

Contents

1	Galois Theory	1
1.1	The Galois Correspondence	3
1.1.1	Field Norm and Trace	4
1.2	The Discriminant	5
2	Galois Groups of Cubics	7
3	Structure Theorem of Modules Over a PID	7
3.1	Interlude on Torsion-Freeness	8
3.2	The Structure Theorem	8
3.3	Smith Normal Form	10
4	Nakayama's Lemma	10
5	Groups of Lie Type	11
6	Products of Ideals	11
7	Induced Representations	11
7.1	Restriction	11
7.1.1	The Case of a Normal Subgroup	12
7.2	Induction and Coinduction	12
8	Noetherian Normalization	13
9	Going Up and Going Down	14
10	Flatness	17
10.1	Vector Bundles	19

1 Galois Theory

Proposition 1.0.1. Let E be the splitting field of a $f \in K[x]$. Then,

$$|\text{Aut}(E/K)| \leq [E : K]$$

with equality if and only if f is separable.

Proof. Dummit and Foote p.561. □

Lemma 1.0.2 (Independence of Characters). Let $\sigma_1, \dots, \sigma_n : G \rightarrow E^\times$ be distinct linear characters. Then in $E[G]$ the elements $\sigma_1, \dots, \sigma_n$ are linearly independent.

Proof. We proceed by induction on n . For the case $n = 1$ this is obvious because a character $G \rightarrow E^\times$ is nonzero as a map $G \rightarrow E$.

Now suppose that,

$$a_1\sigma_1 + \dots + a_n\sigma_n = 0$$

Now, this must hold for both $x \in G$ and $gx \in G$ so,

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0$$

and likewise,

$$a_1\sigma_1(gx) + \cdots + a_n\sigma_n(gx) = 0$$

but $\sigma_i(gx) = \sigma_i(g)\sigma_i(x)$. Multiplying the first equation by $\sigma_n(g)$ and subtracting we find,

$$a_1[\sigma_n(g) - \sigma_1(g)]\sigma_n(x) + \cdots + a_{n-1}[\sigma_n(g) - \sigma_{n-1}(g)]\sigma_n(x) = 0$$

Therefore by the independence of $\sigma_1, \dots, \sigma_{n-1}$ by assumption, we see that,

$$a_1[\sigma_n(g) - \sigma_1(g)] = 0$$

Therefore either $a_1 = 0$ or $\sigma_1 = \sigma_n$ for all g . Since we assumed the characters are distinct this shows that $a_1 = 0$ reducing to the $n - 1$ case so $a_i = 0$ for all i by the induction hypothesis. Thus $\sigma_1, \dots, \sigma_n$ are independent. \square

Corollary 1.0.3. Distinct field embeddings $\sigma_1, \dots, \sigma_n : K \hookrightarrow L$ are independent.

Proof. Indeed, these are independent as characters $K^\times \rightarrow L^\times$ inside the L -vectorspace of maps $K^\times \rightarrow L$. Therefore, they must be independent as maps $K \rightarrow L$. \square

Corollary 1.0.4. Let $x_1, \dots, x_n \in E$ be a basis for E/K and $n = [E : K]$. Let $G \subset \text{Aut}(E/K)$ then the vectors $v_\sigma \in E^n$ defined by $(v_\sigma)_i = \sigma(x_i)$ are independent over E .

Proof. Suppose that,

$$\sum_{\sigma \in G} \alpha_\sigma v_\sigma = 0$$

for $\alpha_\sigma \in E$. Then for each $i = 1, \dots, n$ we have,

$$\sum_{\sigma \in G} \alpha_\sigma \sigma(x_i) = \sum_{\sigma \in G} \alpha_\sigma (v_\sigma)_i = 0$$

Furthermore, we can write any $x \in E$ as,

$$x = \beta_1 x_1 + \cdots + \beta_n x_n$$

for $\beta_i \in K$. Since σ is a K -algebra map, multiplying the i^{th} equation by β_i and adding them gives,

$$\sum_{i=1}^n \beta_i \sum_{\sigma \in G} \alpha_\sigma \sigma(x_i) = \sum_{\sigma \in G} \alpha_\sigma \sum_{i=1}^n \beta_i \sigma(x_i) = \sum_{\sigma \in G} \alpha_\sigma \sigma(\beta_1 x_1 + \cdots + \beta_n x_n) = \sum_{\sigma \in G} \alpha_\sigma \sigma(x)$$

and thus,

$$\sum_{\sigma \in G} \alpha_\sigma \sigma(x) = 0$$

Since $x \in E$ is arbitrary, we see that,

$$\sum_{\sigma \in G} \alpha_\sigma \sigma = 0$$

showing that $\alpha_\sigma = 0$ for all $\sigma \in G$ by the independence of the characters thus proving that the $v_\sigma \in E^n$ are independent. \square

Corollary 1.0.5. If $G \subset \text{Aut}(E/K)$ then $|G| \leq [E : K]$.

Proposition 1.0.6. Let E/K be a field extension and $G \subset \text{Aut}(E/K)$. Then,

$$|G| = [E : K] \iff K = E^G$$

Proof. Suppose that $|G| = [E : K]$. Take $F = E^G$ giving a tower $K \subset F \subset E$. We know that $[E : K] = [E : F][F : K] = |G|$. However, $G \subset \text{Aut}(E/F)$ because each automorphism fixes F by definition. Thus $|G| \leq [E : F]$ meaning that,

$$|G| \leq [E : F] \leq [E : K] = |G|$$

proving that $[E : F] = [E : K]$ so $F = K$.

Now suppose that $K = E^G$. See Dummit and Foote p.571. □

Remark. The proof shows that in general,

$$[E : K] = |G| \cdot [E^G : K]$$

Definition 1.0.7. We say that E/K is *Galois* if $K = E^{\text{Aut}(E/K)}$ and write $\text{Gal}(E/K) := \text{Aut}(E/K)$.

Corollary 1.0.8. We see that E/K is Galois if and only if $|\text{Aut}(E/K)| = [E : K]$.

1.1 The Galois Correspondence

Proposition 1.1.1. Let E/K be a finite extension and $G \subset \text{Aut}(E/K)$. Let $F = E^G$ then E/F is Galois and $G = \text{Aut}(E/F)$.

Proof. By definition, $G \subset \text{Aut}(E/F)$. Since $F = E^G$ we have $|G| = [E : F]$ and therefore,

$$|G| \leq |\text{Aut}(E/F)| \leq [E : F] = |G|$$

proving that $|G| = |\text{Aut}(E/F)| = [E : F]$ and thus $G = \text{Aut}(E/F)$ and that E/F is Galois (note we actually automatically get that E/F is Galois because $F = E^G = E^{\text{Aut}(E/F)}$ using that $G = \text{Aut}(E/F)$). □

Proposition 1.1.2 (Galois Connection). Let E/K be a finite extension and $G = \text{Aut}(E/K)$.

$$\{\text{subgroups } H \subset G\} \begin{matrix} \xrightarrow{H \mapsto E^H} \\ \xleftarrow{F \mapsto \text{Aut}(E/F)} \end{matrix} \{\text{intermediate extensions } K \subset F \subset E\}$$

satisfy the following properties,

- (a) $H \mapsto E^H \mapsto \text{Aut}(E/E^H) = H$ meaning that

1.1.1 Field Norm and Trace

Definition 1.1.3. Let L/K be a finite extension of fields. Then we define the relative trace,

$$\mathrm{Tr}_{L/K} : L \hookrightarrow \mathrm{End}_K(L) \xrightarrow{\mathrm{tr}} K$$

and relative norm,

$$\mathrm{N}_{L/K} : L \hookrightarrow \mathrm{End}_K(L) \xrightarrow{\det} K$$

and the relative characteristic polynomial,

$$\mathrm{char}_{L/K} : L \hookrightarrow \mathrm{End}_K(L) \xrightarrow{\text{char poly}} K[x]$$

Remark. By Cayley-Hamilton, if $p = \mathrm{char}_{L/K}(\alpha)$ then $p(\alpha) = 0$. Therefore $m_\alpha \mid \mathrm{char}_{L/K}$ where m_α is the minimal polynomial of α over K .

Lemma 1.1.4. Suppose that L/K is separable. Then for any $\alpha \in L$,

$$\mathrm{char}_{L/K}(\alpha) = \prod_{\sigma: L \hookrightarrow \overline{K}} (x - \sigma(\alpha)) = m_\alpha^{\frac{[L:K]}{\deg \alpha}}$$

where the sum is taken over K -linear embeddings of L into \overline{K} .

Proof. Consider $L/K(\alpha)/K$. Then choosing a $K(\alpha)$ -basis of L decomposes L into isomorphic α -invariant K -subspaces of which there are $e = [L : K(\alpha)] = \frac{[L:K]}{\deg \alpha}$. Therefore, $\mathrm{char}_{L/K}(\alpha) = \mathrm{char}_{K(\alpha)/K}(\alpha)^e$. Furthermore, $\mathfrak{m}_\alpha \mid \mathrm{char}_{K(\alpha)/K}(\alpha)$ and they both have degree $\deg \alpha$ and are monic so $\mathfrak{m}_\alpha = \mathrm{char}_{K(\alpha)/K}$.

Now let $E/L/K$ be the Galois closure. Then $\mathrm{Hom}_K(L, K^{\mathrm{sep}}) = \mathrm{Hom}_K(L, E)$ are given by cosets of $H = \mathrm{Gal}(E/L) \subset \mathrm{Gal}(E/K)$. Thus,

$$\prod_{\sigma \in \mathrm{Hom}_K(L, E)} (x - \sigma(\alpha)) = \prod_{\sigma H \in G/H} (x - \sigma(\alpha))$$

which makes sense because any $\tau \in \sigma H$ is $\tau = \sigma\gamma$ for $\gamma \in H = \mathrm{Gal}(E/L)$ fixes L by definition so $\tau(\alpha) = \sigma(\gamma(\alpha)) = \sigma(\alpha)$. Now let $H' = \mathrm{Gal}(E/K(\alpha)) \supset H$. Then,

$$\prod_{\sigma H \in G/H} (x - \sigma(\alpha)) = \prod_{\sigma \in G/H'} \prod_{\tau \in \sigma H'/H} (x - \tau(\alpha)) = \prod_{\sigma \in G/H} (x - \sigma(\alpha))^{[L:K(\alpha)]}$$

where $|H'/H| = [L : K(\alpha)]$ because $\tau \in \sigma H'$ is $\tau = \sigma\gamma$ for $\gamma \in H' = \mathrm{Gal}(E/K(\alpha))$ fixes α by definition so $\tau(\alpha) = \sigma(\gamma(\alpha)) = \sigma(\alpha)$. Therefore,

$$\prod_{\sigma \in \mathrm{Hom}_K(L, E)} (x - \sigma(\alpha)) = \left(\prod_{G/H'} (x - \sigma(\alpha)) \right)^{[L:K(\alpha)]}$$

Now I claim that,

$$f(x) = \prod_{\sigma \in G/H'} (x - \sigma(\alpha))$$

is the minimal polynomial of α . Consider $\tau \in G$ then,

$$\tau(f(x)) = \prod_{\sigma \in G/H'} (x - \tau(\sigma(\alpha))) = \prod_{\sigma' \in G/H'} (x - \sigma'(\alpha)) = f(x)$$

so $f \in K[x]$ and clearly $f(\alpha) = 0$ (because $(x - \alpha)$ for $\sigma = \text{id}$ is a factor) so $\mathfrak{m}_\alpha \mid f$ in $K[x]$. However, $m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0$ since $m_\alpha \in K[x]$ so each $\sigma(\alpha)$ is a root of m_α . Furthermore, the $\sigma(\alpha)$ appearing in f are *distinct* because if $\sigma(\alpha) = \sigma'(\alpha)$ then $\sigma^{-1}\sigma'(\alpha) = \alpha$ so $\sigma^{-1}\sigma' \in \text{Gal}(E/K(\alpha))$ and thus $\sigma H' = \sigma' H'$. Therefore, $f \mid m_\alpha$ in $E[x]$ because each linear factor divides m_α since each $\sigma(\alpha)$ is a root of m_α . Therefore $f = m_\alpha$ and we conclude. \square

Corollary 1.1.5. Let $m_\alpha = x^n + a_1 x^{n-1} + \dots + a_n$. Then,

$$\text{Tr}_{L/K}(\alpha) = \sum_{\sigma: L \hookrightarrow \overline{K}} \sigma(\alpha) = (-1)^{[L:K]} a_1^{\frac{[L:K]}{\deg \alpha}} \quad \text{and} \quad \text{N}_{L/K}(\alpha) = \prod_{\sigma: L \hookrightarrow \overline{K}} \sigma(\alpha) = a_n^{\frac{[L:K]}{\deg \alpha}}$$

Lemma 1.1.6. Let L/K be a finite extension of fields. Let V be a finite dimensional L -vectorspace and $\varphi: L \rightarrow V$ an L -linear map. Then,

$$\text{Tr}_K(\varphi) = \text{Tr}_{L/K}(\text{Tr}_L(\varphi))$$

and likewise,

$$\det_K(\varphi) = \text{N}_{L/K}(\det_L(\varphi))$$

Proof. Choosing bases this becomes a direct computation (see Tag 0BIE). \square

Corollary 1.1.7. Given a tower of finite field extensions $F/L/K$,

$$\text{Tr}_{F/K} = \text{Tr}_{L/K} \circ \text{Tr}_{F/L} \quad \text{and} \quad \text{N}_{F/K} = \text{N}_{L/K} \circ \text{N}_{F/L}$$

1.2 The Discriminant

Lemma 1.2.1. Given a bilinear form $B: V \times V \rightarrow K$ if we choose any basis $e_1, \dots, e_n \in V$ then,

$$\Delta(B) = \det B(e_i, e_j) \in K/(K^\times)^2$$

is independent of the choice of basis.

Proof. Let $M_{ij} = B(e_i, e_j)$ and $M'_{ij} = B(e'_i, e'_j)$. There is a change of basis matrix,

$$e'_j = \sum_k C_{kj} e_k$$

and therefore,

$$M'_{ij} = \sum_{k, \ell} C_{ki} B(e_k, e_\ell) C_{\ell j} = (C^\top M C)_{ij}$$

Thus,

$$\Delta'(B) = \det M' = \det (C^\top M C) = (\det C)^2 \det M = (\det C)^2 \Delta(B)$$

so in $K/(K^\times)^2$ we have $\Delta'(B) = \Delta(B)$. \square

Lemma 1.2.2. The quadratic form B is degenerate iff $\Delta(B) = 0$.

Proof. If B is degenerate then there exists $v \in V$ such that $B(v, -) = 0$ and then extending to a basis of V we see immediately that $\Delta(B) = 0$. Conversely, if $\Delta(B) = 0$ then for some basis $e_1, \dots, e_n \in V$ the columns $B(e_i, e_j)$ are dependent meaning that there exist v_1, \dots, v_n such that,

$$\sum_j B(e_i, e_j) v_j = 0$$

for all i and thus setting $v = v_1 e_1 + \dots + v_n e_n$ we see that $B(e_i, v) = 0$ for all e_i and thus since the e_i span V we find that $B(-, v) = 0$ so B is degenerate. \square

Lemma 1.2.3. Let L/K be a finite separable extension and $e_1, \dots, e_n \in L$ a K -basis of L . Then,

$$\det(\mathrm{Tr}_{L/K}(e_i e_j)) = \det(\sigma_i(e_j))^2$$

running over $\sigma_j \in \mathrm{Hom}_K(L, K^{\mathrm{sep}})$ of which there are $[L : K]$ because L/K is separable.

Proof. Let $M_{ij} = \sigma_i(e_j)$ then,

$$A_{ij} = \mathrm{Tr}_{L/K}(e_i e_j) = \sum_k \sigma_k(e_i) \sigma_k(e_j) = \sum_k M_{ki} M_{kj} = (M^\top M)_{ij}$$

Therefore,

$$\det A = \det(M^\top M) = (\det M)^2$$

proving the proposition. □

Lemma 1.2.4. Let L/K be a finite extension of fields. Then the following are equivalent,

- (a) L/K is separable
- (b) $\mathrm{Tr}_{L/K}(xy)$ is not identically zero
- (c) the bilinear form $B_{L/K}(x, y) = \mathrm{Tr}_{L/K}(xy)$ is nondegenerate
- (d) $\Delta_{L/K} = \Delta(B_{L/K}) \neq 0$.

Proof. If $\mathrm{Tr}_{L/K}(\gamma) \neq 0$ then for any $\alpha \in L$ we have $B_{L/K}(\alpha, \gamma/\alpha) = \mathrm{Tr}_{L/K}(\gamma) \neq 0$ so $B_{L/K}$ is nondegenerate. Clearly (c) \implies (b) so we see that (b) \iff (c). Furthermore, (c) \iff (d) by a previous lemma.

Now suppose that L/K is inseparable. Then there exists an intermediate extension $L/F/K$ such that F/K is separable and L/F is purely inseparable. Then there exists some $\alpha \in L$ such that $\alpha^p \in F$ but $\alpha \notin F$. Then we have a tower $L/F(\alpha)/F/K$ which implies that,

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{F(\alpha)/F} \circ \mathrm{Tr}_{L/F(\alpha)}$$

Therefore, it suffices to show that $\mathrm{Tr}_{F(\alpha)/F} = 0$. Indeed, $[F(\alpha) : F] = p$ so $\mathrm{Tr}_{F(\alpha)/F}(1) = p = 0$ in F . Furthermore, the minimal polynomial of α^i for $0 < i < p$ is $x^p - \alpha^{ip}$ and thus $\mathrm{Tr}_{F(\alpha)/F}(\alpha^i) = 0$ showing that $\mathrm{Tr}_{F(\alpha)/F} = 0$ by linearity.

Finally, suppose that L/K is separable. Then by the previous result, it suffices to show that $\det(\sigma_i(e_j)) \neq 0$. Suppose that there exist $v_1, \dots, v_n \in K$ such that,

$$\sum_i v_i \sigma_i(e_j) = 0$$

for all j and therefore because $\{e_j\}$ span L we have,

$$\sum_i v_i \sigma_i = 0$$

so by independence of characters $v_i = 0$. Thus the square matrix $\sigma_i(e_j)$ has independent rows and thus $\det(\sigma_i(e_j)) \neq 0$. □

2 Galois Groups of Cubics

3 Structure Theorem of Modules Over a PID

Remark. In this section let R be a PID.

Proposition 3.0.1. Any submodule $M \subset R^n$ is free of rank at most n .

Proof. We prove this by induction on n . The case $n = 1$ is the definition of a PID since any submodule of R is an ideal. Now consider a submodule $M \subset R^n$ and its image $N \subset R^{n-1}$ under the projection and kernel $K \subset R$ giving,

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \longrightarrow & R^n & \longrightarrow & R^{n-1} \longrightarrow 0 \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & K & \longrightarrow & M & \longrightarrow & N \longrightarrow 0 \end{array}$$

by the case $n = 1$ we see that N is free of rank at most 1 and N is free of rank at most $n - 1$ by the induction hypothesis. Since N is projective, the sequence splits giving $M \cong K \oplus N$ which is thus free of rank at most n proving the claim. \square

Remark. The rank inequality is a general fact about modules over a domain A . If $M \subset N$ then $\text{rank}(M) \leq \text{rank}(N)$ because if $K = \text{Frac}(A)$ then,

$$M \otimes_A K \hookrightarrow M \otimes_A N$$

since K is flat over A . Therefore,

$$\text{rank}_A(M) = \dim_K M \leq \dim_K N = \text{rank}_A(N)$$

Here, rank means “rank at the generic point” which agrees with the notion of rank for free modules.

Lemma 3.0.2. Let A be a domain. Let M be a finite A -module. Then M is torsion-free if and only if M is contained in a finite free module.

Proof. If M is a submodule of R^n then clearly M is torsion-free. Assume that M is torsion-free. Let $K = \text{Frac}(A)$. Because M is torsion-free, the map $M \hookrightarrow M \otimes_A K$ is injective and $M \otimes_A K$ is a finite-dimensional K -vectorspace. Choose generators x_1, \dots, x_n of M . By clearing denominators, choose a basis $e_1, \dots, e_r \in M \otimes_A K$ such that each x_i is in the A -span of e_1, \dots, e_r . Then,

$$M \subset Ae_1 \oplus \dots \oplus Ae_r \subset M \otimes_A K$$

and the module $Ae_1 \oplus \dots \oplus Ae_r \cong A^r$ is an internal direct sum (i.e. is free) by the K -independence (and thus R -independence) of e_1, \dots, e_r . \square

Proposition 3.0.3. A finite R -module is torsion-free if and only if it is free.

Proof. Clearly free modules are torsion-free so assume that M is finite and torsion-free. By the previous lemma, there is an embedding $M \hookrightarrow R^n$ and thus by the previous result M is free as the submodule of a free module. \square

3.1 Interlude on Torsion-Freeness

Lemma 3.1.1. Let A be a domain. Any flat A -module is torsion free.

Proof. Let M be a flat A -module. Since A is a domain for any nonzero $x \in A$ the map $A \xrightarrow{x} A$ is injective. Since M is flat we see that $M \xrightarrow{x} M$ is injective so M has no x -torsion and thus M is torsion-free. \square

Lemma 3.1.2. If A is a valuation ring then M is flat if and only if M is torsion-free.

Proof. See Tag 0539. \square

Proposition 3.1.3. Let A be a Dedekind domain.

- (a) An A -module is flat if and only if it is torsion-free
- (b) A finite torsion-free A -module is finite locally free.

Proof. We know that flat implies torsion-free. Suppose that M is torsion-free. Then for each maximal ideal $\mathfrak{m} \subset A$ we know that $M_{\mathfrak{m}}$ is a torsion-free $A_{\mathfrak{m}}$ -module but $A_{\mathfrak{m}}$ is a DVR and hence a valuation ring so $M_{\mathfrak{m}}$ is flat. Thus M is flat because exactness can be checked on maximal ideals.

The second follows from the fact that finite flat modules are finitely locally free (see Tag 00NX). \square

3.2 The Structure Theorem

Remark. Again let R be a PID and let M be a finite R -module. Then consider the torsion submodule $T(M) \subset M$. We get an exact sequence,

$$0 \longrightarrow T(M) \longrightarrow M \longrightarrow M/T(M) \longrightarrow 0$$

where $M/T(M)$ is finite and torsion-free and thus free by our previous work. Thus $M/T(M) \cong R^n$ is projective so the sequence splits showing that,

$$M \cong R^n \oplus T(M)$$

where $n = \text{rank}_A(M)$ (immediate from tensoring the above sequence by K). Therefore, it suffices to classify the structure of torsion modules.

Definition 3.2.1. For each prime element $p \in R$ consider the p -torsion subgroup,

$$M_p = \{m \in T(M) \mid \exists n : p^n m = 0\}$$

Proposition 3.2.2. For any finite R -module M ,

$$T(M) = \bigoplus_p M_p$$

where only finitely many M_p are nonzero.

Proof. First suppose that $r \in M_p \cap M_q$ for distinct prime elements p and q . Then because nonzero prime ideals are maximal (since being a prime element implies irreducible) and thus $(p) + (q) = R$ since $q \notin (p)$ this is a strictly larger ideal. Therefore, if $p^n m = 0$ and $q^n m = 0$ (take n to be sufficiently large for both) then $R = (p^n, q^n) \subset \text{Ann}_A(m)$ (if $1 \in (p, q)$ then $1 \in (p, q)^{2n} \subset (p^n, q^n)$) so $1 \in \text{Ann}_A(m)$ and thus $m = 0$.

Now, since $\text{Ann}_A(m) \subset R$ is an ideal we have $\text{Ann}_A(m) = (r)$. Because $m \in T(M)$ the annihilator is nontrivial so $r \neq 0$ and if $r \in R^\times$ then $1 \in \text{Ann}_A(m)$ meaning that $m = 0$ which is in M_p for each p . Otherwise $\text{Ann}_A(m) = (r)$ is a nontrivial ideal. We apply the fact that R is a UFD to write,

$$r = p_1^{e_1} \cdots p_r^{e_r}$$

in terms of prime elements p_i . If $r = 1$ then we are done because $r = p_1^{e_1}$ and thus $p_1^{e_1} m = 0$ so $m \in M_{p_1}$. Otherwise, $(p_1, \dots, p_r) = R$ and thus taking sufficiently large n ,

$$R = (p_2^{e_2} \cdots p_r^{e_r}, \dots, p_1, \dots, p_r)^n \subset (p_1^{e_1} \cdots p_{r-1}^{e_{r-1}})$$

and thus we can write,

$$1 = \alpha_1 p_2^{e_2} \cdots p_r^{e_r} + \cdots + \alpha_r p_1^{e_1} \cdots p_{r-1}^{e_{r-1}}$$

meaning that,

$$m = \alpha_1 p_2^{e_2} \cdots p_r^{e_r} m + \cdots + \alpha_r p_1^{e_1} \cdots p_{r-1}^{e_{r-1}} m$$

where the i^{th} -term is clearly killed by $p_i^{e_i}$ and thus is in M_{p_i} proving that the M_{p_i} span $T(M)$.

Finally, the finiteness statement follows immediately from the fact that M is finitely generated and that $M_p \cap M_q = (0)$ if $p \neq q$ are distinct primes. \square

Lemma 3.2.3. Let A be an Artin local ring with principal maximal ideal $\mathfrak{m} = (\varpi)$. Then for any finite A -module M there is a decomposition,

$$M \cong \bigoplus_{i=1}^n R/(\varpi^{a_i})$$

where the numbers $a_1 \leq a_2 \leq \cdots \leq a_n$ are uniquely determined by M .

Proof. Notice that every ideal is of the form (ϖ^k) for some k . Indeed, for any proper nonzero ideal $\mathfrak{a} \subset A$ because \mathfrak{m} is the unique maximal ideal, $\mathfrak{a} \subset \mathfrak{m}$ but because $\mathfrak{m}^N = (0)$ for sufficiently large N there is a maximal power k such that $\mathfrak{a} \subset \mathfrak{m}^k$. Choose $y \in \mathfrak{a} \setminus \mathfrak{m}^{k+1}$. Thus $y = u\varpi^k$ but $y \notin \mathfrak{m}^{k+1}$ so we must have $u \notin \mathfrak{m}$ and thus u is a unit. Thus $\mathfrak{m}^k = (\varpi^k) = (y) \subset \mathfrak{a} \subset \mathfrak{m}^k$ so $\mathfrak{a} = (\varpi^k)$.

Let $\kappa = A/\mathfrak{m}$ be the residue field then we proceed by induction on,

$$n = \dim_\kappa(M \otimes_A \kappa) = \dim_\kappa M/\varpi M$$

Since A is local, by Nakayama's lemma, M can be generated by n elements. Thus if $n = 1$ then $M = A/(\varpi^{a_1})$ because the kernel of $A \twoheadrightarrow M$ is some ideal and thus of the form (ϖ^{a_1}) .

Now consider $\text{Ann}_A(M) = (\varpi^k)$ then M is an $A' = A/(\varpi^k)$ -module and there is some element $m \in M$ such that m is not killed by any smaller power of ϖ (else then $(\varpi^{k-1}) \subset \text{Ann}_A(M)$) and thus $\text{Ann}_{A'}(m) = (0)$ because it does not contain any (ϖ^i) for $i < k$. Therefore $A' \hookrightarrow M$ sending $1 \mapsto m$ is injective so we get an exact sequence,

$$0 \longrightarrow A \xrightarrow{1 \mapsto m} M \longrightarrow K \longrightarrow 0$$

of A' -modules. However A' is an injective module over itself (use Baer's criterion DO THIS!!) and thus the sequence of A' -modules is split. Therefore we get an exact sequence,

$$0 \longrightarrow \kappa \longrightarrow M \otimes_A \kappa \longrightarrow K \otimes_A \kappa \longrightarrow 0$$

and thus $\dim_\kappa(K \otimes_{A'} \kappa) = \dim_\kappa(K \otimes_A \kappa) = n - 1$ so by induction it is of the required form. Therefore, by the splitting,

$$M \cong A' \oplus K \cong A' \oplus \bigoplus_{i=1}^{n-1} A'/(\varpi^{a_i}) = A/(\varpi^k) \oplus \bigoplus_{i=1}^{n-1} A/(\varpi^{a_i})$$

with $a_1 \leq \dots \leq a_{n-1} \leq a_n$ where we set $a_n = k$.

For uniqueness, we use the fact that the clearly intrinsic decreasing sequence,

$$b_i = \dim_\kappa \varpi^i M / \varpi^{i+1} M = \#\{j \mid a_j \geq i\}$$

uniquely characterizes the sequence $a_1 \leq \dots \leq a_n$ (including the number $n = b_0$). \square

Proposition 3.2.4. Let M be a finie R -module and $p \in R$ a prime element. Then,

$$M_p \cong \bigoplus_{i=1}^n R/(p^{a_i})$$

where the numbers $a_1 \leq a_2 \leq \dots \leq a_n$ are uniquely determined by M .

Proof. Because M is finitely generated $M_p \subset M$ is finitely generated (R is Noetherian) so there is some maximum power n such that p^k kills the generators and thus all of M . Therefore, M_p is a $A = R/(p^k)$ -module. Then, A is an Artin local ring with maximal ideal (p) and M_p is a finite A -module. Therefore, the theorem follows directly from the previous lemma since $A/(p^{a_i}) = R/(p^{a_i})$ for $a_i \leq k$. \square

Theorem 3.2.5 (Structure Theorem). Let R be a PID and M be a finite R -module. Then,

$$M \cong R^r \oplus \bigoplus_p \bigoplus_{i=1}^{n_p} R/(p^{a_{p,i}})$$

where the numbers $r, n_p, a_{p,i}$ are unique and may be computed as follows,

$$r = \dim_K(M \otimes_R K) \quad n_p = \dim_{R/(p)} M_p/pM_p \quad b_{p,i} = \dim_{R/(p)} p^i M_p/p^{i+1} M_p$$

where $K = \text{Frac}(R)$ and M_p is the p -torsion submodule and the $b_{p,i}$ determine the $a_{p,i}$ as above.

3.3 Smith Normal Form

Proposition 3.3.1 (Smith Normal Form).

4 Nakayama's Lemma

Proposition 4.0.1. Let R be a (possibly noncommutative) ring and M a finitely generated left R -module and $I \subset R$ a left-ideal. Then if $I \cdot M = M$ then there exists some $r \in R$ such that $1 - r \in I$ and $rM = 0$.

Proof. \square

5 Groups of Lie Type

6 Products of Ideals

Lemma 6.0.1. Let $I, J \subset R$ be ideals. Then,

$$V(IJ) = V(I \cap J) = V(I) \cup V(J)$$

Proof. If $I \subset \mathfrak{p}$ then $\mathfrak{p} \supset I \cap J \subset IJ$ so it is clear that,

$$V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ)$$

Thus suppose that $\mathfrak{p} \supset IJ$ but $\mathfrak{p} \not\subset V(I) \cup V(J)$. Then there is $x \in I$ and $y \in J$ such that $x, y \notin \mathfrak{p}$ so that $\mathfrak{p} \not\supset I$ and $\mathfrak{p} \not\supset J$. Then $xy \in IJ \subset \mathfrak{p}$ so $xy \in \mathfrak{p}$ contradicting the primality of \mathfrak{p} and proving the claim. \square

Proposition 6.0.2. Let R be a comutative ring and $I, J \subset R$ are ideals. If any of the following are true,

- (a) $I + J = R$
- (b) $\text{nilrad}(R/IJ) = (0)$

then $I \cap J = IJ$.

Proof. If $I + J = R$ then for any $r \in I \cap J$ consider $1 = x + y$ with $x \in I$ and $y \in J$ and $r = rx + ry \in IJ$ so $I \cap J \subset IJ \subset I \cap J$ proving equality.

Now suppose that $\text{nilrad}(R/IJ) = (0)$. Consider the ideal $(I \cap J)/IJ \subset R/IJ$. I claim that it is contained in the nilradical. Indeed, for any prime \mathfrak{p} of R/IJ , that is a prime of R above IJ because $V(IJ) = V(I \cap J)$ and thus $(I \cap J)/IJ \subset \text{nilrad}(R/IJ)$ so $I \cap J = IJ$. \square

7 Induced Representations

7.1 Restriction

Remark. There is a functor $\text{Rep}_R : \mathbf{Grp}^{\text{op}} \rightarrow \mathbf{Cat}$ sending $G \mapsto \text{Rep}_R(G)$ taking $\phi : G \rightarrow H$ to the functor $\text{Res}_\phi(-) : \text{Rep}_R(H) \rightarrow \text{Rep}_R(G)$ via $\rho_W \mapsto \rho_W \circ \phi$ and $(T : W \rightarrow W') \mapsto (T : W \rightarrow W')$ which still commutes with $\rho_W \circ \phi$ by definition.

This restriction functor is just restriction of modules from the ring map $R[G] \rightarrow R[H]$.

Therefore we get a map $\text{Aut}(G)^{\text{op}} \rightarrow \text{Aut}(\text{Rep}_R(G))$ and thus a natural right action (which we turn into a left action via $\text{Aut}(G) \rightarrow \text{Aut}(G)^{\text{op}}$ sending $g \mapsto g^{-1}$) on G -representations.

Proposition 7.1.1. If $\phi : G \rightarrow H$ is surjective then $\text{Rep}_R(H) \rightarrow \text{Rep}_R(G)$ preserves irreducibles.

Proof. If W is an irreducible H -rep then if $V \subset \text{Res}_\phi(W)$ is a G -invariant subspace then $\rho_W(\phi(g)) \cdot V = V$ and thus $\rho_W(h) \cdot V = V$ so V is H -invariant because ϕ is surjective. \square

7.1.1 The Case of a Normal Subgroup

Remark. For the special case of a normal subgroup $H \subset G$ we denote the conjugation action $c : G \rightarrow \text{Aut}(H)$ and then applying the above construction we find the following.

Definition 7.1.2. Let $H \subset G$ be a normal subgroup and W an H -representation. Then for $g \in G/H$ we define $g * W$ to be the H -representation given by $\rho_W \circ c_g^{-1}$

Remark. Notice that if $g' = gh$ then $\rho_W \circ c_{g'}^{-1} = \rho_W \circ c_h^{-1} \circ c_g^{-1}$ but $\rho_W \circ c_h^{-1} \cong \rho_W$ so we get $g * W \cong g' * W$ as required. This is a manifestation of the fact that $\text{Rep}_R : \mathbf{Grp}^{\text{op}} \rightarrow \mathbf{Cat}$ is really a 2-functor sending the natural transformation (isomorphism) $\eta : \phi \rightarrow \phi'$ (which just says that $\phi' = c_h \circ \phi$ for some $h = \eta_* \in H$) to the natural isomorphism $\text{Res}_\eta(V) : \text{Res}_\phi(V) \rightarrow \text{Res}_{\phi'}(V)$ given by $v \mapsto h \cdot v$ because then,

$$h \cdot (g \cdot_\phi v) = h \cdot (\phi(g) \cdot v) = (h\phi(g)h^{-1}) \cdot (h \cdot v) = g \cdot_{\phi'} (h \cdot v)$$

Proposition 7.1.3. If $H \subset G$ is normal and V is a G -representation then $g * \text{Res}_H^G(V) \cong \text{Res}_H^G(V)$.

Proof. Consider the map $\eta : V \rightarrow V$ by sending $\eta : v \mapsto g \cdot v$. I claim this is an isomorphism $\eta : g * \text{Res}_H^G(V) \rightarrow \text{Res}_H^G(V)$. Indeed it is clearly bijective and linear. Now,

$$(g * \rho)(h) \cdot v = g^{-1}hg \cdot v \mapsto g \cdot (g^{-1}hg) \cdot v = hg \cdot v = h \cdot (g \cdot v) = \rho(h) \cdot v$$

so $\eta \circ (g * \rho)(h) = \rho(h) \circ \eta$. □

Proposition 7.1.4. Let $H \subset G$ be normal and V a G -representation. Then G/H acts on the H -subrepresentations $W \subset \text{Res}_H^G(V)$ via $W \mapsto g \cdot W$ where $g \cdot W \cong g * W$ as H -representations.

Proof. We need to show that $g \cdot W$ is a well-defined subrepresentation. First, for $v \in W$,

$$h \cdot (g \cdot v) = hg \cdot v = g(g^{-1}hg) \cdot v = g \cdot ((g^{-1}hg) \cdot v)$$

proving that $g \cdot W$ is indeed H -invariant since $g^{-1}hg \in H$ so $g^{-1}hg \cdot v \in W$ and also that $g * W \cong g \cdot W$ via $v \mapsto g \cdot v$ by the same argument above. Furthermore, if $g' = gh$ then $g' \cdot W = g \cdot (h \cdot W) = g \cdot W$ because W is H -invariant. □

Remark. It is clear that the G -invariant subspaces of V are exactly the fixed points under the G/H -action.

7.2 Induction and Coinduction

Proposition 7.2.1. Let $H \subset G$ then $R[G]$ is a free $R[H]$ -module.

Proof. Consider,

$$R[G] \cong \bigoplus_{g \in HG} gR[H]$$

as *right* $R[H]$ -modules (we can make them left modules by $R[H]^{\text{op}} \cong R[H]$) via sending $g \cdot h \mapsto gh$. This is clearly surjective because gh covers each coset. Furthermore, this is injective because if,

$$\sum_{g \in G/H} g \left(\sum_{h \in H} \alpha_{g,h} h \right) = \sum_{g \in G/H} \sum_{h \in H} \alpha_{g,h} gh = 0$$

but there is an bijection $G/H \times H \rightarrow G$ via $(g, h) \mapsto gh$ then $\alpha_{g,h} = 0$. Finally, this map is $R[H]$ -linear because $g \cdot hh' \mapsto gh h' = (gh) \cdot h'$. □

Proposition 7.2.2. If $H \subset G$ is normal then for any H -representation W ,

$$\operatorname{Res}_H^G \left(\operatorname{Ind}_H^G (W) \right) \cong \bigoplus_{g \in G/H} g * W$$

Proposition 7.2.3. If $H \subset G$ is normal then for any G -representation V ,

$$\operatorname{Ind}_H^G \left(\operatorname{Res}_H^G (V) \right) \cong R[G/H] \otimes_R V$$

as $R[G]$ -modules.

Proof. Consider the map, $\operatorname{Ind}_H^G \left(\operatorname{Res}_H^G (V) \right) \cong R[G] \otimes_{R[H]} V \rightarrow R[G/H] \otimes_R V$ defined by,

$$g \otimes v \mapsto [g] \otimes g \cdot v$$

This is well-defined because,

$$gh \otimes v \mapsto [gh] \otimes gh \cdot v \quad \text{and} \quad g \otimes (h \cdot v) \mapsto [g] \otimes gh \cdot v = [gh] \otimes gh \cdot v$$

This is clearly surjective and both sides are free R -modules of equal rank so it is an isomorphism. \square

(DEFINITION OF INDUCTION AND COINDUCTION) (WHEN ARE THEY EQUAL) (EXPLICIT DESCRIPTIONS) (CHARACTER FORMULAE) (FORMULA FOR $\operatorname{IND}(\operatorname{RES})$) (NON-NORMAL CASE?)

8 Noetherian Normalization

Theorem 8.0.1. Let A be a finitely generated K -algebra domain. Then there are algebraically independent $x_1, \dots, x_d \in A$ where $d = \dim A$ such that,

$$K[x_1, \dots, x_d] \subset A$$

is a finite extension of domains.

Proof. We proceed by induction on the number of generators of A as a K -algebra. If $n = 0$ then $A = K$ and we are done. Now we apply an induction hypothesis and assume that A is generated by n elements y_1, \dots, y_n over K . If these are algebraically independent then we are done. Otherwise there is some relation $f \in K[x_1, \dots, x_n]$ such that,

$$f(y_1, \dots, y_n) = 0$$

in A . Let $z_i = y_i - y_n^{r^i}$ for $i < n$. Then obviously,

$$f(z_1 + y_n^r, \dots, z_{n-1} + y_n^{r^{n-1}}, y_n) = 0$$

The monomials in this expansion are of the form,

$$\alpha \left(\prod_{i=1}^{n-1} (z_i + y_n^{r^i})^{a_i} \right) y_n^{a_n} = \alpha y_n^{a_n + a_1 r + \dots + a_{n-1} r^{n-1}} + \dots$$

However the exponent of y_n encodes a unique base r number if we choose r larger than every exponent in f . Therefore, there is only one term of f that can contribute to this largest y_n exponent

term (each monomial has a different y_n exponent). Dividing by α we get a monic polynomial $f' \in K[z_1, \dots, z_{n-1}][x]$ such that $f'(y_n) = 0$ and thus y_n is integral over $K[z_1, \dots, z_{n-1}]$. By using the induction hypothesis, there exist algebraically independent $x_1, \dots, x_d \in K[z_1, \dots, z_{n-1}]$ (the dimensions are the same because the extension is integral) such that,

$$K[x_1, \dots, x_d] \subset K[z_1, \dots, z_{n-1}] \subset A$$

is a sequence of integral extensions proving the claim for A and thus for all A by induction on the number of generators. \square

9 Going Up and Going Down

Lemma 9.0.1. Let $A \subset B$ be an integral extension of domains. Then A is a field iff B is a field.

Proof. Let A be a field. Let $b \in B$ be nonzero then b is integral over A so,

$$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$$

By dividing though by b we may assume that $a_0 \neq 0$ and thus $a_0 \in A$ is invertible so,

$$b^{-1} = (-a_0)^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1) \in B$$

proving that B is a field. If B is a field then for any nonzero $a \in A$ we have $a^{-1} \in B$ is integral over A so,

$$a^{-n} + c_{n-1}a^{-n+1} + \dots + c_0 = 0$$

and therefore,

$$a^{-1} = -(c_{n-1} + \dots + a_0 a^{n-1}) \in A$$

so A is a field. \square

Remark. Notice that if B is a domain then any subring $A \subset B$ is automatically a domain.

Lemma 9.0.2. Let $f : A \rightarrow B$ be an integral map of rings and $\mathfrak{p} \subset B$ a prime. Then $f^{-1}(\mathfrak{p})$ is maximal if and only if \mathfrak{p} is maximal.

Proof. Indeed, consider $A/f^{-1}(\mathfrak{p}) \subset B/\mathfrak{p}$ which is an integral extension of domains. Thus \mathfrak{p} is maximal iff B/\mathfrak{p} is a field iff $A/f^{-1}(\mathfrak{p})$ is a field iff $f^{-1}(\mathfrak{p})$ is maximal. \square

Proposition 9.0.3 (Lying Over). Let $f : A \hookrightarrow B$ be an integral extension of rings. Then the continuous map $f^* : \text{Spec}(B) \rightarrow \text{Spec}(A)$ is surjective.

Proof. Let $\mathfrak{p} \subset A$ be a prime and $B_{\mathfrak{p}} = S^{-1}B$ for $S = A \setminus \mathfrak{p}$. Consider the diagram,

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \hookrightarrow & B_{\mathfrak{p}} \end{array}$$

where the bottom extension is integral and injective because localization is exact. Since $A_{\mathfrak{p}}$ is a nonzero ring so is $B_{\mathfrak{p}}$ because $A_{\mathfrak{p}} \hookrightarrow B_{\mathfrak{p}}$. Therefore, there exists a maximal ideal $\mathfrak{m} \subset B_{\mathfrak{p}}$. Then \mathfrak{m} pulls back to a maximal ideal in $A_{\mathfrak{p}}$ which must be $\mathfrak{p}A_{\mathfrak{p}}$ since $A_{\mathfrak{p}}$ is local and thus under $A \rightarrow A_{\mathfrak{p}} \rightarrow S^{-1}B$ we see that $\mathfrak{m} \mapsto \mathfrak{p}$. By commutativity the pullback of \mathfrak{m} in B maps to \mathfrak{p} . \square

Corollary 9.0.4 (Going Up). If $f : A \rightarrow B$ is an integral map of rings then f satisfies going up and $f^*(V(I)) = V(f^{-1}(I))$.

Proof. Let $I \subset B$ be an ideal. Consider $\mathfrak{p} \supset f^{-1}(I)$ and the map $A/f^{-1}(I) \hookrightarrow B/\mathfrak{p}$ which is an integral extension of rings. Thus $\text{Spec}(B/I) \rightarrow \text{Spec}(A/f^{-1}(I))$ is surjective. If $\mathfrak{q} \in V(I)$ then $f^{-1}(\mathfrak{q}) \supset f^{-1}(I)$ so $f^*(V(I)) \subset V(f^{-1}(I))$ and the surjectivity proves that $f^*(V(I)) = V(f^{-1}(I))$. In particular, if $I = \mathfrak{q}$ is prime then we recover going up. Namely if $\mathfrak{p} = f^{-1}(\mathfrak{q})$ and $\mathfrak{p}' \supset \mathfrak{p}$ then there exists $\mathfrak{q}' \supset \mathfrak{q}$ such that $\mathfrak{q}' \mapsto \mathfrak{p}'$. \square

Remark. Therefore the image is closed because if $Z \subset \text{Spec}(B)$ is closed then $Z = V(I) = \text{Spec}(B/I)$ and $\text{Spec}(B/I) \rightarrow \text{Spec}(A)$ factors as $\text{Spec}(B/I) \rightarrow \text{Spec}(A/f^{-1}(I)) \rightarrow \text{Spec}(A)$ and $f^*(V(I)) = V(f^{-1}(I))$ meaning $\text{Spec}(B/I) \rightarrow \text{Spec}(A/f^{-1}(I))$ is surjective so the image is closed.

Proposition 9.0.5 (Incomparability). If $A \rightarrow B$ is an integral map and $\mathfrak{p} \subset \mathfrak{p}'$ are primes of B above $\mathfrak{q} \subset A$ then $\mathfrak{p} = \mathfrak{p}'$.

Proof. Since $A/\mathfrak{q} \hookrightarrow B/\mathfrak{p}$ is an integral extension of domains then $(A/\mathfrak{q})_{\mathfrak{q}} \hookrightarrow (B/\mathfrak{p})_{\mathfrak{q}}$ is an integral extension of domains with $(A/\mathfrak{q})_{\mathfrak{q}}$ a field so $(B/\mathfrak{p})_{\mathfrak{q}}$ is a field. Therefore $\mathfrak{p}' = \mathfrak{p}$ since there is a unique prime ideal in a field and $\text{Spec}((B/\mathfrak{p})_{\mathfrak{q}}) \rightarrow \text{Spec}(B)$ is injective. \square

Corollary 9.0.6. If $f : A \hookrightarrow B$ is an integral extension of rings then $\dim A = \dim B$.

Proof. Lying over + going up imply $\dim A \leq \dim B$ and incomparability implies $\dim B \leq \dim A$. \square

Proposition 9.0.7 (Going Down). If $f : A \hookrightarrow B$ is an integral extension of domains and A is integrally closed (a normal domain). Let L/K be the extension of fraction fields. Then,

- (a) if L/K is normal and B is the integral closure of A in L then the fibers of $\text{Spec}(B) \rightarrow \text{Spec}(A)$ are acted on transitively by $G = \text{Gal}(L/K)$
- (b) f satisfies going down.

(DO THIS PROPERLY!!!!!!)

Proof. Let K'/K be Galois and B integrally closed. For each prime $\mathfrak{q} \subset B$ I claim that the fibers of $\text{Spec}(B') \rightarrow \text{Spec}(B)$ are finite (THIS HOLDS IF NOETHERIAN).

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the primes above \mathfrak{p}_1 ordered such that $\mathfrak{p}_1 \not\supset \mathfrak{p}_j$ for $j > 1$ i.e. \mathfrak{p}_1 is minimal (there are no relations by part (a) so there is actually no requirement on the order). Then by prime avoidance, there is some,

$$x \in \mathfrak{p}_1 \setminus \bigcup_{i=2}^n \mathfrak{p}_i$$

otherwise \mathfrak{p}_1 would lie above some \mathfrak{p}_j for $j > 1$. Now consider,

$$y = \prod_{\sigma \in G} \sigma(x)$$

Then $y \in (K')^G = K$. Therefore,

$$y \in \mathfrak{p}_1 \cap K = \mathfrak{p}_1 \cap B' \cap K = \mathfrak{p}_1 \cap B = \mathfrak{q}$$

because $B' \cap K = B$ since B is integrally closed in K . Therefore, $y \in \mathfrak{p}_i$ for each i meaning that for each i there is some $\sigma(x) \in \mathfrak{p}_i$ and thus $x \in \sigma^{-1}(\mathfrak{p}_i)$. However, $\sigma^{-1}(\mathfrak{p}_i) = \mathfrak{p}_j$ for some j since it is a prime lying above \mathfrak{q} . However, $x \in \mathfrak{p}_j$ and thus $\mathfrak{p}_j = \mathfrak{p}_1$. Therefore $\mathfrak{p}_i = \sigma(\mathfrak{p}_1)$ so the Galois group acts transitively.

Now consider part 6. We may assume that L/K is finite since we can always write L as a union of finite extensions. Suppose we have prime ideals \mathbb{P} and \mathbb{P}' of B both above \mathfrak{p} . Assume that $\sigma_i(\mathbb{P}) \neq \mathbb{P}'$ for all i running over the finite group $\text{Aut}(L/K)$. By 2, $\mathbb{P}' \not\subset \sigma_i(\mathbb{P})$ so there exists $x \in \mathbb{P}'$ such that $x \notin \sigma_i(\mathbb{P})$. Take,

$$y = \prod_{i=1}^n \sigma_i(x)$$

and thus $\sigma(y) = y$ which implies that $y^{p^n} \in K$ for $\text{char } K = p$. Since x is integral over A we know that y^{p^n} is integral over A . But A is integrally closed so $y^{p^n} \in A \cap \mathbb{P}' = \mathbb{P}$ then $y \in \mathfrak{p} \subset \mathbb{P}$ which is a prime ideal so $\sigma_i(x) \in \mathbb{P}$ for some i and thus $x \in \sigma_i^{-1}(\mathbb{P})$ a contradiction.

For part 5. we have integral domains $A \subset B$. Let $K = \text{Frac}(A)$ and $L = \text{Frac}(B)$ and let L_1 be the normal closure of K . Take B_1 to be the integral closure of A inside L_1 . Suppose we have a prime $\mathfrak{p} \subset \mathfrak{p}'$ in A and \mathbb{P}' above \mathfrak{p}' . Furthermore, we can find $\mathbb{P}_1 \subset \mathbb{P}'_1$ in B_1 above $\mathfrak{p} \subset \mathfrak{p}'$ by surjectivity of the spec map and the going up property and also \mathbb{P}'_1 in B_1 above \mathbb{P}' in B . Now \mathbb{P}'_1 and \mathbb{P}_1 both lie above the same prime of A so there is an automorphism $\sigma \in \text{Aut}(L_1/K)$ such that $\mathbb{P}'_1 = \sigma(\mathbb{P}_1)$. Thus,

$$\sigma(\mathbb{P}_1) \subset \sigma(\mathbb{P}'_1) = \mathbb{P}'_1$$

Define $\mathbb{P} = \sigma(\mathbb{P}_1) \cap B \subset \sigma(\mathbb{P}'_1) = \mathbb{P}'_1$. Thus, $\mathbb{P} \subset \mathbb{P}'_1 \cap B = \mathbb{P}'$. Finally,

$$\mathbb{P} \cap A = \sigma(\mathbb{P}_1) \cap B \cap A = \sigma(\mathbb{P}_1) \cap A = \sigma(\mathbb{P}_1 \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p}$$

which satisfies the going down property. □

Example 9.0.8. Let $C = \text{Spec}(R)$ with $R = k[x, y]/(y^2 - x^2(x+1))$ be the nodal cubic curve and $\widetilde{C} = \text{Spec}(k[t])$ its normalization where $\widetilde{C} \rightarrow C$ is given by $x \mapsto t^2 - 1$ and $y \mapsto t(t^2 - 1)$. This is dominant so $R \subset k[t]$. Then consider the map $\mathbb{A}^2 = \widetilde{C} \times \mathbb{A}^1 \rightarrow C \times \mathbb{A}^1$ given by,

$$A = R[z] = k[x, y, z]/(y^2 - x^2(x+1)) \hookrightarrow k[t, z] = B$$

This is an integral extension of domains because $R \hookrightarrow k[t]$ is finite (also $t^2 = x + 1$) and therefore satisfies lying over, incomparability, and going up. However, I claim it does not satisfy going down (and indeed A is not normal). Visualize this map as the plane mapping down to the plane with the lines $t = 1$ and $t = -1$ glued together. Consider the diagonal line L cut out by $\mathfrak{q} = (t - z) \subset B$. Then its image \bar{L} in A is a line cut out by the ideal $\mathfrak{p}' = (x - z^2 + 1, y - z(z^2 - 1))$ wrapping around and intersecting the singular line twice. Therefore the preimage of \bar{L} is $L \cup (-1, 1) \cup (1, -1)$. The point $\mathfrak{p} = (x, y, z - 1)$ is on the image of this line so $\mathfrak{p}' \subset \mathfrak{p}$ and is mapped to by the point $\mathfrak{P} = (t + 1, z - 1)$ (this is $(-1, 1)$ in the plane). However, I claim that there is no prime $\mathfrak{P}' \subset \mathfrak{P}$ with $\mathfrak{P}' \mapsto \mathfrak{p}'$. Indeed, the only height 1 prime (there is a unique height zero prime (0) and height 2 primes are maximal and thus map to height 2 primes) mapping to \mathfrak{p}' is \mathfrak{q} because the map is generically injective over \bar{L} (injective exactly away from the points $(x, y, z - 1)$ and $(x, y, z + 1)$).

More geometrically, this means that $f : \text{Spec}(B) \rightarrow \text{Spec}(A)$ is not open (going down implies “stability under generalization” which for finite type maps is equivalent to f being open). Indeed, let $U = L^C$ be the complement of the line. Then $f(U) = \bar{L}^C \cup \{(0, 0, 1), (0, 0, -1)\}$ is not open.

10 Flatness

Definition 10.0.1. A module M over a ring A is *faithfully flat* if any sequence of A -modules,

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3$$

is exact if and only if the sequence,

$$N_1 \otimes_A M \xrightarrow{f \otimes \text{id}_M} N_2 \otimes_A M \xrightarrow{g \otimes \text{id}_M} N_3 \otimes_A M$$

is also exact.

Remark. The “only if” direction immediately implies that M is flat over A so faithful flatness says additionally that tensoring cannot “make a sequence exact”.

Lemma 10.0.2. Let M be a flat A -module. Then the following are equivalent,

- (a) M is faithfully flat
- (b) for any A -module N if $M \otimes_A N = 0$ then $N = 0$
- (c) $\mathfrak{m}M \neq M$ for every maximal ideal $\mathfrak{m} \subset A$.

Proof. We first show the equivalent of (a) and (b). Assuming (a) if $M \otimes_A N = 0$ then the sequence,

$$0 \longrightarrow N \longrightarrow 0$$

becomes exact after tensoring and therefore it was already exact so $N = 0$ proving (b). Conversely, suppose that,

$$N_1 \otimes_A M \xrightarrow{f \otimes \text{id}_M} N_2 \otimes_A M \xrightarrow{g \otimes \text{id}_M} N_3 \otimes_A M$$

is exact. Then $(g \circ f) \otimes_A M = 0$ so $\text{im}(g \circ f) \otimes_A M = \text{im}((g \circ f) \otimes \text{id}_M) = 0$ by flatness so by assumption $\text{im}(g \circ f) = 0$ and thus $g \circ f = 0$. Furthermore, by flatness

$$(\ker g / \text{im } f) \otimes_A M = \ker(g \otimes \text{id}_M) / \text{im}(f \otimes \text{id}_M) = 0$$

and thus $\ker g = \text{im } f$ so the original sequence is exact proving (a).

Now we show that (b) and (c) are equivalent. Assuming (b) let $\mathfrak{m} \subset A$ be a maximal ideal. Since $A/\mathfrak{m}_A \neq 0$ we have $M \otimes_A A/\mathfrak{m}_A \neq 0$ by (b) so $\mathfrak{m}M \neq M$ proving (c). Conversely, suppose that $M \otimes_A N = 0$ with $N \neq 0$. Then there is some nonzero $x \in N$ and we have $M \otimes_A Ax \hookrightarrow M \otimes_A N = 0$ so $M \otimes_A Ax = 0$. Let $I = \text{Ann}_A(x)$ then $A/I \xrightarrow{\sim} Ax$ so $M \otimes_A A/I = 0$. Since $x \neq 0$ the ideal $I \subset A$ does not contain 1 so we can choose a maximal ideal $\mathfrak{m} \supset I$. Then $A/I \twoheadrightarrow A/\mathfrak{m}$ so $M \otimes_A A/I \twoheadrightarrow M \otimes_A A/\mathfrak{m}$ but $M \otimes_A A/I = 0$ so $M \otimes_A A/\mathfrak{m} = 0$ showing that $\mathfrak{m}M = M$. \square

Proposition 10.0.3. Let $\varphi : A \rightarrow B$ be flat local map of local rings and M a nonzero finite B -module. Then M is flat over A if and only if M is faithfully flat over A .

Proof. Faithfully flat modules are flat so it suffices to show that if M is A -flat it is faithfully flat over A . Because $\mathfrak{m}_A \subset A$ is the unique maximal ideal it suffices to show that $\mathfrak{m}_A M \neq M$. Suppose that $\mathfrak{m}_A M = M$ then $M \otimes_A A/\mathfrak{m}_A = 0$. Then there is a surjection, $B/\mathfrak{m}_A B \twoheadrightarrow B/\mathfrak{m}_B$. Therefore, there is a surjection, $M \otimes_B B/\mathfrak{m}_A B \twoheadrightarrow M \otimes_B B/\mathfrak{m}_B$. However,

$$M \otimes_B B/\mathfrak{m}_A B = M \otimes_B (B \otimes_A A/\mathfrak{m}_A) = M \otimes_A A/\mathfrak{m}_A = 0$$

and hence $M \otimes_B B/\mathfrak{m}_B = 0$ meaning $\mathfrak{m}_B M = M$. Since M is a finite B -module by Nakayama $M = 0$ giving a contradiction. This conclusion holds without A -flatness of M but then if M is A -flat the property $\mathfrak{m}_A M \neq M$ implies that M is faithfully flat over A . \square

Corollary 10.0.4. Let $\varphi : A \rightarrow B$ be a flat local map of local rings. Then φ is faithfully flat.

Proof. This is immediate from the previous proposition but we can also prove it directly as follows. We want to show that for any A -module N we have $B \otimes_A N = 0$ implies that $N = 0$. First we reduce to the case that N is finitely generated. If N is not finitely generated then for every $N' \subset N$ finitely generated consider $B \otimes_A N' \subset B \otimes_A N$ (because B is flat it is still injective) but $B \otimes_A N = 0$ so $B \otimes_A N' = 0$. Therefore, if we can prove the claim for finitely generated N' then we would conclude that $N' = 0$ proving that $N = 0$ because for each $x \in N$ the submodule $Ax \subset N$ is zero.

Thus we may assume that N is finitely generated. Consider the injection of fields $A/\mathfrak{m}_A \hookrightarrow B/\mathfrak{m}_B$. Since A/\mathfrak{m}_A -module $N \otimes_A A/\mathfrak{m}_A$ is a flat A/\mathfrak{m}_A -module since A/\mathfrak{m}_A is a field there is an injection,

$$N \otimes_A A/\mathfrak{m}_A \hookrightarrow (N \otimes_A A/\mathfrak{m}_A) \otimes_{A/\mathfrak{m}_A} B/\mathfrak{m}_B = N \otimes_A B/\mathfrak{m}_B = (N \otimes_A B) \otimes_B B/\mathfrak{m}_B$$

Since $N \otimes_A B = 0$ we see that $N \otimes_A A/\mathfrak{m}_A = 0$. Therefore $N = \mathfrak{m}_A N$ and N is finitely generated so by Nakayama we see that $N = 0$ proving the claim. \square

Indeed, φ is faithfully flat. If M is an A -module such that $M \otimes_A B = 0$ then for every finitely generated submodule $M' \subset M$ we have $M' \otimes_A B \subset M \otimes_A B = 0$ (injective by flatness). Consider the injection of fields $\kappa_A \hookrightarrow \kappa_B$. Since $M' \otimes_A \kappa_A$ is a flat κ_A -module (κ_A is a field) we get an injection,

$$M' \otimes_A \kappa_A \hookrightarrow M' \otimes_A \kappa_B = (M' \otimes_A B) \otimes_B \kappa_B = 0$$

and therefore $M' \otimes_A \kappa_A = 0$ and thus $M' = 0$ by Nakayama. Therefore $M = 0$ so φ is faithfully flat.

Proposition 10.0.5. Let $\varphi : A \rightarrow B$ be flat. Then the following are equivalent,

- (a) φ is faithfully flat
- (b) $\varphi^* : \text{Spec}(B) \rightarrow \text{Spec}(A)$ is surjective
- (c) $\text{mSpec}(A) \subset \text{im } \varphi$ meaning every maximal ideal is in the image.

Proof. Suppose that φ is faithfully flat. For any $\mathfrak{p} \in \text{Spec}(A)$ we know that $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \neq 0$ so $B \otimes_A A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \neq 0$ by faithful flatness and therefore $\text{Spec}(B \otimes_A A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})$ is nonempty proving that the fiber over \mathfrak{p} is nonempty so $\text{Spec}(B) \rightarrow \text{Spec}(A)$ is surjective. Thus (a) implies (b). It is clear that (b) implies (c). Now suppose that $\text{mSpec}(A) \subset \text{im } \varphi$. Since B is a flat A -module to show that B is faithfully flat it suffices to show that $\mathfrak{m}B \neq B$ for all maximal ideals $\mathfrak{m} \subset A$. For each maximal $\mathfrak{m} \subset A$ there is some $\mathfrak{p} \subset B$ so that $\varphi^{-1}(\mathfrak{p}) = \mathfrak{m}$ and thus $B/\mathfrak{m}B \twoheadrightarrow B/\mathfrak{p}$ is nonzero so $\mathfrak{m}B \neq B$ (the fiber $\text{Spec}(B \otimes_A A/\mathfrak{m})$ is nonempty so $B/\mathfrak{m}B = B \otimes_A A/\mathfrak{m} \neq 0$). \square

Proposition 10.0.6 (Going Down). Any flat ring map $\varphi : A \rightarrow B$ satisfies going down.

Proof. Going down is equivalent to surjectivity of $\text{Spec}(B_{\mathfrak{p}}) \rightarrow \text{Spec}(A_{\varphi^{-1}(\mathfrak{p})})$ for each prime $\mathfrak{p} \subset B$ which follows because $A_{\varphi^{-1}(\mathfrak{p})} \rightarrow B_{\mathfrak{p}}$ is a flat local map and hence faithfully flat. \square

10.1 Vector Bundles

Proposition 10.1.1. Let $\varphi : A \rightarrow B$ be a flat local map of local rings. Let M be a finitely presented B -module which is flat over A . Suppose that $M/\mathfrak{m}_A M$ is a free $B/\mathfrak{m}_A B$ -module. Then M is a free M -module.

Proof. Choose an isomorphism,

$$(B/\mathfrak{m}_A B)^n \xrightarrow{\sim} M/\mathfrak{m}_A M$$

and choose a lift to a map $B^n \rightarrow M$ inducing a sequence,

$$0 \longrightarrow K \longrightarrow B^n \longrightarrow M \longrightarrow C \longrightarrow 0$$

Since M is finitely-presented, K and C are finite B -modules. From the exact sequence, $C/\mathfrak{m}_A C = 0$ and thus,

$$C/\mathfrak{m}_A C \rightarrow C/\mathfrak{m}_B C$$

proves that $C = \mathfrak{m}_B C$ and thus by Nakayama's lemma $C = 0$. Therefore, we have a short exact sequence,

$$0 \longrightarrow K \longrightarrow B^n \longrightarrow M \longrightarrow 0$$

Since M is flat over A this sequence remains exact after applying $-\otimes_A (A/\mathfrak{m}_A)$ and thus $K/\mathfrak{m}_A K = 0$ and hence $K/\mathfrak{m}_B K = 0$. Since K is a finite B -module, by Nakayama, we see that $K = 0$ and hence $B^n \xrightarrow{\sim} M$. \square

Corollary 10.1.2. Let $f : X \rightarrow Y$ be a flat map of schemes and \mathcal{F} a coherent \mathcal{O}_X -module flat over Y . Suppose that $\mathcal{F}|_{X_y}$ is a vector bundle on X_y for some y . Then there is an open neighborhood $U \subset X$ of X_y such that $\mathcal{F}|_U$ is a vector bundle.

Proof. Since \mathcal{F} is coherent, it suffices to show that \mathcal{F}_x is a free $\mathcal{O}_{X,x}$ -module for each $x \in X_y$ which follows immediately from the previous result. \square

Example 10.1.3. Consider $X = \mathbb{A}^3 \setminus \{(0,0,0)\} \rightarrow \mathbb{A}^1 = \text{Spec}(k[z])$ and $\mathcal{F} = \widetilde{(x,y)}$. This sheaf is obviously flat but its fiber over $z = 0$ is a vector bundle since it is \mathcal{O}_X away from $x = y = 0$. However, it is not a vector bundle on any other fiber.

Corollary 10.1.4. Let $f : X \rightarrow Y$ be a flat and proper map of schemes and \mathcal{F} a coherent \mathcal{O}_X -module flat over Y . Suppose that $\mathcal{F}|_{X_{y_0}}$ is a vector bundle on X_{y_0} for some $y_0 \in Y$. Then there is an open $y_0 \in V \subset Y$ such that $\mathcal{F}|_{X_V}$ is a vector bundle. In particular for all $y \in V$ we have that $\mathcal{F}|_{X_y}$ is a vector bundle.

Proof. Using the previous result, it suffices to show that the set,

$$V = \{y \in Y \mid \mathcal{F}|_{X_y} \text{ is a vector bundle}\}$$

is open. For any $y \in V$ there is an open neighborhood $X_y \subset U \subset X$ so that $\mathcal{F}|_U$ is a vector bundle and thus $y \in f(U^c)^c \subset V$ is open because f is closed. \square

Example 10.1.5. Let $\pi_1 : X = \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1 = S$ be the projection. Let $x = X$ be a point and $\mathcal{I} \subset \mathcal{O}_X$ the ideal sheaf of $x = (0,0) \in X$. For each fiber X_t with $t \neq 0$ we have $\mathcal{I}|_{X_t} = \mathcal{O}_{X_t}$ is a vector bundle. However, \mathcal{I} is not a vector bundle so we cannot have $\mathcal{I}|_{X_0}$ be a vector bundle by the above result. I claim that \mathcal{I} is π_1 -flat. This is clear on $X \setminus \{x\}$ so I consider the local structure around x . On a dense open we have the following algebra problem,

$$A = k[x]_{(x)} \rightarrow k[x,y]_{(x,y)} = B \quad \text{with the ideal} \quad I = \mathfrak{m}_B = (x,y) \subset k[x,y]_{(x,y)}$$

I claim that I is flat over A . There is an exact sequence,

$$0 \longrightarrow B \xrightarrow{(y-x)} B^2 \xrightarrow{(x \ y)} I \longrightarrow 0$$

Then applying Tag 00MK we just need to show that $B/\mathfrak{m}_A B \rightarrow (B/\mathfrak{m}_A B)^2$ is injective which is true because y is a non zero-divisor on $B/\mathfrak{m}_A B$. Thus I is A -flat. Furthermore, there is an exact sequence,

$$0 \longrightarrow (B/\mathfrak{m}_A B) \xrightarrow{(y \ 0)} (B/\mathfrak{m}_A B)^2 \xrightarrow{(0 \ y)} I/\mathfrak{m}_A I \longrightarrow 0$$

Therefore, we get the local structure,

$$I/\mathfrak{m}_A I \cong k \oplus k[y]_{(y)}$$

but its image in $B/\mathfrak{m}_A B$ is just (y) which is locally free. This we see that $\mathcal{S}|_{X_0} \cong \mathcal{O}_{X_0}(-1) \oplus \iota_* k$ which has degree zero as it must because $\mathcal{S}|_{X_t} \cong \mathcal{O}_{X_t}$ for $t \neq 0$ and degree is constant in flat families.

Example 10.1.6. Consider a degeneration,

$$f : X = \text{Proj} \left(k[t][X, Y, Z]/(XY - tZ^2) \right) \rightarrow \text{Spec}(k[t]) = S$$

with X smooth and f flat and proper but f has a singular fiber over $t = 0$. Then there is a sequence,

$$0 \longrightarrow f^* \Omega_S^1 \longrightarrow \Omega_X \longrightarrow \Omega_{X/S} \longrightarrow 0$$

Now $\Omega_{X/S}|_{X_t} = \Omega_{X_t}$ is a vector bundle for the smooth fibers ($t \neq 0$). However, $\Omega_{X/S}|_{X_0} = \Omega_{X_0}$ is not a vector bundle since X_0 is singular. I claim that $\Omega_{X/S}$ is flat over S . We consider the local structure, on the chart $D_+(Z)$. Let $A = k[t]$ and $B = k[t][x, y]/(xy - t)$ then the above exact sequence becomes,

$$0 \longrightarrow B dt \xrightarrow{xdy + ydx} B dx \oplus B dy \longrightarrow \Omega_{D_+(Z)/S} \longrightarrow 0$$

Therefore,

$$M = \Omega_{D_+(Z)/S} = (B dx \oplus B dy)/(xdy + ydx)$$

Thus the rank jumps at $\mathfrak{m} = (x, y)$. However, I claim that M is flat over A . Applying Tag 00MK we just need to show that,

$$(B/tB)_{\mathfrak{m}} dt \rightarrow (B/tB)_{\mathfrak{m}} dx \oplus (B/tB)_{\mathfrak{m}} dy$$

is injective. Indeed, if $f dt \mapsto 0$ then $fx = 0$ and $fy = 0$ in $(B/tB)_{\mathfrak{m}} = (k[x, y]/(xy))_{\mathfrak{m}}$. Then $f \in \text{Ann}(x) \cap \text{Ann}(y) = (y) \cap (x) = (xy)$ so $f = 0$ in $(B/tB)_{\mathfrak{m}}$. Thus the map is injective.

Remark. We saw in the first example that a smooth proper map can have a flat ideal sheaf fail to be a vector bundle. However, this does not happen if the closed subscheme is flat over the base.

Proposition 10.1.7. Let $f : X \rightarrow Y$ be a smooth proper map of schemes and $Z \subset X$ a closed subscheme flat over Y . Then the locus,

$$V = \{y \in Y \mid Z_y \subset X_y \text{ is Cartier}\}$$

is clopen.

Proof. Consider the ideal sheaf sequence,

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{O}_X \longrightarrow \iota_* \mathcal{O}_Z \longrightarrow 0$$

Because $Z \rightarrow Y$ is flat, $\mathcal{I}|_{X_y}$ is the ideal sheaf of $Z_y \subset X_y$. By the previous result, the locus where $\mathcal{I}|_{X_y}$ is a vector bundle (and hence a line bundle since it embeds in \mathcal{O}_X) is open. Thus we just need to prove closedness. It suffices to show that V is stable under specialization. (REDUCE TO THE DVR CASE, 1 NOETHERIAN, 2 BLOW UP, 3 NORMALIZE) Thus we can assume that $Y = \text{Spec}(R)$ where R is a DVR and $D_K \subset X_K$ is a Cartier divisor. We need to show that $D_0 \subset X_0$ is Cartier. For each $x \in X_0$ let $A = \mathcal{O}_{X,x}$ and we have the following: a flat ring map $R \rightarrow A$ with A regular, an ideal $I \subset A$ with $R \rightarrow A/I$ flat such that $I \otimes_R K \subset A \otimes_R K$ is principal. Since $R \rightarrow A/I$ is flat A/I can only have associated points in the generic fiber thus A/I is unmixed since in the generic fiber I is principal and A is regular so I has no embedded primes by the unmixedness theorem. Consider the primary decomposition,

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

where Q_i is \mathfrak{p}_i -primary where $\text{ht}(\mathfrak{p}_i) = 1$ by unmixedness. Since A is a UDF we have $\mathfrak{p}_i = (p_i)$ are principal. Therefore, \square

Remark. The following example shows that smoothness really is necessary.

Example 10.1.8. Consider,

$$f : X = \text{Proj} \left(k[t][X, Y, Z] / (X^3 - Y^2Z) \right) \rightarrow S = \text{Spec}(k[t])$$

and the divisor

$$D = \text{Proj} \left(k[t][X, Y, Z] / (X^3 - Y^2Z, X - t^2Z, Y - t^3Z) \right)$$

which is the image of a section of f and hence flat. For $t \neq 0$ we have $D_t \subset X_t$ a Cartier divisor but $D_0 \subset X_0$ is not a Cartier divisor.