Contents

1 Nakayama's Lemma

Proposition 1.0.1. 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 $1 - r \in R$ and $rM = 0$.

Proof. □

2 Galois Theory

Proposition 2.0.1. Let E be the splitting field of a $f \in K[x]$. Then,

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

with equality if and only if f is separable.

Proof. Dummit and Foote p.561. □

Lemma 2.0.2 (Independence of Characters)**.** Let $\sigma_1, \dots, \sigma_n : G \to E^\times$ be distinct linear characters. Then in $E[G]$ the elements $\sigma_1, \dots, \sigma_n$ are independent.

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

Now suppose that,

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

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. ☐

Corollary 2.0.3. Distinct field embeddings $\sigma_1, \dots, \sigma_n : K \hookrightarrow L$ are independent.

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

Corollary 2.0.4. Let $x_1, \dots, x_n \in E$ be a basis for E/K and $n = [E : K]$. Let $G \subset \mathrm{Aut}\,(E/K)$ 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. ☐

Corollary 2.0.5. If $G \subset \mathrm{Aut}\,(E/K)$ then $|G| \leq [E : K]$.

Proposition 2.0.6. Let E/K be a field extension and $G \subset \mathrm{Aut}\,(E/K)$. 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, $G \subset \mathrm{Aut}\,(E/F)$ 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 2.0.7. We say that E/K is *Galois* if $K = E^{\mathrm{Aut}(E/K)}$ and write $\mathrm{Gal}\,(E/K) := \mathrm{Aut}\,(E/K)$.

Corollary 2.0.8. We see that E/K is Galois if and only if $|\mathrm{Aut}\,(E/K)\,| = [E : K]$.

2.1 The Galois Correspondence

Proposition 2.1.1. Let E/K be a finite extension and $G \subset \mathrm{Aut}\,(E/K)$. Let $F = E^G$ then E/F is Galois and $G = \mathrm{Aut}\,(E/F)$.

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

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

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

Proposition 2.1.2 (Galois Connection)**.** Let E/K be a finite extension and $G = \mathrm{Aut}\,(E/K)$.

$$\{\text{subgroups } H \subset G\} \underset{F \mapsto \mathrm{Aut}(E/F)}{\overset{H \mapsto E^H}{\rightleftarrows}} \{\text{intermediate extensions } K \subset F \subset E\}$$

satisfy the following properties,

(a) $H \mapsto E^H \mapsto \mathrm{Aut}\left(E/E^H\right) = H$ meaning that

3 Groups of Lie Type

4 Galois Groups of Cubics

5 Products of Ideals

Lemma 5.0.1. 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 $\mathfrak{p} \notin V(I) \cup V(J)$. 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. □

Proposition 5.0.2. 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 $I \cap J = IJ$. □

6 Induced Representations

6.1 Restriction

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

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

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

Proposition 6.1.1. If $\phi : G \to H$ is surjective then $\text{Rep}_R(H) \to \text{Rep}_R(G)$ 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. □

6.1.1 The Case of a Normal Subgroup

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

Definition 6.1.2. 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 $\mathrm{Rep}_R : \mathbf{Grp}^{\mathrm{op}} \to \mathbf{Cat}$ is really a 2-functor sending the natural transformation (isomorphism) $\eta : \phi \to \phi'$ (which just says that $\phi' = c_h \circ \phi$ for some $h = \eta_* \in H$) to the natural isomorphism $\mathrm{Res}_\eta(V) : \mathrm{Res}_\phi(V) \to \mathrm{Res}_{\phi'}(V)$ 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 6.1.3. If $H \subset G$ is normal and V is a G-representation then $g * \mathrm{Res}^G_H(V) \cong \mathrm{Res}^G_H(V)$.

Proof. Consider the map $\eta : V \to V$ by sending $\eta : v \mapsto g \cdot v$. I claim this is an isomorphism $\eta : g * \mathrm{Res}^G_H(V) \to \mathrm{Res}^G_H(V)$. 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 $\eta \circ (g * \rho)(h) = \rho(h) \circ \eta$. $\square$

Proposition 6.1.4. Let $H \subset G$ be normal and V a G-representation. Then G/H acts on the H-subrepresentations $W \subset \mathrm{Res}^G_H(V)$ 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. $\square$

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

6.2 Induction and Coinduction

Proposition 6.2.1. 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 $R[H]^{\mathrm{op}} \cong R[H]$) 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 $G/H \times H \to G$ via $(g, h) \mapsto gh$ then $\alpha_{g,h} = 0$. Finally, this map is $R[H]$-linear because $g \cdot hh' \mapsto ghh' = (gh) \cdot h'$. $\square$

Proposition 6.2.2. If $H \subset G$ is normal then for any H-representation W,

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

Proposition 6.2.3. If $H \subset G$ is normal then for any G-representation V,

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

as $R[G]$-modules.

Proof. Consider the map, $\mathrm{Ind}^G_H\left(\mathrm{Res}^G_H(V)\right) \cong R[G] \otimes_{R[H]} V \to R[G/H] \otimes_R V$ 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. □

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

7 Noetherian Normalization

Theorem 7.0.1. 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,

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

However the exponent of y_n encodes a unique base r number if we choose r larger than every exponent in r. 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. □

8 Cohen's Theorem

Lemma 8.0.1. Let $A \subset B$ be an integral extension of domains. Then A is a field iff B is a field.

Proof. If nonzero $b \in B$ is integral over a then $b^{-1} \in B$ from the polynomial since its trailing term is invertible. Thus A a field implies B a field. If B is a field then since a^{-1} is integral over A we see that $a^{-1} \in A$ from the polynomial so A is a field. □

Lemma 8.0.2. Let $f : A \to B$ 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 $A/f^{-1}(\mathfrak{p}) \subset A/\mathfrak{p}$ which is an integral extension of domains. Thus $\mathfrak{p}$ is maximal iff $A/\mathfrak{p}$ is a field iff $A/f^{-1}(\mathfrak{p})$ is a field iff $f^{-1}(\mathfrak{p})$ is maximal. □

Proposition 8.0.3 (Lying Over)**.** Let $A \subset B$ be an integral extension of rings. Then the continuous map $f^* : \mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ is surjective.

Proof. Let $\mathfrak{p} \subset A$ be a prime. Consider, $S = A \setminus \mathfrak{p}$ then there is a diagram,

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d] & B \arrow[d] \\ A_{\mathfrak{p}} \arrow[r, hook] & S^{-1}B \end{tikzcd}$$

and the bottom extension is integral. Choose a maximal ideal $\mathfrak{m} \subset S^{-1}B$ which is nonzero because $A_{\mathfrak{p}}$ is contained inside it. 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 $A \to A_{\mathfrak{p}} \to S^{-1}B$ we see that $\mathfrak{m} \mapsto \mathfrak{p}$. By commutativity the pullback of $\mathfrak{m}$ in B maps to $\mathfrak{p}$. □

Corollary 8.0.4 (Going Up)**.** If $f : A \to B$ 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 domains. Thus $\mathrm{Spec}\,(B/I) \to \mathrm{Spec}\,(A/f^{-1}(I))$ 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 $\mathfrak{q}' \mapsto \mathfrak{p}$. □

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

Proposition 8.0.5 (Incompatibility)**.** If $A \to B$ is an integral map and $\mathfrak{p} \subset \mathfrak{p}'$ are primes of B above $\mathfrak{q} \subset A$ then $\mathfrak{p} = \mathfrak{p}'$.

Proposition 8.0.6 (Going Down)**.** 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 prime ideal.