pf + qg$ i.e.,

$$1 = \left(\frac{p_0(x)}{u_0(x)} + \frac{p_1(x)}{u_1(x)} y + \cdots + \frac{p_n(x)}{u_n(x)} y^n \right) f(x, y) + \left(\frac{q_0(x)}{v_0(x)} + \frac{q_1(x)}{v_1(x)} y + \cdots + \frac{q_m(x)}{v_m(x)} y^m \right) g(x, y)$$

$$i.e., \ P(X) = a(x, y) f(x, y) + b(x, y) g(x, y).$$

Thus $P(x) \in \mathbb{C}[x]$ lies in $\mathfrak{P}$. Since we can factor $P(x)$ into linear factors, $x - a \in \mathfrak{P}$ for some $a \in \mathbb{C}$. Similarly for some $b \in \mathbb{C}$, $y - b \in \mathfrak{P}$. This forces $(x - a, y - b) \in \mathfrak{P}$ and hence we have $\mathfrak{P} = (x - a, y - b)$.

3.4 Spec Version of Morphisms

Remark 3.7 A polynomial map or morphism or regular map between affine varieties is defined as $\varphi : V \subseteq \mathbb{A}^n \to W \subseteq \mathbb{A}^m$ such that $\varphi(P) = (\varphi_1(P), \ldots, \varphi_m(P))$, $\varphi_i \in k[X_1, X_2, \ldots, X_n]$. For such φ we can define

$$\varphi^* : \mathrm{Spec}(k[X_1, X_2, \ldots, X_m]) \to \mathrm{Spec}(k[X_1, X_2, \ldots, X_n])$$

such that $\varphi^*(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$.