

# Math 220C: Modern Algebra

Simon Rubinstein-Salzedo

June 16, 2004

## **0.1 Introduction**

Professor: Adebisi Agboola

Office Hours: Tuesday: 11:15-12:30, Wednesday: 11:15-12:30, Thursday: 11:15-12:30.

# Chapter 1

## Preliminaries

**Question** How can we tell whether a polynomial is irreducible?

**Definition 1.1** Suppose that  $R$  is a unique factorization domain and  $k$  the field of fractions of  $R$ . If  $f \in R[x]$ , define the **content**  $c(f)$  of  $f$  by  $c(f) = \gcd(\text{the coefficients of } f)$ . (This is only defined up to a unit factor.) If  $f \in k[x]$ , then  $\exists d \in R$  such that  $df \in R[x]$ . Then define  $c(f) = c(df)/d$ . (This is independent of  $d$ .)

**Lemma 1.2** (Gauss) If  $f, g \in k[x]$ , then  $c(fg) = c(f)c(g)$ .

**Proof** It suffices to assume that  $f, g \in R[x]$ . Suppose that  $p$  is a prime in  $R$  not dividing  $c(f)c(g)$ . Set  $f(x) = \sum_i a_i x^i$  and  $g(x) = \sum_j b_j x^j$ . Choose  $i$  and  $j$  minimal such that  $p \nmid a_i$  and  $p \nmid b_j$ . Then the coefficient of  $x^{i+j}$  in  $fg$  is not divisible by  $p$ , and so neither is  $c(fg)$ . The proof now follows by induction on the number of primes in the factorization of  $c(fg)$ .

**Corollary 1.3** Suppose that  $f$  is irreducible in  $R[x]$ . Then  $f$  is also irreducible in  $k[x]$ .

**Proof** If  $f$  is irreducible in  $R[x]$  and is not constant, then  $c(f) = 1$ . Furthermore, if  $f = gh$ , with  $g, h \in k[x]$  and  $\deg g$  and  $\deg h > 0$ , then Gauss's Lemma implies that  $1 = c(g)c(h)$ . Thus

$$f = \frac{g}{c(g)} \frac{h}{c(h)},$$

which is a contradiction since  $f$  is irreducible. So for example to factor a polynomial with integer coefficients over the rationals, it suffices to look only at factorizations with integer coefficients.

**Theorem 1.4** (Eisenstein's Criterion) Let  $p$  be a prime in a unique factorization domain  $R$ . Suppose that  $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$  is a polynomial in  $R[x]$  such that  $p \nmid a_0$ ,  $p \mid a_i$  ( $i \leq i \leq n$ ), and  $p^2 \nmid a_n$ . Then  $f(x)$  is irreducible in  $k[x]$ .

**Proof** Set  $I = R/(p)$ , so  $I$  is an integral domain. Suppose that  $f = gh$  and  $\deg g = r$  ( $1 \leq r < n$ ). Corollary 1.3 implies that we may assume that  $g, h \in R[x]$ . Let  $\bar{f}, \bar{g}$ , and  $\bar{h}$  be the polynomials in  $I[x]$  obtained by reducing the coefficients of  $f, g$ , and  $h$  modulo  $p$ . So  $\bar{f} = \bar{g}\bar{h}$ ,  $\deg \bar{g} \leq r$ , and  $\deg \bar{h} \leq n - r$ . However,  $\bar{f} = \bar{a}_0 x^n$ , and so  $\bar{g} = \alpha x^r$  and  $\bar{h} = \beta x^{n-r}$  for some  $\alpha, \beta \in R$  (since  $I$  is an integral domain). Thus  $\bar{g}(0) = \bar{h}(0) = 0$ , i.e.  $p \mid g(0)$  and  $p \mid h(0)$ , and so  $p^2 \mid a_n$ , which is a contradiction.

**Theorem 1.5** For each  $n \geq 1$ , let  $\Phi_n(x) = \prod_{\zeta} (x - \zeta)$ , where the product is over those  $\zeta \in \mathbb{C}$  of exact multiplicative order  $n$ . Then  $\Phi_n(x)$  is called the  $n^{\text{th}}$  **cyclotomic polynomial**. Then  $\Phi_n \in \mathbb{Z}[x]$ , and  $\Phi_n(x)$  is irreducible over  $\mathbb{Q}$ .

**Proof** First observe that  $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$  since these are monic polynomials with the same distinct roots in  $\mathbb{C}$ . So, if we assume by induction that  $\Phi_d(x) \in \mathbb{Z}[x]$  for  $d < n$ , then it follows first that  $\Phi_n(x) \in \mathbb{Q}[x]$ , and then, by Gauss's Lemma, that  $\Phi_n(x) \in \mathbb{Z}[x]$ . Now suppose that  $f$  is a monic irreducible factor of  $\Phi_n(x)$ ; we wish to prove that  $f = \Phi_n$ . We still have to prove that whenever  $\zeta$  is a root of  $f$ , then so is  $\zeta^p$  for any prime  $p \nmid n$ . Set  $x^n - 1 = f(x)g(x)$ . If  $\zeta^p$  is not a root of  $f$ , then it must be a root of  $g$ ; in this case,  $\zeta$  is a root of  $g(x^p)$ . Thus  $f(x) \mid g(x^p)$ , i.e.  $g(x^p) = f(x)h(x)$ , say. Reducing all these polynomials modulo  $p$  and using  $\bar{g}(x^p) = \bar{g}(x)^p$ , etc. gives

$$x^{np} - 1 = (x^n - 1)^p = \bar{f}(x^p)\bar{g}(x^p) = \bar{f}(x)^{p+1}\bar{h}(x),$$

and so  $\bar{f}(x)^{p+1} \mid (x^n - 1)^p$ . So if we factor  $x^n - 1$  in  $\mathbb{F}_p[x]$ , it has a square factor,  $F^2$ , say. Differentiating, we deduce that  $F$  divides  $nx^{n-1}$ . So  $x^n - 1$  and  $nx^{n-1}$  have a common factor, which is a contradiction if  $p \nmid n$ .

**Recall** For each field  $k$ , there is a homomorphism  $\phi : \mathbb{Z} \rightarrow k$  given by  $\phi(n) = 1 + 1 + \cdots + 1$  ( $k$  times).

**Definition 1.6** Suppose that  $L$  and  $K$  are fields with  $K \subset L$ . Then  $L$  is called an **extension of  $K$** , and we write  $L/K$ . The **degree**  $[L : K]$  of  $L$  over  $K$  is the dimension of  $L$  viewed as a  $K$ -vector space.

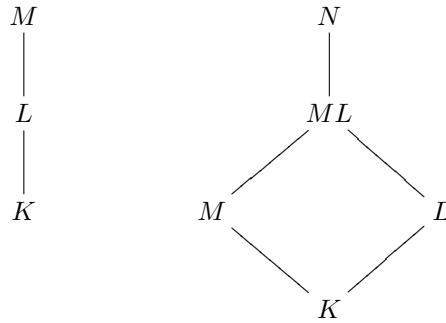
**Theorem 1.7** (The Tower Law) Suppose that  $M \supset L \supset K$  are three fields. Then  $[M : K] = [M : L][L : K]$ .

**Proof** (The equality means that if either  $[M : L]$  or  $[L : K]$  is infinite, then so is  $[M : K]$ ; otherwise  $[M : K]$  is finite and equal to  $[M : L][L : K]$ .) If  $[M : L]$  or  $[L : K]$  is infinite, the result is plain. Let  $x_1, x_2, \dots, x_m$  denote a basis of  $L/K$ . Let  $y_1, y_2, \dots, y_n$  denote a basis of  $M/L$ . So each element of  $L$  has a unique expansion  $\sum_{i=1}^m x_i z_i$  ( $z_i \in K$ ), and each element of  $M$  has a unique expression of the form  $\sum_{j=1}^n y_j w_j$  ( $w_j \in L$ ). We claim that the set  $\{x_i y_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$  is a basis

of  $M/K$ . For if  $t \in M$ , then  $t = \sum_{j=1}^n y_j w_j$  ( $w_j \in L$ ), and then  $w_j = \sum_{i=1}^m x_i z_{ij}$  ( $z_{ij} \in K$ ). So  $t = \sum_{i,j} x_i y_j z_{ij}$ , with  $z_{ij} \in K$ . Since the  $w_j$ s are unique and so are the  $z_{ij}$ s, the set of  $\{x_i y_j\}$  do form a basis, as desired.

**Definition 1.8** Suppose that  $C$  is a class of extensions  $L/K$ . Then  $C$  is said to be **distinguished** if it satisfies the following conditions:

1. (Tower Property) Whenever  $M/L$  and  $L/K$  lie in  $C$ , then so does  $M/K$ .
2. (Lifting Property) If  $N \supset L \supset K$  and  $N \supset M \supset K$  are two towers of fields and  $L/K$  lies in  $C$ , then so does  $ML/M$ . (Here  $ML$  denotes the smallest subfield of  $N$  containing both  $M$  and  $L$ .)



**Definition 1.9** Let  $L/K$  be an extension, and let  $\alpha \in L$ . We denote by  $K(\alpha)$  the smallest subfield of  $L$  containing both  $K$  and  $\alpha$ . ( $K(\alpha)/K$  is a **simple extension**.) If  $[K(\alpha) : K] < \infty$ , then  $\alpha$  is said to be **algebraic**. If  $[K(\alpha) : K] = \infty$ , then  $\alpha$  is said to be **transcendental**.

**Theorem 1.10** If  $\alpha$  is algebraic, then there is an irreducible polynomial  $f \in K[x]$  with  $f(\alpha) = 0$ ; moreover,  $K(\alpha) \simeq K[x]/(f)$ . If  $\alpha$  is transcendental, then  $K(\alpha) \simeq K(x)$  (the field of factors of  $K[x]$ ).

**Proof** Consider the homomorphism  $\phi : K[x] \rightarrow K(\alpha)$  given by  $\phi(g(x)) = g(\alpha)$ . If  $\alpha$  is algebraic with  $[K(\alpha) : K] = n$ , say, then  $1, \alpha, \alpha^2, \dots, \alpha^n$  are linearly dependent over  $K$ . So  $\ker \phi \neq \{0\}$ . If  $gh \in \ker \phi$ , then  $g(\alpha)h(\alpha) = 0$ . Hence either  $g \in \ker \phi$  or  $h \in \ker \phi$ , i.e.  $\ker \phi$  is a prime ideal.  $K[x]$  is a principal ideal domain, and so  $\ker \phi = (f)$  for some irreducible polynomial  $f$ .  $\ker \phi$  is maximal, so  $K[x]/(f)$  is a field. Hence  $\phi$  induces a monomorphism  $\tilde{\phi} : K[x]/(f) \rightarrow K(\alpha)$ . Since  $\text{Im } \tilde{\phi}$  is a field containing both  $K$  and  $\alpha$ , we have  $\text{Im } \tilde{\phi} = K(\alpha)$ . If  $\alpha$  is transcendental, then  $\ker \phi = \{0\}$ , so  $\phi$  extends to an isomorphism  $K(x) \xrightarrow{\sim} K(\alpha)$ .

**Definition 1.11** The monic polynomial  $f$  above is called the **minimal polynomial** of  $\alpha$  over  $K$ .

**Theorem 1.12** Let  $K$  be a field and  $f$  an irreducible polynomial in  $K[x]$ . Then  $\exists$  an extension  $L$  of  $K$  in which  $f$  has a root.

**Proof** Since  $f$  is irreducible, the quotient  $L = K[x]/(f)$  is a field. Identify  $K$  with its image in  $L$  and let  $\alpha$  be the image of  $x$  in  $L$ . Then  $f(\alpha) = 0$ , as required.

**Corollary 1.13** (To Theorem 1.10) Suppose that  $L$  and  $M$  are extensions of  $K$  containing roots  $\alpha$  and  $\beta$ , respectively, of  $f$ . Then there is an isomorphism  $\sigma : K(\alpha) \rightarrow K(\beta)$  such that  $\sigma|_K = id_K$  and  $\sigma(\alpha) = \beta$ .

**Proof** By Theorem 1.10, there are isomorphisms  $\phi : K[x]/(f) \rightarrow K(\alpha)$  and  $\psi : K[x]/(f) \rightarrow K(\beta)$ . Set  $\sigma = \psi\phi^{-1}$ .

**Theorem 1.14** Let  $K$  be a field and  $f$  a polynomial in  $K[x]$ . Then there is an extension  $L$  of  $K$  in which  $f$  factors completely (i.e. into linear factors).

**Proof** Exercise.

**Definition 1.15** The field  $L$  above generated by  $K$  and the roots of  $f$  is called a **splitting field** of  $f$  over  $K$ .

**Example** A splitting field over  $\mathbb{Q}$  of  $x^4 - 5$ . Let  $\alpha \in \mathbb{R}^+$  be such that  $\alpha^4 = 5$ , and let  $i \in \mathbb{C}$  satisfy  $i^2 = -1$ . Then  $x^4 - 5 = (x - \alpha)(x + \alpha)(x - i\alpha)(x + i\alpha)$ , and so  $x^4 - 5$  factors completely in  $\mathbb{Q}(\alpha, i)$ . Now  $x^4 - 5$  is irreducible over  $\mathbb{Q}$  by Eisenstein, and so  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ . Also  $x^2 + 1$  is irreducible over  $\mathbb{Q}(\alpha)$  since  $i \notin \mathbb{R} \supseteq \mathbb{Q}(\alpha)$ , so  $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$ . Hence  $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8$  by the Tower Law.

## 1.1 Ruler and Compass Constructions

Examples of constructions that one can carry out with a straightedge and compass are:

1. Bisecting an angle,
2. Dropping a perpendicular from a point to a line,
3. Drawing a line through a point parallel to a given line, and so dividing an interval into a given ratio.

We begin with two distinct points  $P_0$  and  $P_1$  in the plane. We take  $P_0$  as the origin, and we take as our first axis the line through  $P_0$  and  $P_1$  and as our second axis the line through  $P_0$  perpendicular

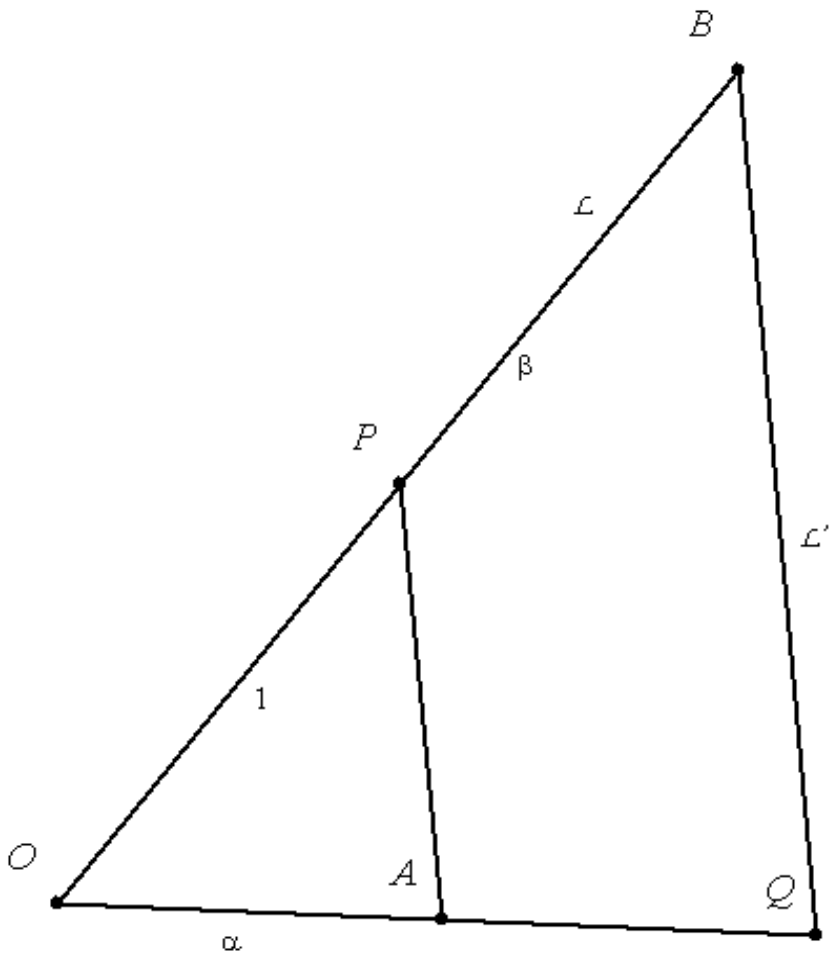
to  $P_0P_1$ . Take  $P_0P_1$  as our unit of distance, and think of each point in the plane as an element  $(x, y) \in \mathbb{R} \times \mathbb{R}$ .

**Definition 1.16** A real number  $\alpha$  is **constructible** if we can construct a line segment of length  $|\alpha|$  in a finite number of steps from  $P_0P_1$  by using a straightedge and compass. Alternatively, we say that a point  $P$  is **constructible** if  $\exists$  a finite sequence  $P_0, P_1, \dots, P_n = P$  of points in the plane with the following property: Let  $S_j = \{P_0, P_1, \dots, P_j\}$  for  $1 \leq j \leq n$ . For each  $2 \leq j \leq n$ ,  $P_j$  is one of the following:

1. The intersection of two distinct straight lines each joining two points of  $S_{j-1}$ ,
2. A point of intersection of a straight line joining two points of  $S_{j-1}$  and a circle with center a point of  $S_{j-1}$  and radius the distance between two points in  $S_{j-1}$ , or
3. A point of intersection of two distinct circles each with center a point of  $S_{j-1}$  and radius the distance between two points in  $S_{j-1}$ . (Note that the centers of these circles *must* be different if the circles are to intersect.)

**Theorem 1.17** If  $\alpha$  and  $\beta$  are constructible, then so are  $\alpha + \beta$ ,  $\alpha - \beta$ ,  $\alpha\beta$ , and  $\alpha/\beta$  if  $\beta \neq 0$ .

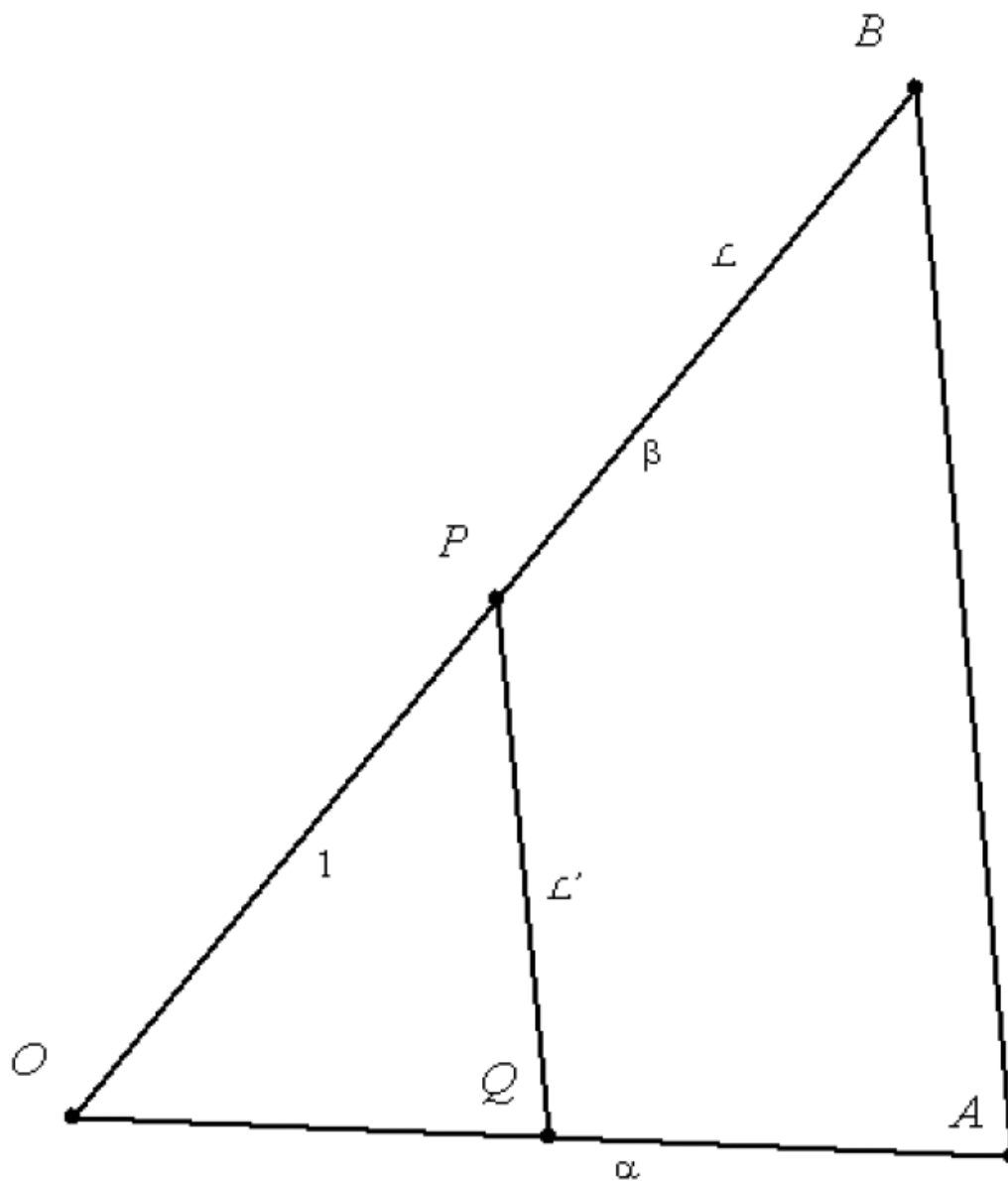
**Proof** The only difficult cases are  $\alpha\beta$  and  $\alpha/\beta$ . Let's start with  $\alpha\beta$ :



Construct  $OA$  with  $|OA|$  of length  $\alpha$ . Construct a line  $l$  through  $O$  not containing  $OA$ . Find points  $P$  and  $B$  on  $l$  with  $|OP| = 1$  and  $|OB| = \beta$ . Draw  $PA$ , and construct  $l'$  through  $B$  parallel to  $PA$  and intersecting  $OA$  extended at  $Q$ . By similar triangles, we have

$$\frac{1}{\alpha} = \frac{\beta}{|OQ|},$$

and so  $|OQ| = \alpha\beta$ .



Construct  $OA$  of length  $\alpha$ . Construct a line  $l$  through  $O$  not containing  $OA$ . Find  $B$  and  $P$  on  $l$  such that  $|OB| = \beta$  and  $|OP| = 1$ . Draw  $BA$ , and construct  $l'$  through  $P$  parallel to  $BA$  and intersecting  $OA$  at  $Q$ . By similar triangles, we have

$$\frac{|OQ|}{1} = \frac{\alpha}{\beta},$$

i.e.  $|OQ| = \alpha/\beta$ .

**Corollary 1.18** The set of all constructible real numbers forms a subfield  $F$  of the real numbers. We have  $\mathbb{Q} \subseteq F$  since  $\mathbb{Q}$  is the smallest subfield of  $\mathbb{R}$ .

**Theorem 1.19** If  $P = (x, y)$  is a constructible point, the extension  $\mathbb{Q}(x, y)/\mathbb{Q}$  is finite, and  $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$  for some  $r \in \mathbb{N}$ .

**Proof** Since  $P$  is constructible,  $\exists$  a sequence  $P_0, P_1, \dots, P_n = P$  of points satisfying the requirements of the definition. Set  $P_j = (x_j, y_j)$ , and for each  $1 \leq j \leq n$ , set  $F_j = \mathbb{Q}(x_1, y_1, x_2, y_2, \dots, x_j, y_j)$ . Then  $F_{j+1} = F_j(x_{j+1}, y_{j+1})$  for  $0 \leq j \leq n-1$ . We shall show that  $[F_{j+1} : F_j] = 1$  or  $2$ ; then by the Tower Law,  $[F_n : F_0] = [F_n : \mathbb{Q}] = 2^s$  for some  $s$ . Now  $\mathbb{Q}(x, y) = \mathbb{Q}(x_n, y_n)$  is a subfield of  $F_n$  containing  $\mathbb{Q}$ . So applying the Tower Law again gives  $[F_n : \mathbb{Q}(x, y)][\mathbb{Q}(x, y) : \mathbb{Q}] = 2^s$ , whence  $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$  for some  $r$ . To show that  $[F_{j+1} : F_j] = 1$  or  $2$ ,

1. If  $(a_1, b_1), (a_2, b_2) \in S_j$ , then the equation of the line joining these points is  $(x - a_2)(b_1 - b_2) = (a_1 - a_2)(y - b_2)$ . So this has the form  $\lambda x + \mu y + \gamma = 0$ , with  $\lambda, \mu, \gamma \in F_j$ .
2. The equation of the circle with center  $(a_1, b_1)$  and radius the distance between  $(a_2, b_2)$  and  $(a_3, b_3)$  in  $S_j$  is  $(x - a_1)^2 + (y - b_1)^2 = (a_2 - a_3)^2 + (b_2 - b_3)^2$ ; this has the form  $x^2 + y^2 + 2gx + 2fy + c = 0$ , with  $f, g, c \in F_j$ . There are three cases to consider:
  - (a)  $(x_{j+1}, y_{j+1})$  is the intersection of two distinct straight lines each joining two points of  $S_j$ .
  - (b)  $(x_{j+1}, y_{j+1})$  is a point of intersection of an appropriate straight line and a circle.
  - (c)  $(x_{j+1}, y_{j+1})$  is a point of intersection of two appropriate circles.

**Exercise** Show that in each case  $[F_{j+1} : F_j] = 1$  or  $2$ .

**Theorem 1.20** “Squaring the circle” is impossible, i.e. it is not possible to construct a square equal in area to the area of a circle of radius 1.

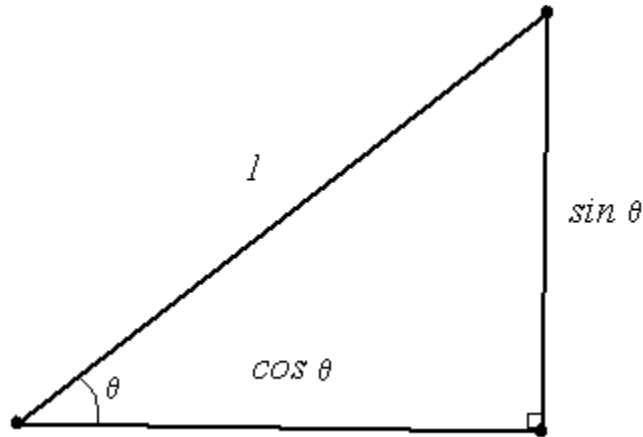
**Proof** The circle has an area of  $\pi$ , and so we would have to construct a square of side  $\sqrt{\pi}$ . So  $\pi$  would have to be algebraic over  $\mathbb{Q}$  of degree  $2^m$  for some  $m \geq 0$ . But this is a contradiction since Lindemann proved in 1882 that  $\pi$  is transcendental.

**Theorem 1.21** “Duplicating the cube” is impossible, i.e. given a side of a cube, it is not always possible to construct the side of another cube whose volume is twice that of the original cube.

**Proof** Suppose that the original cube has side 1. The cube being sought would have volume 2 and hence a side of  $\sqrt[3]{2}$ . But  $\sqrt[3]{2}$  is a zero of the irreducible (over  $\mathbb{Q}$ ) polynomial  $x^3 - 2$ . So  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ . So  $\sqrt[3]{2}$  is not constructible.

**Theorem 1.22** “Trisecting the angle” is impossible, i.e.  $\exists$  an angle that cannot be trisected using straightedge and compass.

**Proof** First observe that an angle  $\theta$  can be constructed iff a line segment of length  $|\cos \theta|$  can be constructed:



Set  $\theta = 3\beta$ ; then we must solve the equation  $\cos 3\beta = \cos \theta = \lambda$ , say. Now  $\cos 3\beta = 4 \cos^3 \beta - 3 \cos \beta$ . So we must solve the equation  $4 \cos^3 \beta - 3 \cos \beta = \lambda$ , i.e.  $4x^3 - 3x = \lambda$ . Now e.g. for  $\lambda = 1/2$  (i.e.  $\theta = 60^\circ$ ), the equation becomes (we put  $y = 2x$ )  $y^3 - 3y - 1 = 0$ . But this is irreducible over  $\mathbb{Q}$  (put  $y = z + 1$  and apply Eisenstein).

## Chapter 2

# Embeddings

Henceforth all extensions will be finite, unless otherwise specified. Throughout this chapter,  $L/k$  will denote a *fixed, sufficiently large* extension, i.e.  $L$  contains all roots of various polynomials over  $k$ . So  $L$  remains fixed, and for each extension  $K/k$ , we look at the  $k$ -**embedding** of  $K$  in  $L$ , i.e. field homomorphisms  $\sigma : K \rightarrow L$  such that  $\sigma|_k = id_k$ .

**Lemma 2.1** Let  $K = k(\alpha)$  be a simple extension of  $k$  with  $f$  the minimal polynomial of  $\alpha$  over  $k$  and  $\alpha_1, \dots, \alpha_r$  the distinct roots of  $f$  in  $L$ . Then there are precisely  $r$   $k$ -embeddings  $\sigma_1, \sigma_2, \dots, \sigma_r$  of  $K$  in  $L$  determined by  $\sigma_i(\alpha) = \alpha_i$ ,  $i = 1, 2, \dots, r$ .

**Proof** We have already shown that for each  $i = 1, 2, \dots, r$ ,  $\exists$  a  $k$ -embedding  $\sigma_i : K \rightarrow L$  with  $\sigma_i(\alpha) = \alpha_i$  (Corollary 1.13). Recall that  $\sigma_i$  was constructed as follows:

$$K \simeq k(\alpha) \simeq \frac{k[\alpha]}{(f(x))} \simeq k(\alpha_i) \subset L.$$

Conversely, suppose that  $\sigma$  is a  $k$ -embedding of  $K$  in  $L$ . Then  $f(\sigma\alpha) = (\sigma f)(\alpha) = f(\alpha) = 0$  (as the coefficients of  $f$  are unaffected by  $\sigma$ ). Thus  $\sigma\alpha = \alpha_i$  for some  $i = 1, 2, \dots, r$ , and so  $\sigma = \sigma_i$ , as required.

The following result is critical.

**Theorem 2.2** (Artin's Extension Theorem) Suppose that  $\sigma : k \rightarrow M$  is a field isomorphism and  $f$  is an irreducible polynomial in  $k[x]$  possessing a root  $\alpha$  in an extension  $K$ . Then  $\sigma f$  is an irreducible polynomial in  $M[x]$ , and if  $\beta$  is root of  $\sigma f$  in an extension  $L$  of  $M$ , then  $\exists$  an isomorphism  $\tau : k(\alpha) \rightarrow M(\beta)$  such that  $\tau|_k = \sigma$  and  $\tau(\alpha) = \beta$ .

**Proof** If  $\sigma f$  were to factor in  $M[x]$  as  $gh$ , then we would have  $f = (\sigma^{-1}g)(\sigma^{-1}h)$ , so  $\sigma f$  is indeed

irreducible. We now obtain  $\tau$  by composing the following isomorphisms:

$$k(\alpha) \simeq \frac{k[x]}{(f)} \xrightarrow{\sigma} \frac{M[x]}{(\sigma f)} \simeq M(\beta).$$

**Point** Since we can “lift” an embedding to any simple extension, we can by induction embed any extension.

**Corollary 2.3** Let  $f \in k[\alpha]$  and  $K$  and  $L$  be two splitting fields for  $f$  over  $k$ . Then there is a  $k$ -isomorphism  $K \rightarrow L$ .

**Proof** Let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be the roots of  $f$  in  $K$ . Then each rung of the following ladder is obtained by applying Artin’s Theorem to the previous rung:

$$\begin{array}{ccc}
 K = k(\alpha_1, \alpha_2, \dots, \alpha_n) & \xrightarrow{\sigma} & L = k(\beta_1, \beta_2, \dots, \beta_n) \\
 \vdots & & \vdots \\
 k(\alpha_1, \alpha_2) & \longrightarrow & k(\beta_1, \beta_2) \\
 \downarrow & & \downarrow \\
 k(\alpha_1) & \longrightarrow & k(\beta_1) \\
 & \searrow & \swarrow \\
 & k & 
 \end{array}$$

Here  $\beta_1, \beta_2, \dots, \beta_n$  denote the roots of  $f$  in  $L$  in some order.

**Note** The order of the roots  $\beta_1, \beta_2, \dots, \beta_n$  may not be determined arbitrarily, e.g. if  $\sigma\alpha_1 = \beta_1$ , then it follows that if  $g \in k[x]$  and  $g(\alpha_1) = 0$ , then  $g(\beta_1) = 0$ , so  $\alpha_1$  and  $\beta_1$  are roots of the same irreducible factor of  $f$ .

**Theorem 2.4** Let  $K/k$  be a finite extension. Then there are at most  $[K : k]$   $k$ -embeddings of  $K$  in  $L$ .

**Proof** If  $K = k(\alpha)$  and  $\alpha$  has minimal polynomial  $f$ , then each  $k$ -embedding of  $K$  in  $L$  corresponds to a root of  $f$  in  $L$ , of which there are at most  $\deg f = [K : k]$ . Now assume the result is true for all extensions of smaller degree than  $[K : k]$ . Let  $M \neq K$  be an extension of  $k$  with  $[K : M]$  minimal. Then  $K = M(\alpha)$ , for some  $\alpha$  and  $M$ , has at most  $[M : k]$   $k$ -embeddings into  $L$ , and each of these has at most  $[K : M]$  extensions to  $K$ . Thus there are at most  $[K : k]$  embeddings in all.

When is this bound attained?

If  $\alpha \in K$  with minimal polynomial  $f$  over  $k$ , then we require  $f$  to have distinct roots (in some extension of  $k$ ). In this case,  $\alpha$  (and  $f$ ) are said to be **separable** over  $k$ .

**Theorem 2.5** Let  $K/k$  be a separable extension. Then there are exactly  $[K : k]$   $k$ -embeddings of  $K$  in  $L$ . Conversely, if  $K/k$  is an extension for which there are  $[K : k]$   $k$ -embeddings in  $L$ , then  $K/k$  is separable.

**Proof** The result is clearly true if  $K/k$  is simple. Assuming that the result is true for extensions of smaller degree, let  $M \neq K$  be such that  $[K : M]$  is minimal, so  $K = M(\alpha)$  for some  $\alpha \in K$ . We claim that  $\alpha$  is separable over  $M$ . To prove this, note that if  $f$  is its minimal polynomial over  $k$  and  $g$  is its minimal polynomial over  $M$ , then  $g \mid f$ , and so  $g$  also has distinct roots. Thus there are  $[M : k]$   $k$ -embeddings of  $M$  in  $L$  by assumption, and by Artin's Law, each of these extends in  $[K : M]$  ways to embeddings of  $K$  in  $L$ ; thus there are  $[K : M][M : k] = [K : k]$   $k$ -embeddings in all.

For the converse, first observe that if  $\alpha \in K$  is inseparable over  $k$ , then there are no fewer than  $[k(\alpha) : k]$  embeddings of  $k(\alpha)$  in  $L$ . By Theorem 2.4, each yields at most  $[K : k(\alpha)]$  embeddings of  $K$  in  $L$ , and so there are fewer than  $[K : k]$  in all. Hence each  $\alpha \in R$  is separable over  $k$ .

**Theorem 2.6** (The Primitive Element Theorem) Let  $K/k$  be a finite, separable extension. Then  $K/k$  is simple.

**Proof** If  $K$  is finite, then  $K$  has a cyclic multiplicative group whose generator generates the extension  $K/k$ . Suppose that  $k$  is infinite. By induction on the number of generators, it suffices to treat the case  $K = k(\alpha, \beta)$ . Let  $n = [K : k]$  and  $\sigma_1, \sigma_2, \dots, \sigma_n$  be the distinct  $k$ -embeddings of  $K$  in  $L$ . Consider a general element  $\gamma \in K$ . When is  $\gamma$  a primitive element? If  $\sigma_1\gamma, \sigma_2\gamma, \dots, \sigma_n\gamma$  are distinct, then  $[k(\gamma) : k] \geq n$ , and so  $K = k(\gamma)$ . Conversely, if  $K = k(\gamma)$ , then  $\sigma_i$  is determined by  $\sigma_i\gamma$ , and so  $\sigma_1\gamma, \sigma_2\gamma, \dots, \sigma_n\gamma$  are distinct. If we choose  $\gamma = \alpha + \lambda\beta$ , with  $\lambda \in k$ , we merely have to ensure that

$$\sigma_i\alpha + \lambda\sigma_i\beta \neq \sigma_j\alpha + \lambda\sigma_j\beta \quad \text{for } i \neq j.$$

Since  $k$  is infinite, we can choose such a  $\lambda$ .

**Note** To find a primitive element, we construct  $\sigma_1, \sigma_2, \dots, \sigma_n$  and *then* find  $\gamma$  with  $\sigma_1\gamma, \sigma_2\gamma, \dots, \sigma_n\gamma$  distinct.

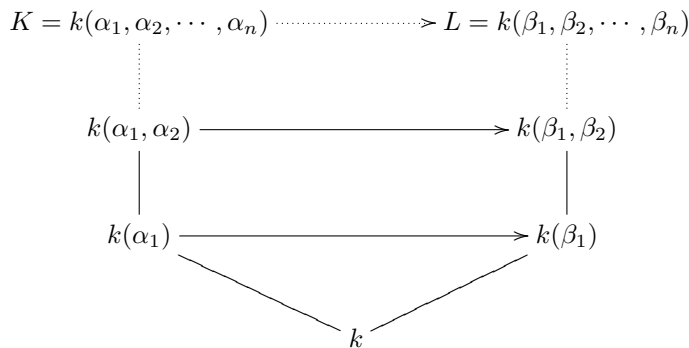
**Example** Find all primitive elements of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ . Let  $L = \mathbb{C}$  and  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , where  $\sqrt{2}, \sqrt{3} \in \mathbb{R}^+$ . Then  $x^2 - 2$  is irreducible over  $\mathbb{Q}$  by Eisenstein; hence  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , and so  $\exists$  two  $\mathbb{Q}$ -embeddings  $\sigma_1$  and  $\sigma_2$  of  $\mathbb{Q}(\sqrt{2})$  into  $L$  given by  $\sigma_1(\sqrt{2}) = \sqrt{2}$  and  $\sigma_2(\sqrt{2}) = -\sqrt{2}$ . Now consider  $x^2 - 3$ . If this were reducible over  $\mathbb{Q}(\sqrt{2})$ , then we would have  $a, b \in \mathbb{Q}$  with  $\sqrt{3} = a + b\sqrt{2}$ .

Then  $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ , and this implies that  $ab = 0$ , which is a contradiction. Hence  $x^2 - 3$  is irreducible over  $\mathbb{Q}(\sqrt{2})$ , and so it follows that  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ . There are 4 embeddings  $\tau_1, \tau_2, \tau_3$ , and  $\tau_4$  of  $K$  in  $L$  with  $\tau_1(\sqrt{3}) = \tau_3(\sqrt{3}) = \sqrt{3}$ ,  $\tau_2(\sqrt{3}) = \tau_4(\sqrt{3}) = -\sqrt{3}$ ,  $\tau_1(\sqrt{2}) = \tau_2(\sqrt{2}) = \sqrt{2}$ , and  $\tau_3(\sqrt{2}) = \tau_4(\sqrt{2}) = -\sqrt{2}$ . So  $\tau_1|_{\mathbb{Q}(\sqrt{2})} = \sigma_1$ .

Any element  $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$  can be written uniquely in the form  $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$  (see proof of the Tower Law), and  $\alpha$  is primitive iff  $\tau_1\alpha, \tau_2\alpha, \tau_3\alpha$ , and  $\tau_4\alpha$  are distinct. Now e.g.  $\tau_1\alpha = \tau_2\alpha$  if  $c = d = 0$ . Show that  $\alpha$  is primitive iff no two of  $b, c$ , and  $d$  are zero.

**Theorem 2.7** Suppose that  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$  are separable over  $k$ . Then  $k(\alpha_1, \alpha_2, \dots, \alpha_n)/k$  is separable.

**Proof** Let  $m_i = [k(\alpha_1, \alpha_2, \dots, \alpha_i) : k(\alpha_1, \alpha_2, \dots, \alpha_{i-1})]$  for  $i = 1, 2, \dots, n$ . So  $[k(\alpha_1, \alpha_2, \dots, \alpha_n) : k] = \prod_{i=1}^n m_i$ . By applying Artin's Theorem, we may construct each rung of the following ladder:



The  $(i - 1)^{\text{st}}$  rung may be lifted in  $m_i$  ways to the  $i^{\text{th}}$  rung. Hence we may construct  $m_1 m_2 \cdots m_n$   $k$ -embeddings of  $k(\alpha_1, \alpha_2, \dots, \alpha_n)$  in  $L$ . Hence by Theorem 2.5,  $k(\alpha_1, \alpha_2, \dots, \alpha_n)/k$  is separable.

**Corollary 2.8** Let  $K/k$  be an algebraic extension. Let  $S$  be the set of elements of  $K$  that are separable over  $k$ . Then  $S$  is a field and is separable over  $k$ .

**Proof** Exercise.

**Corollary 2.9** Separable extensions form a distinguished class.

**Remark** We may define differentiation in  $k[x]$  purely formally: if  $f(x) = \sum_{i=0}^n a_i x^i$ , then  $f'(x) = \sum_{i=1}^n i a_i x^{i-1}$ . If  $\alpha$  is a double root of  $f$  in  $L$ , i.e.  $(x - \alpha)^2 \mid f(x)$ , then  $(x - \alpha) \mid f'(x)$ . So if  $f$  is irreducible, then since  $\deg f' < \deg f$ , it follows that either  $f$  has distinct roots (in any extension) or  $f' = 0$ . The latter happens only in positive characteristics.

So inseparability can only occur in characteristic  $p$ , and in this case, if  $f$  is irreducible, then  $f$  is inseparable iff  $f(x) \in k[x^p]$ .

**Definition 2.10** Say that  $\alpha$  is **purely separable** over  $k$  if its minimal polynomial  $f$  has all of its roots equal to  $\alpha$ . Say that  $K/k$  is purely inseparable if every element of  $K$  is purely inseparable.

**Theorem 2.11** Let  $K/k$ , with  $\text{char } k = p$ . Then the following are equivalent:

1.  $K/k$  is purely inseparable.
2.  $K$  has just one  $k$ -embedding in  $L$ .
3.  $\exists n$  such that  $\alpha^{p^n} \in k$  for each  $\alpha \in K$ .

**Proof** We first show that (1) is equivalent to (2). Suppose that  $K/k$  is purely inseparable. Then if  $L'$  is any intermediate field,  $L'/k$  is purely inseparable. Moreover, if  $\alpha \in K$  with minimal polynomial  $f$  over  $k$  and  $g$  over  $L'$ , then  $g \mid f$ , and so all of the roots of  $g$  are equal. Thus  $K$  is purely inseparable over  $L'$ . Thus (c.f. the proof of Theorem 2.5) Artin's Extension Theorem implies that there is just one  $k$ -embedding of  $K$  in  $L$ . Conversely, if  $K/k$  is not purely inseparable, say  $\alpha \in K$  is not, then there are at least two  $k$ -embeddings of  $k(\alpha)$  in  $L$ . Artin's Theorem implies that we can lift these two disjoint  $k$ -embeddings of  $K$  in  $L$ . So (1) is equivalent to (2).

We now show that (3) implies (1). Suppose that  $\alpha^{p^n} = \beta \in k$ . Then  $\alpha$  satisfies  $x^{p^n} - \beta = 0$ . Now  $\text{char } k = p$ , and so  $x^{p^n} = (x - \alpha)^{p^n}$ . So the minimal polynomial of  $\alpha$  (which divides  $x^{p^n} - \beta$ ) has all of its roots equal to  $\alpha$ .

Finally, we show that (1) implies (3). Suppose that  $\alpha$  is purely inseparable over  $k$ . Then its minimal polynomial  $f$  factors in  $k(\alpha)$  as  $(x - \alpha)^m$ , say. Set  $m = p^a b$  with  $p \nmid b$ . The coefficient of  $x^{p^a}$  in  $f$  is

$$\binom{p^a b}{p^a} (-\alpha)^{p^a(b-1)} \in k.$$

Since  $p \nmid \binom{p^a b}{p^a}$ , we have  $\alpha^{p^a(b-1)} \in k$ . Hence  $\alpha$  satisfies  $x^{p^a(b-1)} - \alpha^{p^a(b-1)} = 0$ , a polynomial of smaller degree than  $f$ . Hence  $b = 1$ ,  $m = p^a$ , and  $\alpha^{p^a} \in k$ . Now let  $\alpha_1, \alpha_2, \dots, \alpha_r$  be a  $k$ -basis of  $K$ , and let  $n$  be such that  $\alpha^{p^n} \in k$  for  $i = 1, 2, \dots, r$ . Then if  $\alpha \in K$ ,  $\alpha = \sum_{i=1}^r x_i \alpha_i$ ,  $x_i \in k$ , and so

$$\alpha^{p^n} = \sum_{i=1}^r x_i^{p^n} \alpha_i^{p^n} \in k.$$

Thus (1) implies (3).

## Chapter 3

# The Fundamental Theorem of Galois Theory

Throughout this chapter,  $K/k$  is a finite extension.

Let  $G$  be the group of  $k$ -automorphisms of  $K$ . The aim is to use information about  $G$  to deduce information about  $K$ .

**Example** Let  $k = \mathbb{Q}$  and  $K = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ . Any  $\mathbb{Q}$ -automorphism  $\sigma$  of  $K$  satisfies  $\{\sigma\sqrt[3]{2}\}^3 = 2$ . But the other cube roots of 2 lie outside  $\mathbb{R}$ , so  $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ , and hence  $\sigma = id$ . So we have distinguished by  $G$  alone between  $k = \mathbb{Q}$  and  $K = \mathbb{Q}(\sqrt[3]{2})$ .

The problem is that  $K$  is too small; it does not contain the other cube roots of 2. Take instead  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ , where  $\omega^2 + \omega + 1 = 0$ ,  $\omega \in \mathbb{C}$ . Then  $K$  has six  $\mathbb{Q}$ -automorphisms (take  $K = L$  in Theorem 2.5) because  $K$  is a “sufficiently large extension” in the previous sense.

**Definition 3.1** An extension  $K/k$  is **normal** if, whenever  $L/K$  is an extension and  $\sigma$  is a  $k$ -embedding of  $K$  in  $L$ , then  $\sigma(K) = K$ .

**Theorem 3.2** Let  $K/k$  be a finite extension. Then the following are equivalent:

1.  $K/k$  is normal.
2. If  $\alpha \in K$  has minimal polynomial  $f$  over  $k$ , then  $f$  factors completely in  $K$ .
3.  $K$  is the splitting field of some polynomial over  $k$ .

**Proof** First we shall show that (1) implies (2). To do this, let  $L$  be a splitting field for  $f$  over  $K$ , and let  $\beta$  be any root of  $f$  in  $L$ . By Artin’s Theorem, there is a  $k$ -embedding  $\sigma$  of  $K$  in  $L$  such that

$\sigma(\alpha) = \beta$ . Since  $\sigma(K) = K$ ,  $\beta \in K$ , and  $f$  factors completely in  $K$ , as required.

Now we shall show that (2) implies (3). To do this, suppose that  $K/k$  is generated by  $\alpha_1, \alpha_2, \dots, \alpha_r$ , with minimal polynomials  $f_1, f_2, \dots, f_r$  (respectively). Let  $f = f_1 f_2 \cdots f_r$ . Then  $f$  factors completely in  $K$ , and its roots generate  $K/k$ . Thus  $K$  is the splitting field for  $f$  over  $k$ .

Finally, we shall show that (3) implies (1). Suppose that  $K$  is the splitting field for  $f$  over  $k$  and that  $f$  has roots  $\alpha_1, \alpha_2, \dots, \alpha_n$  in  $K$ . If  $\sigma$  is a  $k$ -embedding of  $K$  in  $L$ , then

$$f(\sigma\alpha_j) = (\sigma f)(\alpha_j) = f(\alpha_j) = 0.$$

So  $\sigma\alpha_j = \alpha_i$  for some  $i$ . Since  $\sigma$  is one-to-one, it follows that  $\sigma$  permutes the set  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ . As these generate  $K/k$ , we have  $\sigma(K) = K$ .

**Definition 3.3** An extension  $K/k$  which is both separable and normal is said to be **Galois**. The group  $G$  of  $k$ -automorphisms of  $K$  is called the **Galois group** of  $K/k$  and is written  $\text{Gal}(K/k)$ . Theorem 2.5 implies that  $|G| = |K : k|$ .

Associated with any subgroup  $H$  of  $G$  is the subfield of  $K$  given by

$$\text{Fix}(H) = \{x \in K : \sigma x = x \forall \sigma \in H\}.$$

Associated with any intermediate field  $L$  (i.e.  $k \subseteq L \subseteq K$ ) is a subgroup

$$\text{Gal}(K/L) = \{\sigma \in G : \sigma|_L = id_L\}.$$

**Theorem 3.4** (The Fundamental Theorem of Galois Theory) Let  $K/k$  be a finite Galois extension with Galois group  $G$ .

1. The maps  $I : H \mapsto \text{Fix}(H)$  and  $J : L \mapsto \text{Gal}(K/L)$  between subgroups of  $G$  and fields intermediate between  $k$  and  $K$  are inverse bijections.
2. The maps  $I$  and  $J$  induce a correspondence between normal subgroups of  $G$  and normal extensions of  $k$  (contained in  $K$ ). If  $L/k$  is normal, with  $k \subseteq L \subseteq K$ , then  $\text{Gal}(L/k) \simeq G/(L)$ .
3.  $I$  and  $J$  are lattice-preserving isomorphisms. This means
  - (a)  $H \subset K'$  iff  $I(H) \supset I(K')$ .
  - (b)  $I(H \cap K') = I(H)I(K')$ .
  - (c)  $I\langle H, K' \rangle = I(H) \cap I(K')$ .

**Proof**

1. First observe that clearly  $H \subset (J \circ I)(H)$  and  $L \subset (I \circ J)(L)$  for each  $H$  and  $L$ . So  $|(J \circ I)(H)| \geq |H|$ , and  $[K : L] \geq [K : (I \circ J)(L)]$ . Theorem 2.5 implies that  $|J(L)| = [K : L]$ . Theorem 2.4 implies that  $|H| \leq [K : I(H)]$ . To establish the reverse inequality, we use the Primitive Element Theorem. Let  $\alpha$  be a primitive element for  $K/k$ . Consider the polynomial

$$f(x) = \prod_{\sigma \in H} (x - \sigma\alpha).$$

If  $\tau \in H$ , the map  $\sigma \mapsto \sigma\tau$  permutes the elements of  $H$ . Hence this map preserves  $f$ . So  $f$  has coefficients in  $I(H) = \text{Fix}(H)$ , and thus  $[K : I(H)] \leq |H|$ , as required. So  $|H| = [K : I(H)]$ . Hence we have  $|(J \circ I)(H)| = [K : I(H)] = |H|$  and  $[K : (J \circ I)(L)] = |J(L)| = [K : L]$ , so  $J \circ I$  and  $I \circ J$  are both identity maps, as required.

2. Suppose first that  $H \triangleleft G$ ,  $x \in \text{Fix}(H)$ , and  $\tau \in G$ . For each  $\sigma \in H$ , we have  $\sigma\tau(x) = \tau(\tau^{-1}\sigma\tau)(x) = \tau(x)$ , so  $\tau(x) \in \text{Fix}(H)$ . Hence  $\tau(\text{Fix}(H)) = \text{Fix}(H)$  for each  $\tau \in G$ , and so  $\text{Fix}(H)/k$  is a normal extension. Conversely, suppose that  $L/k$  is normal and  $\tau \in \text{Gal}(K/L)$ . If  $l \in L$  and  $\sigma \in G$ , then  $\sigma = m \in L$ . But

$$\sigma^{-1}\tau\sigma(l) = \sigma^{-1}\tau(m) = \sigma^{-1}(m) = l.$$

Hence  $\sigma^{-1}\tau\sigma \in \text{Gal}(K/l)$ , and so  $\text{Gal}(K/L) \triangleleft G$ . The map  $\sigma \mapsto \sigma|_L$  induces the required isomorphism.

3. Exercise, e.g.

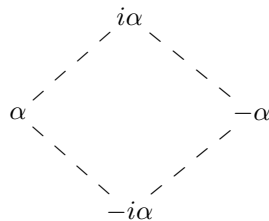
$$\begin{aligned} I(H) \cap I(K') &= \{x \mid \sigma x = x \text{ for } \sigma \in H \cup K'\} \\ &= \{x \mid \sigma x = x \text{ for } \sigma \in \langle H, K' \rangle\} \\ &= I(\langle H, K' \rangle), \text{ etc.} \end{aligned}$$

**Example** Let  $K$  denote the splitting field of  $x^4 - 2$  over  $\mathbb{Q}$ . Determine  $\text{Gal}(K/\mathbb{Q})$ . Find all the subfields of  $K$  and all inclusion relations between them, identifying which ones are normal over  $\mathbb{Q}$ .

Let  $\alpha \in \mathbb{R}^+$  satisfy  $\alpha^4 = 2$ , and let  $i \in \mathbb{C}$  satisfy  $i^2 = -1$ . Since

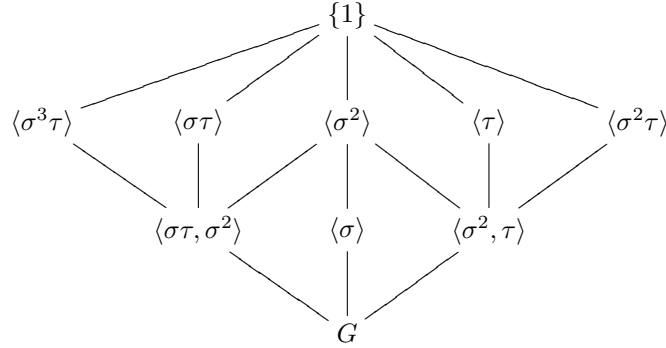
$$x^4 - 2 = (x - \alpha)(x + \alpha)(x - i\alpha)(x + i\alpha),$$

we have  $K = \mathbb{Q}(\alpha, i)$ . Eisenstein implies that  $x^4 - 2$  is irreducible over  $\mathbb{Q}$ , so  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ . Moreover,  $i \notin \mathbb{R} \supset \mathbb{Q}(\alpha)$ , so  $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$ , and hence  $[K : \mathbb{Q}] = 8$ . Let  $X = \{\alpha, -\alpha, i\alpha, -i\alpha\}$ . Then  $G = \text{Gal}(K/\mathbb{Q})$  permutes  $X$ , and  $|G| = 8$ . Let  $S$  be a square with vertices labelled by the elements of  $X$ , and let  $D_8$  be the group of rigid motions of  $S$ :

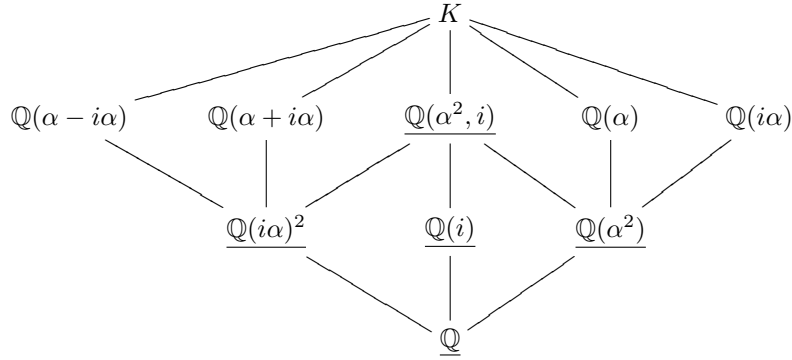


If  $\sigma \in G$ , then  $\sigma(-\alpha) = \sigma\alpha$ , so  $\sigma(-\alpha)$  and  $\sigma\alpha$  are “opposite” one another. Thus  $G \subset D_8$ , and so  $G = D_8$ , as  $|G| = |D_8|$ .

Now  $D_8 = \langle \sigma, \tau \rangle$ , where  $\sigma$  is a rotation by  $\pi/2$  and  $\tau$  is a reflection in  $\alpha, -\alpha$  axis, and  $\sigma^4 = \tau^2 = 1$ , and  $\tau\sigma\tau = \sigma^{-1}$ . Thus  $\sigma\alpha = i\alpha$ ,  $\sigma(i\alpha) = -\alpha$ ,  $\tau(i\alpha) = -i\alpha$ , etc. In  $D_8$ ,  $\sigma$  and  $\sigma^3$  have order 4; other elements have order 2.



Any subgroup of index 2 is normal, but only  $\langle \sigma^2 \rangle$  of order 2 is. Some obvious subfields are  $\mathbb{Q}(\alpha)$ ,  $\mathbb{Q}(i\alpha)$ ,  $\mathbb{Q}(i)$ ,  $\mathbb{Q}(\alpha^2)$ , and  $\mathbb{Q}(i\alpha^2)$  ( $\alpha^2 = \sqrt{2}$ , and  $i\alpha^2 = \sqrt{-2}$ ). Now  $\tau\alpha = \alpha$ , so  $\mathbb{Q}(\alpha) \subseteq \text{Fix}(\langle \tau \rangle)$ , and they are in fact equal since their degrees over  $\mathbb{Q}$  are. Similarly,  $\mathbb{Q}(i\alpha) = \text{Fix}(\langle \sigma^2 \rangle)$  and  $\mathbb{Q}(i) = \text{Fix}(\langle \sigma \rangle)$ . Now if  $\beta \in K$ , then  $\beta + \sigma\tau\beta \in \text{Fix}(\langle \sigma\tau \rangle)$ . Hence  $\mathbb{Q}(\alpha + i\alpha) = \text{Fix}(\langle \sigma\tau \rangle)$ , for  $[K : \mathbb{Q}(\alpha + i\alpha)] \leq 2$ , as we only need to adjoin  $i$  to  $\mathbb{Q}(\alpha + i\alpha)$  to get  $K$ . Similarly,  $\mathbb{Q}(\alpha - i\alpha) = \text{Fix}(\langle \sigma^3\tau \rangle)$ .



### Remarks

1. Always start with a fixed model for  $K$  (e.g. if  $K/\mathbb{Q}$  is algebraic, take  $K$  in  $\mathbb{C}$ ). If the group field is not  $\mathbb{Q}$ , then you need to invent a particular model.
2. The first step is to calculate  $[K : \mathbb{Q}]$ . This involves showing that that polynomial is irreducible.
3. You now know what  $|G|$  is and that  $G \leq S_X$ . Therefore, *guess* what  $G$  is, and then prove it. (The only other ways are either to use Artin’s Theorem to build up sufficiently many extensions or to use some more advanced group theory, e.g. Artin’s Theorem implies that

$\exists \sigma \in G$  with  $\sigma(\alpha) = i\alpha$  and  $\sigma(i) = i$ . Also  $\exists$  a complex conjugate  $\tau$ . Thus  $|\langle \sigma, \tau \rangle| = 8$  after some computation.)

4. It's not enough to say "The Galois group is  $D_8$ ." What is meant is "it is isomorphic to  $D_8$ ." A Galois group is a group of permutations of  $K$ .  $D_8 = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ .  $\sigma(\alpha) = i\alpha$ ,  $\sigma(i) = i$ ,  $\tau(\alpha) = \alpha$ , and  $\tau(i) = i$ . All other information can be deduced from this.
5. Use common sense and intelligent guesswork to compute fixed fields.

**Example** (Extensions with the Symmetric Group as Galois Group) Let  $k$  be any field, and set  $E = k(x_1, x_2, \dots, x_n)$ , where the  $x_i$ s are independent indeterminants. Then  $E$  admits  $S_n$  as a group of  $k$ -automorphisms. The fixed field  $F$  of  $S_n$  in  $E$  consists of all symmetric functions in the  $x_i$ s over  $k$ . Let  $e_1, e_2, \dots, e_n$  be the elementary symmetric functions in the  $x_i$ s. Then  $k(e_1, e_2, \dots, e_n) \subseteq F$ , and the  $x_i$ s are the roots of the equation

$$\prod_{i=1}^n (t - x_i) = t^n - e_1 t^{n-1} + \dots + (-1)^n e_n = 0.$$

Plainly,  $k$  is a splitting field of this equation over  $k(e_1, e_2, \dots, e_n)$ . Hence  $[E : k(e_1, e_2, \dots, e_n)] = n!$  since there are at least  $|S_n| = n!$  automorphisms of  $E/k(e_1, e_2, \dots, e_n)$ . Hence  $F = k(e_1, e_2, \dots, e_n)$  and  $[E : F] = n!$ ,  $\text{Gal}(E/F) \simeq S_n$ . In particular,

1. Every symmetric function in  $x_1, x_2, \dots, x_n$  is a rational function in  $e_1, e_2, \dots, e_n$ .
2. Every finite group occurs as the Galois group of some extension. (See Serre's *Topics in Galois Theory*.)

# Chapter 4

## Solubility

1. Recall that a finite group  $G$  is **soluble** if there is a chain

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

of subgroups of  $G$  with  $G_i \triangleleft G_{i+1}$  and  $G_i/G_{i-1}$  is cyclic for  $i = 1, 2, \dots, n$ .

2. If  $H \leq G$  and  $G$  is soluble, then  $H$  is soluble.
3. If  $H \triangleleft G$ , then  $G$  is soluble iff  $H$  and  $G/H$  are soluble.
4. An abelian group is soluble.

Assume  $\text{char } k = 0$ .

**Definition 4.1** An extension  $K/k$  is said to be **soluble by radicals** if there is a chain

$$k = K_0 \subset K_1 \subset \cdots \subset K_n$$

of fields with  $K \subseteq K_n$  and elements  $\alpha_i$  and integers  $m_i$  for  $i = 1, 2, \dots, n$  such that  $K_i = K_{i-1}(\alpha_i)$  and  $\alpha_i^{m_i} \in K_{i-1}$ . The extension  $K_i/K_{i-1}$  is called a **radical extension**.

**Definition 4.2** An extension  $K/k$  is **soluble** if, when  $L$  denotes the normal closure of  $K/k$ , then the group  $\text{Gal}(L/k)$  is soluble.

We want to prove an important theorem, which states that an extension  $K/k$  is soluble iff  $K/k$  is soluble by radicals.

Soluble groups are built up out of cyclic groups. Extensions soluble by radicals are built up out of radical extensions. So we need to prove that radical extensions have cyclic Galois groups, and conversely this is almost true.

**Lemma 4.3** Suppose that  $k(\alpha)/k$  is an extension with  $\alpha^n \in k$ . Suppose further than  $k$  contains an element of multiplicative order  $n$ . Then  $k(\alpha)/k$  is Galois with cyclic group of order dividing  $n$ .

**Proof** Let  $\omega \in k$  have multiplicative order  $n$ . Write  $\beta = \alpha^n \in k$ . Then  $x^n - \beta$  factors in  $k(\alpha)$  as  $\prod_{i=1}^n (x - \omega^i \alpha)$ , so  $k(\alpha)/k$  is Galois with group  $G$ , say. If  $\sigma \in G$ , then  $\sigma(\alpha) = \omega^i \alpha$  for some  $i$ .

Let  $\theta : G \rightarrow \mathbb{Z}/n\mathbb{Z}$  denote the map  $\sigma \mapsto i$ . Verify that  $\theta$  is a monomorphism. If the  $n^{\text{th}}$  roots of unity are not already present, then we adjoin them; this does not affect solubility.

**Lemma 4.4** Suppose that  $k$  is a field and  $K$  is the splitting field for  $x^n - 1$  over  $k$ . Then  $\text{Gal}(K/k)$  is abelian.

**Proof** Let  $\omega$  be a primitive  $n^{\text{th}}$  root of unity in  $K$ . If  $\sigma \in \text{Gal}(K/k)$ , then  $\sigma\omega = \omega^r$ , with  $(r, n) = 1$ . The map  $\Phi : \text{Gal}(K/k) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$  given by  $\Phi(\sigma) = r$  is easily shown to be a monomorphism.

**Lemma 4.5** (Linear Independence of Character) Suppose that  $G$  is any group,  $K$  is a field, and  $\psi_1, \psi_2, \dots, \psi_n$  are distinct multiplicative homomorphisms  $G \rightarrow K^\times$ . Then  $\psi_1, \psi_2, \dots, \psi_n$  is linearly independent over  $K$ .

**Proof** Suppose that  $\exists \alpha_1, \alpha_2, \dots, \alpha_n \in K$ , not all zero, such that  $\forall g \in G$ , we have

$$\alpha_1 \psi_1(g) + \alpha_2 \psi_2(g) + \dots + \alpha_n \psi_n(g) = 0. \quad (*)$$

We may assume that  $\alpha_1 \alpha_2 \neq 0$ . Let  $h$  be an element of  $G$  with  $\psi_1(h) \neq \psi_2(h)$ . Replacing  $g$  by  $gh$  in  $(*)$ , we obtain

$$\alpha_1 \psi_1(g) \psi_1(h) + \alpha_2 \psi_2(g) \psi_2(h) + \dots + \alpha_n \psi_n(g) \psi_n(h) = 0. \quad (**)$$

Multiplying  $(*)$  by  $\psi_1(h)$  and subtracting  $(**)$ , we achieve a smaller nontrivial relation.

Now we shall show that a cyclic extension is radical.

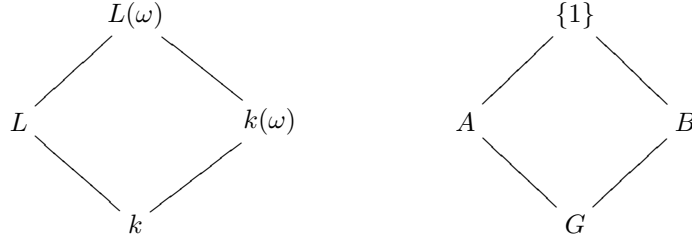
**Lemma 4.6** (Hilbert's Theorem 90) Suppose that  $K/k$  is a Galois extension of degree  $n$  with cyclic Galois group. Suppose further that  $k$  contains all  $n^{\text{th}}$  roots of unity. Then  $\exists \alpha \in K$  such that  $k = k(\alpha)$  and  $\alpha^n \in k$ .

**Proof** Suppose that  $\text{Gal}(K/k) = \langle \sigma \rangle$  and let  $\omega \in k$  be a primitive  $n^{\text{th}}$  root of unity. It suffices to find a nonzero element  $\alpha \in K$  with  $\sigma\alpha = \omega\alpha$ . For then,  $\sigma^n \alpha = (\omega\alpha)^n = \alpha^n$ , so

$\alpha^n \in \text{Fix}\langle\sigma\rangle = k$ , whilst  $\alpha, \sigma\alpha, \dots, \sigma^{n-1}\alpha$  are distinct, and so  $K = k(\alpha)$ . If  $\beta$  is any element of  $K$ , then  $\alpha = \beta + \omega^{-1}\sigma(\beta) + \dots + \omega^{1-n}\sigma^{n-1}(\beta)$  satisfies  $\sigma\alpha = \omega\alpha$ . Lemma 4.5 (with  $G = K^\times$ ) implies that there is some  $\beta$  for which  $\alpha$  does not vanish.

**Theorem 4.7** An extension  $K/k$  is soluble iff  $K/k$  is soluble by radicals.

**Proof** Suppose first that  $K/k$  is soluble. Let  $L$  be a normal closure of  $K$  and set  $n = [L : k]$ . Adjoin a primitive  $n^{\text{th}}$  root of unity  $\omega$  to  $L$ , so  $L(\omega)/k$  is Galois with group  $G$ , say. Suppose that  $L = \text{Fix}(A)$  and  $k(\omega) = \text{Fix}(B)$ . So we have the following diagram:



$\text{Fix}\{1\} = L(\omega) = \text{Fix}(A)\text{Fix}(B)$ , and so  $A \cap B = \{1\}$  (part (i) of Theorem 3.4). So  $A \cap B = \{1\}$ ,  $A \triangleleft G$ , and  $B \triangleleft G$ . Hence  $B$  is isomorphic to a subgroup of  $G/A = \text{Gal}(L/k)$ , which is soluble by assumption. Thus  $\exists$  a chain of subgroups  $\{1\} = B_0 \triangleleft B_1 \triangleleft \dots \triangleleft B_n = B$ , with each  $B_i/B_{i-1}$  cyclic. Thus we obtain a chain of fields

$$k \subseteq k(\omega) = \text{Fix}(B) \subseteq \text{Fix}(B_{m-1}) \subseteq \dots \subseteq \text{Fix}(B_0) = L(\omega).$$

By Hilbert's Theorem 90 (since  $|B| \mid n$ ),  $\exists \alpha_i \in \text{Fix}(B_{i-1})$  with  $\text{Fix}(B_{i-1}) = \text{Fix}(B_i)(\alpha_i)$  and  $\alpha_i^{m_i} \in \text{Fix}(B_i)$ , with  $m_i = [B_i : B_{i-1}]$ . So  $K/k$  is soluble by radicals, as required.

Suppose conversely that  $K/k$  is soluble by radicals. So  $\exists$  a chain

$$k = K_0 \subset K_1 \subset \dots \subset K_m = E,$$

with  $K_i = K_{i-1}(\alpha_i)$ ,  $\alpha_i^{m_i} \in K_{i-1}$  and  $E \supseteq K$ . Let  $n = \prod_{i=1}^m m_i$ ,  $L$  be a normal closure of  $E/k$ , and  $\omega$  be a primitive  $n^{\text{th}}$  root of unity, which we can join to  $L$ . Then  $L(\omega)/k$  is Galois, with group  $G$ , say.

We can reach  $L(\omega)$  from  $k(\omega)$  by a series of radical extensions as follows: Let  $1 = \sigma_1, \sigma_2, \dots, \sigma_r$  denote the elements of  $G$ . Then each step of the tower below is made up of radical steps:

$$F_{s-1} \subset F_{s-1}(\sigma_s \alpha_1) \subset F_{s-1}(\sigma_s \alpha_1, \sigma_s \alpha_2) \subset \dots \subset F_{s-1}(\sigma_s \alpha_1, \sigma_s \alpha_2, \dots, \sigma_s \alpha_n) = F_s.$$

Let the complete tower be denoted by

$$k \subseteq k(\omega) \subset L_1 \subset L_2 \subset \dots \subset L_t = L(\omega),$$

where  $L_i = L_{i-1}(\beta_i)$ ,  $\beta_i^{n_i} \in L_{i-1}$  for some  $n_i \mid n$ . By Lemma 4.3, it follows that each  $L_i/L_{i-1}$  is a Galois extension with cyclic Galois group. Converting this tower into subgroups of  $G$ , we deduce

that  $G$  is soluble and thus that  $\text{Gal}(L/k)$  is soluble, as required.

**Example** (The Quadratic Equation) Let  $f(x) = x^2 + bx + c$ . Then the roots of  $f$  are given by

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

There are no roots of unity to adjoin, as  $x^2 - 1$  already splits. So  $K$  is a splitting field for  $f$  over  $k$ . Hence  $K/k$  is Galois of degree 1 or 2. Suppose that  $[K : k] = 2$  and  $G = \langle \sigma \rangle = \text{Gal}(K/k)$ . Via Hilbert's Theorem 90, we look at  $\alpha = \beta - \sigma\beta$  for  $\beta \in K$ . Thus  $\sigma\alpha = -\alpha$ , so  $\alpha^2 \in k$ . Thus if  $\beta_1$  and  $\beta_2$  are the roots of  $f$ , then  $\alpha = \beta_1 - \beta_2$  satisfies

$$\alpha^2 = (\beta_1 - \beta_2)^2 - 4\beta_1\beta_2 = b^2 - 4c.$$

Since  $\beta_1 + \beta_2 = -b$ , we obtain the solution.

**Example** (The General Cubic Equation) Let  $f(x) = x^3 + ax^2 + bx + c$ . Adjoin  $\omega$  to  $k$ , where  $\omega^2 + \omega + 1 = 0$ , so  $\omega$  is a primitive cube root of unity. The Galois group of  $f$  over  $k(\omega)$  is a subgroup of  $S_3$  with composition series  $\{1\} \triangleleft A_3 \triangleleft S_3$ . If  $\beta_1, \beta_2$ , and  $\beta_3$  are the roots of  $f$ , then we consider  $\alpha_1 = \beta_1 + \omega^2\beta_2 + \omega\beta_3$  and  $\alpha_2 = \beta_1 + \omega\beta_2 + \omega^2\beta_3$ . Then  $\alpha_1^3 + \alpha_2^3$  and  $\alpha_1^3\alpha_2^3$  are invariant under  $S_3$  and so lie in  $k(\omega)$ . Hence we obtain a formula for  $\alpha_1$  and  $\alpha_2$ , and so from the above together with the fact  $\beta_1 + \beta_2 + \beta_3 = -a$ , we get the cubic equation.

**Example** (The General Quartic Equation) Let  $f(x) = x^4 + ax^3 + bx^2 + cx + d$ . Suppose that the roots are  $\beta_1, \beta_2, \beta_3$ , and  $\beta_4$ . Observe that if  $\alpha_1 = \beta_1\beta_2 + \beta_3\beta_4$ ,  $\alpha_2 = \beta_1\beta_3 + \beta_2\beta_4$ , and  $\alpha_3 = \beta_1\beta_4 + \beta_2\beta_3$ , then  $\alpha_1, \alpha_2$ , and  $\alpha_3$  are permuted by  $S_4$ . Thus  $\alpha_1, \alpha_2$ , and  $\alpha_3$  are the roots of some cubic which may be determined.

What happens in characteristic  $p > 0$ ? First observe that a cyclic Galois extension of degree  $p$  cannot be of the form  $k(\alpha^{1/p})/k$ , since this is purely inseparable.

**Lemma 4.8** Suppose that  $\text{char } k = p > 0$ .

1. If  $K/k$  is a Galois extension of degree  $p$ , then  $\exists \alpha \in K$  such that  $K = k(\alpha)$  and  $\alpha^p - \alpha \in k$ .
2. Conversely, for each  $a \in k$ , consider the polynomial  $x^p - x - a$ . Either it has a root in  $k$ , in which case all the roots are in  $k$ , or it is irreducible over  $k$ . In the latter case, if  $\alpha$  is a root, then  $k(\alpha)/k$  is a Galois extension of degree  $p$ .

**Proof** Suppose that we find  $\alpha \in K$  such that  $\sigma\alpha = \alpha + 1$ . Then

$$\sigma(\alpha^p - \alpha) = (\sigma\alpha)^p - \sigma\alpha = \alpha^p - \alpha.$$

So  $\alpha^p - \alpha \in k$ , as required. Furthermore, since  $\alpha \notin k$ ,  $K = k(\alpha)$ . Choose

$$\gamma = -\beta - 2\sigma\beta - \cdots - (p-1)\sigma^{p-2}\beta.$$

Then

$$\sigma\gamma - \gamma = \beta + \sigma\beta + \cdots + \sigma^{p-1}\beta = \delta \in k.$$

Linear independence of characters implies that  $\exists \beta \in K$  with  $\delta \neq 0$ . Set  $\alpha = \gamma/\delta$ .

Conversely, consider the polynomial  $f(x) = x^p - x - a$ . If  $\alpha \in k$  is a root, then  $f(x)$  factors as

$$f(x) = \prod_{i=1}^p (x - \alpha - i).$$

On the other hand, if  $f$  has no roots in  $k$ , let  $K = k(\alpha)$ . Then  $f$  factors in  $K$  with Galois group  $G$ , say. If  $\sigma \in G$ ,  $\sigma\alpha = \alpha + r$ , say ( $r \neq 0$ ). Then  $\sigma$  has order  $p$ . So  $|G| \geq p$ ,  $f$  is irreducible over  $k$ , and  $|G| = p$ .

**Definition 4.9** An extension  $K$  of a field  $k$  of char  $p > 0$  is said to be **soluble by radicals** if  $K/k$  is separable and there is a chain

$$k = K_0 \subset K_1 \subset \cdots \subset K_m$$

of fields with  $K_m \supset K$  such that for each  $i$ ,  $\exists$  an element  $\alpha_i \in L_i$  with  $K_i = K_{i-1}(\alpha_i)$  and either  $\alpha_i^{m_i} \in K_{i-1}$  with  $p \nmid m_i$  or  $\alpha_i^p - \alpha_i \in K_{i-1}$ .

**Theorem 4.10** Let  $K/k$  be a finite separable extension with char  $k = p > 0$ . Then  $K/k$  is soluble by radicals iff  $K/k$  is soluble.

**Proof** Exercise.

# Chapter 5

## Miscellanea

### 5.1 Finite Fields

**Theorem 5.1** Let  $K$  be a finite field. Then the multiplicative group  $K^\times$  is cyclic.

**Proof** Let  $m = |K^\times| = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$  be the decomposition into primes. For each  $i$ ,  $\exists x \in K$  with  $x^{m/p_i} \neq 1$  (since  $x^n - 1$  has at most  $n$  roots for any  $n$ ). So  $x_i = x^{m/p_i^{r_i}}$  has order  $p_i^{r_i}$ . We claim that  $y = x_1 x_2 \cdots x_s$  has order  $m$ . Suppose not. Then  $y$  has order  $t$  with  $t \mid m$ , so some  $p_i \mid \frac{m}{t}$ . Then  $1 = y^{m/p_i} = x_i^{m/p_i}$ , which is a contradiction. Hence  $y$  has order  $m$ , and  $K^\times$  is cyclic.

**Theorem 5.2** Suppose that  $K$  is a finite field of order  $q$ . Then  $q$  is a power of some prime, say  $q = p^n$ , and  $K$  is a splitting field over  $\mathbb{F}_p$  of  $x^q - x$ . Moreover,  $K/\mathbb{F}_p$  is Galois of order  $n$  with cyclic Galois group generated by  $\sigma : x \mapsto x^p$ . Conversely, for each integer  $n$ ,  $\exists$  a field of order  $p^n$ .

**Proof** Let  $p = \text{char } K$ . So  $\mathbb{F}_p \subseteq K$ , and  $[K : \mathbb{F}_p] = n$ . If  $x_1, x_2, \dots, x_n$  are an  $\mathbb{F}_p$ -basis of  $K$ , then every element of  $K$  can be written uniquely in the form  $\sum_{i=1}^n \lambda_i x_i$ ,  $\lambda_i \in \mathbb{F}_p$ . Hence  $q = p^n$ , as asserted. If  $0 \neq x \in K$ , then  $x^q = 1$ , and so every  $x \in K$  satisfies  $x^q = x$ . Hence  $K$  is a splitting field for  $x^q - x$  over  $\mathbb{F}_p$ .

The map  $\sigma : x \mapsto x^p$  is an automorphism of  $K$  fixing  $\mathbb{F}_p$ , and  $\sigma^n = 1$ . If  $\sigma^m = 1$ , then  $x^{p^m} = x \forall x \in K$ . So  $p^m \geq |K| = q$ . Thus  $\sigma$  has order  $n$ , and  $\langle \sigma \rangle = \text{Gal}(K/\mathbb{F}_p)$ . Finally, for each  $n \in \mathbb{N}$ , let  $L$  be a splitting field of  $x^{p^n} - x$  in  $L$ . Verify that  $S$  forms a field, and since the roots are distinct,  $|S| = p^n$ , as required.

**Notation** We write  $L = \mathbb{F}_q$ , and  $\sigma$  is the **Frobenius automorphism**.

## 5.2 Transcendental Extensions

**Definition 5.3** Suppose that  $K/k$  is an extension (not necessarily finite). A set  $S$  in  $K$  is **algebraically independent** over  $k$  if whenever  $x_1, x_2, \dots, x_n \in S$  and  $f \in k[x_1, x_2, \dots, x_n]$  satisfies  $f(x_1, x_2, \dots, x_n) = 0$ , then  $f = 0$ . In this case, the field  $k(S)$  is isomorphic to the field of fractions of the ring  $k[x_s : s \in S]$  of polynomials over  $k$  in  $|S|$  indeterminates.

**Definition 5.4** A set  $S$  is called a **transcendence basis** of  $K/k$  if  $S$  is algebraically independent over  $k$  and  $K/k(S)$  is algebraic.

**Theorem 5.5** Suppose that  $S$  and  $T$  are transcendence bases of  $K/k$  and  $S$  is finite. Then  $T$  is finite, and  $|S| = |T|$ .

**Proof** Suppose that  $|T| > |S| = n$  and  $T \supset \{x_1, x_2, \dots, x_n\}$ . Let  $S = \{y_1, y_2, \dots, y_n\}$ . We still have to prove that  $\{x_1, x_2, \dots, x_n\}$  forms a transcendence basis. Now  $x_1$  is algebraic over  $k(S)$ , so  $\exists$  a polynomial  $0 \neq f \in k[x_1, y_1, y_2, \dots, y_n]$  with  $f(x_1, y_1, y_2, \dots, y_n) = 0$ . Now  $x_1$  is transcendental over  $k$ , so  $f$  involves some  $y$ , say  $y_1$ . Then  $y_1$  is algebraic over  $k(x_1, y_2, y_3, \dots, y_n)$ , so  $K$  is also. Also,  $x_1, y_2, y_3, \dots, y_n$  are algebraically independent because otherwise  $x_1$  would be algebraic over  $k(x_1, y_2, y_3, \dots, y_n)$ , and so  $y_1$  would be also. Hence  $x_1, y_2, y_3, \dots, y_n$  is a transcendence basis of  $K/k$ . Repeating this argument, we deduce that  $x_1, x_2, \dots, x_n$  is a transcendence basis, as required.

**Notation** We write  $[K : k]_{tr} = |S|$  if  $|S| < \infty$ , otherwise  $[K : k]_{tr} = \infty$ . If  $K/k$  is algebraic, then  $S = \emptyset$ , and we write  $[K : k]_{tr} = 0$ .

**Theorem 5.6** Suppose that  $L/k$  and  $K/k$  are two extensions. Then  $[L : k]_{tr} = [L : K]_{tr} + [K : k]_{tr}$ .

**Proof** If either  $[L : K]_{tr}$  or  $[K : k]_{tr} = \infty$ , then plainly  $[L : k]_{tr} = \infty$ . So suppose that  $x_1, x_2, \dots, x_n$  is a transcendence basis for  $L/K$  and  $y_1, y_2, \dots, y_m$  is a transcendence basis for  $K/k$ . We still have to prove that  $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$  is a transcendence basis of  $L/k$ . We have that  $L/K(x_1, x_2, \dots, x_n)$  and  $K/k(y_1, y_2, \dots, y_m)$  are algebraic. Hence

$$K(x_1, x_2, \dots, x_n)/k(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m)$$

is algebraic, and therefore so is  $L/k(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m)$ .

Now suppose that  $f \in k[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$ , with  $f(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) = 0$ . Write

$$f = \sum_{\tilde{r}} f_{\tilde{r}} x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n},$$

with  $f_{\tilde{r}} \in k[y_1, y_2, \dots, y_m]$ . Since  $f_{\tilde{r}}(y_1, y_2, \dots, y_m) \in K$  and  $x_1, x_2, \dots, x_n$  are algebraically independent over  $K$ , it follows that  $f_{\tilde{r}}(y_1, y_2, \dots, y_m) = 0 \forall \tilde{r}$ . Since  $y_1, y_2, \dots, y_m$  are algebraically independent over  $k$ , it follows that  $f_{\tilde{r}} = 0$  for each  $\tilde{r}$ , whence  $f = 0$ , as required.

### 5.3 Algebraic Closures

**Definition 5.7** If  $k$  is a field, then an **algebraic closure**  $K$  of  $k$  is a field which is algebraically closed and has the property that  $K/k$  is algebraic. Observe that if  $L$  is algebraically closed and  $k \subseteq L$ , then the set  $X$  of elements in  $L$  algebraic over  $k$  forms an algebraic closure of  $k$ .

**Theorem 5.8** Let  $k$  be a field. Then  $k$  has an algebraic closure.

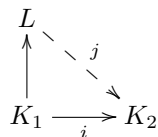
**Proof** Let  $S$  be the set of monic irreducible polynomials over  $k$  in a variable  $x$ . Let  $R$  be the ring of polynomials in the variables  $\{1/f : f \in S\}$  over  $k$ . Let  $I$  be the ideal in  $R$  generated by the polynomials  $f(1/f)$ . We claim that  $I \neq R$ . Otherwise,  $\exists f_1, f_2, \dots, f_n \in S$  and  $g_1, g_2, \dots, g_n \in R$  with  $g_1 f_1(Y_1) + g_2 f_2(Y_2) + \dots + g_n f_n(Y_n) = 1$  as an identity in the indeterminates  $\{Y_f\}$ .

If  $L$  is a splitting field for  $f_1(X)f_2(X) \dots f_n(X)$ , then we may substitute  $Y_{f_i} = \alpha_i$ , whence  $f_i(\alpha_i) = 0$  and obtain a contradiction. Thus  $I$  is a proper ideal of  $R$ , and so (by Zorn's Lemma) it is contained in some maximal ideal  $M$ .

Let  $K = R/M$ . Then  $K$  contains a copy of  $k$  as the constant polynomials. If  $f$  is any irreducible polynomial over  $k$ , then  $f([Y_f]) = 0$  in  $K$ , so  $f$  has a root in  $K$ . Also,  $K/k$  is algebraic, as it is generated by  $\{[Y_f] : f \in S\}$ . Repeat the above to construct extension fields  $K = K_1, K_2, \dots$  successively so that  $K_i/K_{i-1}$  is algebraic, and each polynomial in  $K_{i-1}[X]$  has a root in  $K_i$ . Let  $L = \bigcup_{i=1}^{\infty} K_i$ . Then  $L$  is a field,  $L/k$  is algebraic, and any polynomial in  $L[X]$  has a root in  $L$ . Thus  $L$  is an algebraic closure of  $K$ .

**Theorem 5.9** Suppose that  $i : K_1 \rightarrow K_2$  is a monomorphism, that  $L/K_1$  is algebraic, and that  $K_2$  is algebraically closed. Then  $\exists$  a monomorphism  $j : L \rightarrow K_2$  so that  $j|_{K_1} = i$ .

**Picture**



**Proof** Let

$$S = \left\{ \begin{array}{l} (M, \theta) : M \text{ is a field with } K_1 \subseteq M \subseteq L \\ \theta : M \rightarrow K_2 \text{ is an embedding with } \theta|_{K_1} = i. \end{array} \right.$$

Partially order  $S$  by setting  $(M_1, \theta_1) \leq (M_2, \theta_2)$  if  $M_1 \subseteq M_2$  and  $\theta_2|_{M_1} = \theta_1$ . If  $\mathcal{C}$  is a chain in  $S$ , let  $N = \bigcup\{M : (M, \theta) \in \mathcal{C}\}$ . If  $n \in N$ , then  $n \in M$  for some  $(M, \theta) \in \mathcal{C}$ . Set  $\phi(n) = \theta(n)$ . Verify that  $\phi$  is well-defined,  $\phi : N \rightarrow K_2$  is an embedding, and  $(N, \phi)$  is an upper bound of  $\mathcal{C}$ . Then Zorn's Lemma implies that  $S$  has a maximal element,  $(M, \theta)$ , say. We claim that  $M = L$ . If not,  $\exists \alpha \in L \setminus M$ . Then  $\alpha$  is algebraic over  $M$ . Let  $f(x)$  be the minimal polynomial of  $\alpha$  over  $M$ . Then  $\theta(f)$  splits over  $K_2$  (since  $K_2$  is algebraically closed). Let

$$\theta(f) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_n).$$

Then Artin's Theorem implies that  $\exists$  a monomorphism  $\theta_i : M(\alpha) \rightarrow K_2$  with  $\theta_i(\alpha) = \beta_1$  and  $\theta_i|_M = \theta$ , which is a contradiction since  $(M, \theta)$  is maximal.

**Theorem 5.10** Suppose that  $L_1$  and  $L_2$  are two algebraic closures of  $K$ , with  $i_1 : K \rightarrow L_1$  and  $i_2 : K \rightarrow L_2$ . Then  $\exists$  an isomorphism  $j : L_1 \xrightarrow{\sim} L_2$  such that  $i_2 = ji_1$ .

**Proof** Theorem 5.9 implies that  $\exists$  a monomorphism  $j : L_1 \rightarrow L_2$  such that  $i_2 = ji_1$ .

$$\begin{array}{ccc} L_1 & \xrightarrow{j} & L_2 \\ & \swarrow i_1 & \nearrow i_2 \\ & K & \end{array}$$

If  $f \in K[x]$  is irreducible over  $K$ , then  $i_1(f)$  splits over  $L_1$ , and so  $i_2(f)$  splits over  $j(L_1)$ . Since  $j(L_1)/K$  is algebraic, it follows that  $j(L_1)$  is an algebraic closure of  $K$ . Since  $L_2/K$  is algebraic,  $L_2/j(L_1)$  is also algebraic. Thus  $L_2 = j(L_1)$ . (Show this.)

## Chapter 6

# $KG$ -Modules and Their Representations

**Definition 6.1** Let  $K$  be a field and  $G$  a group. A  $K$ -vector space  $V$  is called a  $KG$ -**module** (and we say that  $G$  acts on  $V$ ) if there is a given map  $G \times V \rightarrow V$  such that

1. For each  $g \in G$ , the map  $v \mapsto g(v)$  is linear.
2.  $1(v) = v \forall v \in V$ .
3.  $(g_1 g_2)(v) = g_1(g_2 v) \forall v \in V \forall g_1, g_2 \in G$ .

**Proposition 6.2**

1. Let  $V$  be a  $KG$ -module, and for  $g \in G$ , let  $\rho(g)$  be the map  $v \mapsto g(v)$ . Then  $\rho(g) \in GL(V)$  ( $GL(V)$  is group of invertible linear maps on  $V$ ), and the map  $\rho : g \mapsto \rho(g)$  is a homomorphism.
2. Conversely, if  $\rho : G \rightarrow GL(V)$  is a homomorphism, write  $g(v) = \rho(g)(v)$  for each  $v \in V, g \in G$ . Then  $V$  becomes a  $KG$ -module.

**Proof** Easy exercise.

**Definition 6.3** A  $K$ -**linear representation** of  $G$  is a homomorphism  $\rho : G \rightarrow GL(V)$ , where  $V$  is a  $K$ -vector space. If  $\dim V$  is finite, then  $\dim V$  is the **degree** of  $\rho$ .

**Motivation**

1. (Group Theoretic) To study arbitrary  $G$ , seek some familiar group so that  $\exists$  many homomorphisms from  $G$  to these groups. These homomorphisms are called representations of  $G$ .
  - (a) For example, homomorphisms into  $S_n$  are permutation representations.
  - (b) Linear groups  $GL(V) \rightsquigarrow$  linear representations.  
The advantage of (b) is that we can bring linear algebra to bear on purely group theoretic problems. For example,

- i. Burnside's  $p^\alpha q^\beta$  Theorem (every group of order  $p^\alpha q^\beta$ , where  $p$  and  $q$  are primes, is soluble) was proven using representation theory in 1912, and a purely group theoretic proof was not found until 1972.
- ii. We can get useful information about a character table of a finite group using representation theory.

There are lots of applications elsewhere in math and physics.

The study of linear representations of a finite group is equivalent to the study of matrix representations.

**Definition 6.4** A **matrix representation** of  $G$  is a homomorphism  $G \rightarrow GL_n(K)$ .

- 1. If  $\rho : G \rightarrow GL(V)$  is a linear representation of  $G$  of degree  $n$ , then we obtain a matrix representation  $\theta : G \rightarrow GL_n(K)$  by choosing a  $K$ -basis of  $V$ .
- 2. Conversely, given a matrix representation  $\theta : G \rightarrow GL_n(K)$ , let  $GL_n(K)$  act on  $K^n$  (column vectors). Then  $K^n$  becomes a  $KG$ -module.

### Examples

- 1. Given a  $K$ -vector space  $V$  and a group  $G$ , define  $g(v) = v \forall g \in G, v \in V$ . Then  $V$  is a  $KG$ -module corresponding to the trivial homomorphism  $\rho$  with  $\rho(g) = 1 \forall g \in G$ .
- 2. Representations of degree 1: If  $\rho$  has degree 1, then each  $\rho(g)$  is multiplication by some scalar  $\lambda g \in K \setminus \{0\}$ .  $\rho$  is a homomorphism

$$\begin{aligned} \rho : G &\rightarrow K^\times \\ g &\mapsto \lambda g. \end{aligned}$$

(a)

$$G = S_n$$

$\epsilon : S_n \rightarrow \{\pm 1\}$  is the signature representation.

Then  $\epsilon$  is a representation of degree 1 (over  $\mathbb{C}$ , say).

- (b) If  $G$  is a group of invertible  $n \times n$  matrices, then  $\det : G \rightarrow K^\times$  is a representation of degree 1.
- (c)  $|G| = n$ ,  $G = \langle t \rangle$ . Define  $\rho(t^r) = \exp(2\pi ir/n)$ , so  $\rho : G \rightarrow S^1$ .
- 3. Let  $V$  be a 2-dimensional  $K$ -vector space with basis  $\{e_1, e_2\}$ . Suppose that  $G$  is infinite,  $G = \langle t \rangle$ . Define  $\rho(t^r)e_1 = e_1 + re_2$  and  $\rho(t^r)e_2 = e_2$ . Then the matrix representation is

$$t^r \mapsto \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}.$$

4. Let  $X$  be a finite set and  $\pi : G \rightarrow S_X$  a homomorphism. Let  $V$  be a  $K$ -vector space with basis elements in one-to-one correspondence with those of  $X$  under the map  $x \mapsto x^*$  ( $x \in X$ ). Define  $\widehat{\pi} : G \rightarrow GL(V)$  by specifying the action of  $G$  on a basis

$$\widehat{\pi}(g)(x^*) = \{\pi(g)x\}^*.$$

Then  $V$  becomes a  $KG$ -module.

**Definition 6.5** A  $KG$ -submodule of  $G$ -invariant subspace of a  $KG$ -module  $V$  is a subspace  $W$  such that  $g(w) \in W \forall w \in W, g \in G$ .

Let  $V_1$  and  $V_2$  be  $KG$ -modules with corresponding representations  $\rho_1$  and  $\rho_2$ . A map  $f : V_1 \rightarrow V_2$  is a  $KG$ -(module) homomorphism iff

1.  $f$  is linear.
2.  $g(f(v)) = f(g(v)) \forall v \in V, g \in G$ , i.e.  $\rho_2(g)(f(v)) = f(\rho_1(g)v)$ , i.e.  $\rho_2(g) \circ f = f \circ \rho_1(g) \forall g \in G$ .

**Definition 6.6** Representations  $\rho_1 : G \rightarrow GL(V_1)$  and  $\rho_2 : G \rightarrow GL(V_2)$  are **equivalent** iff  $V_1$  and  $V_2$  are isomorphic as  $KG$ -modules.

**Proposition 6.7**

1. If  $f : V_1 \rightarrow V_2$  is an isomorphism of a finite dimensional vector space, and  $B_1 = \{e_1, e_2, \dots, e_n\}$  is a basis of  $V_1$ , then  $B_2 = \{f(e_1), f(e_2), \dots, f(e_n)\}$  is a basis of  $V_2$ , and

$$[f\alpha f^{-1}]_{B_2} = [\alpha]_{B_1}$$

for each endomorphism  $\alpha$  of  $V_1$ .

2. Two finite dimensional representations  $\rho_1 : G \rightarrow GL(V_1)$  and  $\rho_2 : G \rightarrow GL(V_2)$  are equivalent iff they give the same matrix representations  $g \mapsto [\rho_1(g)]_{B_1}$  and  $g \mapsto [\rho_2(g)]_{B_2}$  for suitable choices of bases  $B_1$  and  $B_2$ .

**Proof** Exercise in linear algebra.

**Definition 6.8** A  $KG$ -module  $V$  is **irreducible** if  $V \neq 0$  and  $V$  has no submodules except  $V$  and  $\{0\}$ .

## 6.1 Schur's Lemma and Maschke's Theorem

**Theorem 6.9** (Schur's Lemma)

1. If  $U$  and  $V$  are irreducible  $KG$ -modules, and  $f : U \rightarrow V$  is a  $KG$ -homomorphism, then either  $f = 0$  or  $f$  is an isomorphism.
2. If  $U$  is an irreducible  $KG$ -module with  $\dim U$  finite and  $K$  is algebraically closed, then any  $KG$ -homomorphism  $f : U \rightarrow U$  is a multiple of the identity.

**Proof**

1. Assume that  $f \neq 0$ . Then  $\ker f$  is a  $KG$ -submodule of  $U$ , so  $\ker f = \{0\}$ . The image of  $f$  is a  $KG$ -submodule of  $V$ , so  $\text{Im } f = V$ .
2. Since  $K$  is algebraically closed,  $f$  has an eigenvalue  $\lambda$ , say. The map  $f - \lambda 1_U$  is also a  $KG$ -homomorphism with nontrivial kernel. So  $f - \lambda 1_U = 0$ .

**Remark** Let  $U$  be any finite dimensional  $KG$ -module. The set  $\text{hom}_{KG}(U, U)$  of  $KG$ -module maps  $U \rightarrow U$  is a subspace and subring of the space  $\text{hom}_K(U, U)$  of  $K$ -linear maps  $U \rightarrow U$ . If  $U$  is irreducible, then each nonzero element of  $\text{hom}_{KG}(U, U)$  has an inverse, by Schur's Lemma. So  $\text{hom}_{KG}(U, U)$  is a division ring. If  $K$  is algebraically closed, then only division ring finite dimensional as a  $K$ -vector space is  $K$ . Hence Theorem 6.9(2). If  $K = \mathbb{R}$ , the division rings finite dimensional over  $\mathbb{R}$  are  $\mathbb{R}$ ,  $\mathbb{C}$ , and  $\mathbb{H}$ .

**Corollary 6.10** If  $G$  is abelian and  $K$  is algebraically closed, then each irreducible finite dimensional  $KG$ -module  $V$  has dimension 1. So the irreducible representations of  $G$  are the elements of the set  $\text{hom}(G, K^\times)$ .

**Proof** If  $G$  is abelian, then  $g(h(v)) = h(g(v)) \forall v \in V, g, h \in G$ , and so each map  $v \mapsto h(v)$  is a  $KG$ -homomorphism. This implies that each map  $v \mapsto h(v)$  is a scalar multiplication by Theorem 6.9(2). So every  $K$ -subspace is a  $KG$ -submodule, whence it follows that  $\dim V = 1$  since  $V$  is irreducible.

**Definition 6.11** A  $KG$ -submodule is said to be **completely irreducible** if it is a direct sum of irreducible modules.

**Proposition 6.12** The following conditions are equivalent for a finite dimensional  $KG$ -module in  $V$ .

1.  $V$  is a direct sum of irreducible modules.
2.  $V$  is a sum (not necessarily direct) of irreducible modules.
3. For each submodule  $U$  of  $V$ , there is a submodule  $W$  of  $V$  with  $V = U \oplus W$ .

**Proof** It is clear that (1) implies (2). To show that (2) implies (3), we use induction on  $m = \dim V - \dim U$ .  $m = 0$  works. If  $U \subset V$ , there is an irreducible submodule  $M$  of  $V$  such that  $M \not\subseteq U$ .

Now  $M \cap U$  is a submodule of  $M$ , so  $M \cap U = 0$  and  $M + U = M \oplus U$ . But  $\dim V = \dim(M \oplus U) < m$ , so  $\exists$  a submodule  $W$  such that  $V = (U \oplus M) \oplus W_1 = U \oplus (M \oplus W_1)$ .

To show that (3) implies (1), first observe that if  $V$  satisfies (3), so does each submodule  $V$ . If  $U_1$  is a submodule of  $V_1$ , then there is a submodule  $W$  of  $V$  such that  $V = U_1 \oplus W$ . So  $V_1 = U_1 \oplus (W \cap V_1)$  since  $U_1 \leq V_1$ . Now suppose that  $V$  satisfies (3). We prove (1) by induction on  $\dim V$ . If  $V = 0$  or  $V$  is irreducible, then (1) holds. Otherwise  $\exists$  a submodule  $U$  of  $V$  with  $0 < U < V$ , and so by (3),  $\exists$  a submodule  $W$  with  $V = U \oplus W$ . By induction, since  $U$  and  $W$  satisfy (3), we have  $U = U_1 \oplus U_2 \oplus \cdots \oplus U_r$  and  $W = W_1 \oplus W_2 \oplus \cdots \oplus W_s$ , with each  $U_i$  and  $W_j$  irreducible. So  $V = U_1 \oplus U_2 \oplus \cdots \oplus U_r \oplus W_1 \oplus W_2 \oplus \cdots \oplus W_s$ .

**Note** The expression of a completely reducible module as a direct sum of irreducible submodules is rarely unique, e.g. take  $G = 1$ . Then any expression of  $V$  as a direct sum of 1-dimensional subspaces qualifies.

**Proposition 6.13** Let  $V = U_1 \oplus U_2 \oplus \cdots \oplus U_r = U'_1 \oplus U'_2 \oplus \cdots \oplus U'_s$  be two decompositions of a finite dimensional  $KG$ -module  $V$  as a direct sum of irreducible submodules.

1. For any irreducible  $KG$ -module  $X$ , the direct sum  $W$  of the  $U_i$ s isomorphic to  $X$  equals the direct sum  $W'$  of the  $U'_j$ s isomorphic to  $X$ .
2. For each irreducible  $X$ , the number of  $U_i$ s isomorphic to  $X$  equals the number of  $U'_j$ s isomorphic to  $X$ .
3.  $r = s$ .

**Proof**

1. Suppose that  $U_i \simeq X$ . For each  $j$ , consider the map

$$U_i \begin{array}{c} \hookrightarrow V \\ \text{incl} \end{array} \begin{array}{c} \rightarrow U'_j \\ \text{proj} \end{array}$$

By Schur's Lemma, this is 0 unless  $U'_j \simeq X$ . So  $U_i$  has nonzero projection only into the  $U'_j$  with  $U'_j \simeq X$ , so  $U_i \leq W'$ . Hence  $W \leq W'$ . Similarly,  $W' \leq W$ .

2. Observes that  $\dim W = (\dim X) \times (\text{number of } U_j \simeq X)$ .
3. Take the sum of (2) over all relevant  $X$ .

**Theorem 6.14** (Maschke's Theorem) Let  $G$  be a finite group, and let  $K$  be a field of characteristic zero or characteristic prime to  $|G|$ . If  $V$  is a finite dimensional  $KG$ -module and  $U$  is a submodule of  $V$ , then there is a submodule  $W$  of  $V$  such that  $V = U \oplus W$ . So every  $KG$ -module is completely reducible.

**Proof** Take a linear map  $\theta : V \rightarrow U$  such that  $\theta(u) = u \forall u \in U$ . (Extend a basis of  $U$  to a basis of  $V$ .) Define  $\phi : V \rightarrow U$  by

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} (g\theta g^{-1})(v).$$

(Division by  $|G|$  is possible, as the image of  $|G|$  in  $K$  is nonzero.) Each  $g\theta g^{-1}$  is linear, so  $\phi$  is linear.  $\text{Im } \phi \leq U$  since  $\text{Im } \theta \leq U$  and  $U$  is a  $KG$ -submodule of  $V$ . Observe that if  $u \in U$ , then  $g^{-1}(u) \in U$ , and so  $\theta(g^{-1}(u)) = g^{-1}(u)$ , and so  $(g\theta g^{-1})(u) = u$ . So if  $u \in U$ , then  $\phi(u) = u \in U$ . Hence  $\text{Im } \phi = U$ . Since  $\ker \phi \cap U = 0$ , we have  $V = U \oplus \ker \phi$ . But  $\phi$  is a  $KG$ -homomorphism, and so  $\ker \phi$  is a  $KG$ -submodule of  $V$ .

$$h(\phi(v)) = \frac{1}{|G|} \sum_{g \in G} h(g\theta g^{-1})(v) = \frac{1}{|G|} \sum_{g \in G} (hg)\theta(hg)^{-1}(hv) = \phi(h(v))$$

for all  $h \in G$ .

**Corollary 6.15** If  $f : V \rightarrow W$  is a linear map, where  $V$  and  $W$  are  $KG$ -modules, then  $\hat{f}$  is defined by

$$\hat{f} = \sum_{g \in G} gf g^{-1}$$

is a  $KG$ -homomorphism.

**Example** Let  $K$  be a field and  $V$  a  $K$ -vector space of dimension 2 with basis  $\{e_1, e_2\}$ . Let  $t$  be the map defined by

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

(so  $e_1 \mapsto e_1 + e_2$  and  $e_2 \mapsto e_2$ ). For each  $n \in \mathbb{Z}$ ,  $t^n$  has matrix

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}.$$

Hence if  $\text{char } K = p$ ,  $V$  is a module for the cyclic group of order  $p$ ; if  $\text{char } K = 0$ ,  $V$  is a module for an infinite cyclic group.

$V$  is not irreducible. Since  $t(e_2) = e_2$ , the module  $\langle e_2 \rangle$  is a 1-dimensional submodule of  $V$ . If  $V$  were completely reducible, there would exist a 1-dimensional submodule  $\langle f \rangle$  with  $V = \langle f \rangle \oplus \langle e_2 \rangle$ . Suppose that  $t(f) = \lambda f$ , where  $\lambda \in K$ . Then

$$\text{Tr}(t) = \begin{cases} 2 & \text{computed with respect to the basis } \{e_1, e_2\}, \\ 1 + \lambda & \text{computed with respect to the basis } \{f, e_2\}. \end{cases}$$

So  $\lambda = 1$  and  $t$  is the identity, which is a contradiction.

## 6.2 Orthogonality Relations for Irreducible Characters

**Hypothesis**  $G$  is a finite group, and all representations are finite dimensional over an algebraically closed field of characteristic 0 or characteristic coprime to  $|G|$ .

**Lemma 6.16** (“Properties of Trace”) Let  $V$  be a  $K$ -vector space of dimension  $n$ .

1. For  $\alpha \in \text{end}_K(V)$ ,  $\text{tr}(\alpha) = \sum_{i=1}^n a_{ii}$ . This is independent of the basis  $\mathcal{B}$ .  $\text{tr}(\alpha)$  is the sum of the eigenvalues of  $\alpha$ .  $-\text{tr}(\alpha)$  is the coefficient of  $\lambda^{n-1}$  in the characteristic polynomial  $\det(\lambda 1_V - \alpha)$  of  $\alpha$ .
2.  $\text{tr} : \text{end}_K(V) \rightarrow K$  is linear.
3.  $\text{tr}(\alpha\beta) = \text{tr}(\beta\alpha)$  for  $\alpha, \beta \in \text{end}(V)$ .
4. Given another  $K$ -vector space  $S$  and  $\alpha \in \text{end}_K(V)$  and  $\beta \in \text{end}_K(W)$ , define  $\alpha \oplus \beta \in \text{end}_K(V \oplus W)$  by  $(\alpha \oplus \beta)(V \oplus W) = \alpha(V) \oplus \beta(W)$ . Then  $\text{tr}(\alpha \oplus \beta) = \text{tr}(\alpha) + \text{tr}(\beta)$ .

**Definition 6.17** Let  $V$  be a  $KG$ -module corresponding to a representation  $\rho$ . Then the character of  $V$  (or of  $\rho$ ) is the map  $\chi_V : G \rightarrow K$  defined by  $\chi_V(g) = \text{tr}(\rho(g))$ .  $\chi_V$  is called an **irreducible character** if  $V$  is irreducible.

**Proposition 6.18**

1.  $\chi_V(1) = \dim V$ .
2.  $\chi_V(h^{-1}gh) = \chi_V(g) \forall g, h \in G$ .
3.  $\chi_{V \oplus W}(g) = \chi_V(g) + \chi_W(g)$  for any  $g \in G$  and any two  $KG$ -modules  $V$  and  $W$ .
4. For each  $g \in G$ ,  $\chi_V(g)$  is a sum of roots of unity, and if  $K \subseteq \mathbb{C}$ , then  $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ .
5. Equivalent representations have the same character.

**Proof**

1.  $\chi_V(1)$  is the trace of the identity map, which is equal to  $\dim V$ .
2.  $\chi_V(h^{-1}gh) = \chi_V((gh)h^{-1})$  (from 6.16(3))  $= \chi_V(g)$ .
3. This follows from 6.16(4).
4. Suppose that  $\rho(g)$  has eigenvalues  $\omega_1, \omega_2, \dots, \omega_n$ . Then  $\chi_V(g) = \sum_{i=1}^n \omega_i$ . Since  $G$  is finite,  $\rho(g)^m = 1_V$  for some  $m$ , and so  $\omega_1^m = \omega_2^m \dots = \omega_n^m = 1$ . Now  $\rho(g)^{-1}$  has eigenvalues  $\omega_1^{-1}, \omega_2^{-1}, \dots, \omega_n^{-1}$ , and  $\bar{\omega}_i = \omega_i^{-1}$ . So

$$\chi_V(g^{-1}) = \sum \omega_i^{-1} = \sum \bar{\omega}_i = \overline{\chi_V(g)}.$$

5. Suppose that  $\rho_1 : G \rightarrow GL(V_1)$  and  $\rho_2 : G \rightarrow GL(V_2)$  are two equivalent representations of  $G$ . By Proposition 6.7,  $\exists$  bases  $B_1$  and  $B_2$  of  $V_1$  and  $V_2$ , respectively, such that  $[\rho_1(g)]_{B_1} = [\rho_2(g)]_{B_2} \forall g \in G$ . Then

$$\chi_{V_1}(g) = \text{tr } \rho_1(g) = \text{tr}[\rho_1(g)]_{B_1} = \text{tr}[\rho_2(g)]_{B_2} = \chi_{V_2}(g).$$

**Definition 6.19**

1. A function  $\phi : G \rightarrow K$  is a **class function** if it is constant on conjugacy classes (i.e.  $\phi(hgh^{-1}) = \phi(g) \forall h, g \in G$ ), e.g.  $\chi_V$ .
2. If  $\phi, \psi : G \rightarrow K$  are two maps, their **inner product** is defined by

$$(\phi, \psi) = \frac{1}{|G|} \sum_{g \in G} \phi(g^{-1})\psi(g).$$

The set of maps  $G \rightarrow K$  is a  $K$ -vector space:

$$(\phi_1 + \phi_2)(g) = \phi_1(g) + \phi_2(g), \quad (\lambda\phi)(g) = \lambda\phi(g).$$

The dimension of this  $K$ -vector space is  $|G|$ ; a basis of functions is  $\phi_g$  ( $g \in G$ ), where  $\phi_g(h) = \delta_{gh}$ . The set of class functions is a subspace of dimension equal to the number of conjugacy classes of  $G$ .

The above inner product is symmetric, bilinear, and nonsingular on both of the above spaces. (Check this.)

**Proposition 6.20** (Orthogonality of Irreducible Characters)

1. If  $V$  and  $W$  are nonisomorphic, irreducible  $KG$ -modules, then  $(\chi_V, \chi_W) = 0$ .
2. If  $V$  is irreducible, then  $(\chi_V, \chi_V) = 1$ .

**Proof**

1. Choose bases  $B$  and  $C$  of  $V$  and  $W$ , respectively. Let the map  $v \mapsto g(v)$  in  $V$  have matrix  $(a_{ij}(g))$ . Let the map  $w \mapsto g(w)$  on  $W$  have matrix  $(b_{ij}(g))$ . Choose  $f : V \rightarrow W$  to have matrix (with respect to the bases  $B$  and  $C$ ) with entry 1 in position  $(r, s)$  and zeros elsewhere, i.e.  $\delta_{ir}\delta_{js}$ .

Recall (Corollary 6.15) that  $\hat{f} = \sum_{g \in G} g^{-1}fg$  is a  $KG$ -homomorphism. By Schur's Lemma,  $\hat{f}$  is the zero map. We have

$$(i, l)\text{-entry of } [\hat{f}] = \sum_{g \in G} (i, l)\text{-entry of } [g^{-1}fg]$$

$$= \sum_{g,j,k} a_i f(g^{-1}(\delta_{jr}\delta_{ks})b_{kl}(g)) = \sum_g a_{ir}(g^{-1})b_{sl}(g).$$

This is 0 for all  $r, s, i, l$ . Put  $i = r$  and  $l = s$ , and sum over all  $r$  and  $s$  to obtain  $0 = (\chi_V, \chi_W)$ .

- Now suppose that  $V = W$ . Schur's Lemma implies that  $\hat{f}$  is a scalar multiple  $\lambda$  of the identity. Hence, if  $n = \dim V$ , then

$$n\lambda = \text{tr } \hat{f} = \sum_{g \in G} \text{tr}(g^{-1}fg) = \sum_{g \in G} \text{tr}(f) = |G|\text{tr}(f) = |G|\delta_{rs}.$$

Take  $r = s = 1$ . This shows that  $n \neq 0$  in  $K$ . Thus  $\hat{f}$  is multiplication by  $|G|\delta_{rs}/n$ . So  $\forall i, l$ , we have

$$\frac{|G|\delta_{rs}}{n}\delta_{il} = (i, l)\text{-entry in } [\hat{f}] = \sum_{g \in G} a_{ir}(g^{-1})a_{sl}(g^{-1})$$

(as in part (1)). Put  $i = r$  and  $l = s$  and sum over  $r$  and  $s$ . Thus gives

$$(\chi_V, \chi_V) = \frac{1}{|G|} \sum_{g \in G} a_{rr}(g^{-1})a_{ss}(g) = \frac{1}{|G|} \sum_{g \in G} \delta_{rs}\delta_{rs} \frac{|G|}{n} = 1.$$

**Corollary 6.21** There are only finitely many inequivalent irreducible representations; the number is at most the number of conjugacy classes of  $G$ .

**Proof** Characters are elements of the space of class functions of dimension  $d$ , so it suffices to show that the characters of  $\chi^{(1)}, \chi^{(2)}, \dots, \chi^{(r)}$  of any  $r$  inequivalent representations are linearly independent. But if  $\sum \lambda_i x^{(i)} = 0$ , then  $\forall j$ , we have

$$0 = (0, \chi^{(j)}) = \left( \sum \lambda_i \chi^{(i)}, \chi^{(j)} \right) = \sum \lambda_i \delta_{ij} = \lambda_j.$$

**Proposition 6.22** Assume  $\text{char } K = 0$ . Let  $X_1, X_2, \dots, X_r$  be representatives of the isomorphism classes of irreducible  $KG$ -modules. Let  $V$  be an arbitrary  $KG$ -module, and define  $m_i = (\chi_{X_i}, \chi_V)$ .

- $m_i$  is the number of  $U_j$  isomorphic to  $X_i$  in any expression  $V = U_1 \oplus U_2 \oplus \dots \oplus U_j$  of  $V$  as a direct sum of irreducible modules. (Hence it is independent of the decomposition  $U_1 \oplus U_2 \oplus \dots \oplus U_j$ ).
- $V \simeq \bigoplus_{i=1}^r m_i X_i$ , where  $m_i X_i = \underbrace{X_i \oplus X_i \oplus \dots \oplus X_i}_m$ , so  $V$  is determined up to isomorphism by its character.
- So  $(\chi_V, \chi_V)$  is an integer  $\geq 0$ , and  $V$  is irreducible iff  $(\chi_V, \chi_V) = 1$ .

**Note**

- This reproves 6.13(2) and (3) in this case.

2. This plus 6.18(5) shows that two  $KG$ -modules are isomorphic (i.e. 2  $KG$ -modules are equivalent) iff they have the same character.

**Proof**

1. Suppose that  $V = U_1 \oplus U_2 \oplus \cdots \oplus U_j$ . Then

$$(\chi_V, \chi_{X_j}) = \left( \sum_j \chi_{U_j}, \chi_{X_j} \right) = \sum_j (\chi_{U_j}, \chi_{X_j}),$$

which is the number of  $U_j$ s isomorphic to  $X_j$ .

2. This follows immediately from (1).  
3.

$$(\chi_V, \chi_V) = \left( \chi_{\bigoplus_i m_i X_i}, \chi_{\bigoplus_j m_j X_j} \right) = \sum_{i,j} m_i m_j (\chi_{X_i}, \chi_{X_j}) = \sum_i m_i^2.$$

Now if  $V$  is irreducible, then  $(\chi_V, \chi_V) = 1$ . If  $(\chi_V, \chi_V) = 1$ , then  $m_{i_0} = 1$  for some  $i_0$ , and  $m_j = 0$  for some  $j \neq i_0$ . Hence  $V \simeq X_{i_0}$ .

## Chapter 7

# The Group Algebra and the Character Table

**Recall** Let  $K$  be any field and  $G$  any group. The group algebra  $KG$  is a  $K$ -vector space with basis given by the elements of  $G$ . Elements of  $KG$  are of the form  $\sum_g \lambda_g g$ , with  $\lambda_g \in K$  and only finitely many  $\lambda_g$ s nonzero. Identify  $\lambda \in K$  with  $\lambda 1 \in KG$ , where  $1$  is the identity in  $G$ .

**Definition 7.1** The **right regular representation** of  $G$  is the representation  $x \mapsto xg$  for  $x \in KG$ ,  $g \in G$ .  $G$  acts by right multiplication on  $KG$ . (The **left regular representation** is defined similarly.)

**Hypotheses for the rest of this chapter**  $G$  is a finite group,  $K$  is algebraically closed field of characteristic zero, and  $X_1, X_2, \dots, X_r$  are representatives of the isomorphism classes of irreducible  $KG$ -modules.

### Proposition 7.2

1.  $\chi_{KG}(1) = |G|$ , and  $\chi_{KG}(g) = 0$  for  $g \neq 1$ .
2. As  $KG$ -modules, we have  $KG \simeq \bigoplus_{i=1}^r n_i X_i$ , where  $n_i = \dim X_i$ , i.e. each irreducible representation occurs in  $KG$  a number of times equal to its degree.
3.  $|G| = \sum_{i=1}^r n_i^2$ , where  $n_i = \dim X_i$ .

### Proof

1.  $\chi_V(1) = \dim V$  for any  $KG$ -module  $V$ . Compute  $\chi_{KG}(g)$  with respect to the basis  $G$ . Each row of the matrix has one entry 1, and the rest are 0. If some diagonal entry is nonzero, then  $hg = h$  for some  $h \in G$ , so  $g = 1$ .

2. We have  $KG \simeq \bigoplus_{i=1}^r m_i X_i$ , and by Proposition 6.22,

$$m_i = (\chi_{KG}, \chi_{X_i}) = \frac{1}{|G|} \sum_{g \in G} \chi_{KG}(g^{-1} \chi_{X_i}(g)) = \frac{|G|}{|G|} \chi_{X_i}(1) = \dim X_i.$$

3.

$$|G| = \dim KG = \dim \left( \bigoplus_{i=1}^r n_i X_i \right) = \sum_{i=1}^r n_i \dim X_i = \sum_{i=1}^r n_i^2.$$

**Corollary 7.3** The following are equivalent:

1.  $G$  is abelian.
2.  $G$  has  $|G|$  inequivalent irreducible representations.
3. Each irreducible  $KG$ -module has dimension 1.

**Proof** (1) implies (3) by Corollary 6.10 (Corollary to Schur's Lemma). (3) implies (2) by Proposition 7.2(3). To show that (2) implies (1), we note that if  $G$  has  $|G|$  inequivalent irreducible representations, then  $G$  has  $|G|$  conjugacy classes, and so  $G$  is abelian.

**Lemma 7.4** Let  $\psi$  be a class function such that  $(\psi, \chi_{X_i}) = 0$  for  $1 \leq i \leq r$ . Then  $\psi = 0$ .

**Proof** Let  $x = \sum_{g \in G} \psi(g^{-1})g \in KG$ . We claim that, since  $\psi$  is a class function,  $x$  commutes with all elements of  $G$ .

$$h^{-1}xh = \sum_{g \in G} \psi(g^{-1})h^{-1}gh = \sum_{g \in G} \psi((h^{-1}gh)^{-1})h^{-1}gh = \sum_{g \in G} \psi(g^{-1})g = x.$$

This implies that if  $V$  is any  $KG$ -module, the map  $\theta_x : V \rightarrow V$  given by  $x \mapsto vx$  is a  $KG$ -homomorphism.  $(h\theta_x)(v) = hxv = xhv = \theta_x(hv)$ . Take  $v = x_i$ . Then Schur's Lemma implies that  $\theta_x = \lambda x$  (identity) for some  $\lambda \in K$ . Hence  $n_i \lambda = \text{tr}(\theta_x \text{ as an endomorphism of } X_i)$ , which is equal to  $\sum_{g \in G} \psi(g^{-1})\text{tr}(g \text{ as an endomorphism of } x_i)$ , which is equal to

$$\sum_{g \in G} \psi(g^{-1})\lambda x_i(G) = |G|(\psi, \chi_{X_i}) = 0.$$

So  $x$  acts as the zero map on  $X_i$  and hence acts as zero on  $\bigoplus_{i=1}^r n_i X_i \simeq KG$ . Hence

$$0\theta_x(1) = x1 = x = \sum_{g \in G} \psi(g^{-1})g.$$

So  $\psi(g) = 0 \forall g$ , i.e.  $\psi = 0$ .

**Theorem 7.5** Let  $\chi^{(1)}, \chi^{(2)}, \dots, \chi^{(r)}$  be the irreducible characters of  $G$ .

1.  $\phi = \sum_{i=1}^r (\phi, \chi^{(i)}) \chi^{(i)}$  for each class function  $\phi$ .
2.  $\chi^{(1)}, \chi^{(2)}, \dots, \chi^{(r)}$  is a basis for the space of class functions. So the number of irreducible characters is equal to the number of conjugacy classes of  $G$ .

**Proof**

1. Given  $\phi$ , set  $\psi = \phi - \sum_{i=1}^r (\phi, \chi^{(i)}) \chi^{(i)}$ . Then  $(\psi, \chi^{(i)}) = 0 \forall i$ , and so  $\psi = 0$  by Lemma 7.4
2. Part (1) implies that  $\chi^{(1)}, \chi^{(2)}, \dots, \chi^{(r)}$  spans the space of class functions. The proof of Corollary 6.21 implies that they are linearly independent.

**Notation**  $\chi^{(1)}$  is the character of the trivial representation (each element of  $G$  acts as the identity on a 1-dimensional vector space).  $\chi^{(1)}, \chi^{(2)}, \dots, \chi^{(d)}$  are the irreducible characters.  $g_1 = 2, g_2, \dots, g_d$  are representatives of conjugacy classes  $C_1, C_2, \dots, C_d$ .  $S_j$  is the order of the centralizer of  $g_j$  in  $G$ . So  $|C_j| = |G|/S_j$ .

**Definition 7.6** The **character table** of  $G$  is the  $d \times d$  matrix with entry  $\chi^{(1)}(g_j)$  in place  $(i, j)$ . All entries in the 1<sup>st</sup> row are 1. Entries in the 1<sup>st</sup> column are degrees of irreducible characters: integers  $\neq 0$  whose square have sum  $|G|$ .

**Theorem 7.7** Suppose that  $K \subseteq \mathbb{C}$ .

1. Define

$$u_{ij} = \frac{1}{\sqrt{S_i S_j}} \chi^{(1)}(g_j)$$

for  $i, j \leq d$ . The matrix  $U = (u_{ij})$  is unitary (i.e.  $U\bar{U}^t = I$ ).

2. (Orthogonality Relations for Columns)

$$\sum_{k=1}^d \overline{\chi^{(k)}(g_i)} \chi^{(k)}(g_j) = \begin{cases} s_i & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

**Proof**

1. From orthogonality relations for characters (Proposition 6.20), we have

$$\begin{aligned} \delta_{ij} &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi^{(i)}(g)} \chi^{(j)}(g) \\ &= \frac{1}{|G|} \sum_{k=1}^d \frac{|G|}{S_k} \overline{\chi^{(i)}(g_k)} \chi^{(j)}(g_k) \\ &= \sum_{k=1}^d \bar{u}_{ik}, \end{aligned}$$

which is the  $(j, i)$ <sup>th</sup> entry in  $U\bar{U}^t$ . So  $U\bar{U}^t = I$ .

2. Since  $U\bar{U}^t = I$ ,  $U^{-1} = \bar{U}^t$ , and so  $\bar{U}^t U = I$ . So for all  $i$  and  $j$ ,

$$\delta_{ij} = \sum_{k=1}^d \bar{U}_{ki} U_{kj} = \frac{1}{\sqrt{S_i S_j}} \sum_{k=1}^d \overline{\chi^{(k)}(g_i)} \chi^{(k)}(g_j).$$

### Comments

1. Orthogonality Relations for Rows:

$$|G| \delta_{ij} = \sum_{k=1}^d \frac{|G|}{S_k} \chi^{(i)}(g_k) \chi^j(g_k).$$

(In practice, orthogonality relations for columns are often more useful.)

2. Also useful: The degrees  $\chi^{(i)}(1)$  of irreducible characters divide  $|G|$ . (Proof later.)

**Example**  $G = S_4$ . Conjugacy classes have representatives  $g_1 = 1$ ,  $g_2 = (12)$ ,  $g_3 = (123)$ ,  $g_4 = (12)(34)$ , and  $g_5 = (1234)$ .  $\chi^{(1)}$  is the trivial character, and  $\chi^{(2)}$  is the alternating character.

**Exercise** Show that if  $\chi$  is an irreducible character, then so is  $\chi^{(3)}\chi$ .

Now observe that  $\chi^{(2)}\chi = \chi$  iff  $\chi(g_2) = \chi(g_5) = 0$ . But  $\chi^{(1)} + \chi^{(2)}, \chi^{(3)}, \chi^{(4)}, \chi^{(5)}$  are linearly independent. Hence these cannot all vanish on  $g_2$  and  $g_5$  (otherwise e.g. the class function defined by  $\phi(g_2) = 1, \phi(\text{rest}) = 0$  would not lie in the span of  $\{\chi^{(1)} + \chi^{(2)}, \chi^{(2)}, \chi^{(3)}, \chi^{(4)}, \chi^{(5)}\}$ , which is a contradiction).

Suppose that  $\chi^{(2)}\chi^{(3)} \neq \chi^{(3)}$ . Then we can take  $\chi^{(4)} = \chi^{(2)}\chi^{(3)}$ . Then the set of irreducible characters of  $G$  is given by

$$\underbrace{\{\chi^{(1)}, \chi^{(2)}, \chi^{(3)}, \chi^{(2)}\chi^{(3)}, \chi^{(5)}\}}_{\substack{\text{multiplication by } \chi^{(2)} \\ \text{permutes these}}}$$

We must have  $\chi^{(2)}\chi^{(5)} = \chi^{(5)}$ . So  $\chi^{(5)}(g_2) = \chi^{(5)}(g_5) = 0$ . Each element of  $G$  is conjugate to its inverse. Hence  $\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$ . So the character table is real.

If  $d_3 := \chi^{(3)}(1)$  and  $d_5 := \chi^{(5)}(1)$ , then  $1 + 1 + d_3^2 + d_3^2 + d_5^2 = |G| = 24$ , i.e.  $2d_3^2 + d_5^2 = 22$ . The only solution is  $d_3 = 3$  and  $d_5 = 2$ .

Let  $C(i, j)$  denote “orthogonality relations applied to columns  $(i, j)$ .”  $C(2, 2)$  gives us that entries in the 2<sup>nd</sup> column are  $\pm x$ , real, and satisfy  $2|x|^2 = 2$ , and so  $x = \pm 1$ .  $C(5, 5)$  gives us that entries

in the 5<sup>th</sup> column are  $\pm 1$ . Then  $C(2, 5)$  gives the signs.  $C(3, 1)$  and  $C(3, 3)$  give us entries in the 3<sup>th</sup> column. (We know that 0s have to be the same.)  $C(3, 4)$  and  $C(1, 4)$  give us entries in the 4<sup>th</sup> column. (Again we know that the the 0s have to be the same.)

	1	$g_2$	$g_3$	$g_4$	$g_5$
$ C_i $	1	6	8	3	6
$S_i$	24	4	3	8	4
$\chi^{(1)}$	1	1	1	1	1
$\chi^{(2)}$	1	-1	1	1	-1
$\chi^{(3)}$	3	1	0	-1	-1
$\chi^{(4)}$	3	-1	0	-1	1
$\chi^{(5)}$	2	0	-1	2	0

**Remark** We have not used the “obvious” representation, a vector space  $V$  with basis the four points permuted by  $S_4$ . Then  $\chi_V(g)$  would be the number of points fixed by  $g$ .

	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$
$\chi_V$	4	2	1	0	0

Then  $(\chi_V, \chi_V) = \frac{1}{24}(1 \cdot 16 + 6 \cdot 4 + 8 \cdot 1) = 2$ . Thus  $\chi_V$  is a sum of two irreducible characters. Now  $(\chi_V, \chi^{(1)}) = 1$ , so  $\chi_V - \chi^{(1)}$  is irreducible.

**Objective** We want to characterize  $KG$  as a ring and deduce another proof that the number of irreducible characters is equal to the number of conjugacy classes.

### Proposition 7.8

1. If  $V$  is any  $KG$ -module, then the map  $\hat{\rho} : KG \rightarrow \text{end}_K(V)$  defined by  $\hat{\rho}(x)v = xv$  for  $v \in V$  and  $x \in KG$  is a ring and vector space homomorphism. (This follows from the (ring theoretic) definition of a  $KG$ -module.)
2. Let  $X_1, X_2, \dots, X_r$  be representatives of the equivalence classes of irreducible representations of  $G$ , and let  $\hat{\rho}_1, \hat{\rho}_2, \dots, \hat{\rho}_r$  be the corresponding maps  $KG \rightarrow \text{end}_K(X_i)$ . Then the map

$$\sigma : KG \rightarrow \bigoplus_{i=1}^r \text{end}_K(X_i)$$

defined by  $\sigma(x) = (\hat{\rho}_1(x), \hat{\rho}_2(x), \dots, \hat{\rho}_r(x))$  is a ring and vector space isomorphism.

### Proof

2.  $\sigma$  is a ring and vector space homomorphism by (1). If  $\sigma(x) = 0$ , then  $\hat{\rho}_i(x) = 0 \forall i$ , so  $x$  acts as zero on each  $X_i$ , hence on any direct sum of modules isomorphic to  $X_i$ , hence on any

$KG$ -module  $V$ . Take  $V = KG$ . Then  $0 = x \cdot 1 = x$ , so  $\sigma$  is injective. Now we compute dimensions:  $\dim KG = |G|$ , and

$$\dim \left( \bigoplus_{i=1}^r \text{end}_K X_i \right) = \sum_{i=1}^r \dim(\text{end}_K X_i) = \sum_{i=1}^r \dim(X_i)^2 = |G|.$$

(See Proposition 7.2(3).)

**Definition 7.9** The **center**  $Z(R)$  of a ring  $R$  is  $\{z : xz = zx \forall x \in R\}$ . It is a subring of  $R$ .

**Proposition 7.10**

1.  $Z(M_n(K)) = \{\lambda 1 : \lambda \in K\}$ .
2. If  $R \simeq S$ , then  $Z(R) \simeq Z(S)$ . So if  $\dim V = n$ , then  $\dim(Z(\text{end}_K V)) = \dim(Z(M_n(K))) = 1$ .
3.  $Z(R_1 \oplus R_2 \oplus \cdots \oplus R_r) = Z(R_1) \oplus Z(R_2) \oplus \cdots \oplus Z(R_r)$ .

4.

$$\dim(Z(KG)) = \dim Z \left( \bigoplus_{i=1}^r \text{end}_K X_i \right) = \dim \left( \bigoplus_{i=1}^r Z(\text{end}_K X_i) \right) = r.$$

5. Let  $C_1 = \{1\}, C_2, \dots, C_d$  be the conjugacy classes of  $G$ . Set  $c_i = \sum_{g \in C_i} g$ . Let  $W$  be the space spanned by  $c_1, c_2, \dots, c_d$ . Then  $Z(KG) = W$ .
6. The number of conjugacy classes is equal to the number of irreducible characters. Thus  $c_1, c_2, \dots, c_d$  are linearly independent, so  $\dim Z(KG) = d$ . Now compare with part (4).

**Proof**

5. Plainly, each  $c_i \in Z(KG)$  since  $gc_i g^{-1} = c_i \forall g \in G$ . So  $W \subseteq Z(KG)$ . Now  $\sum \lambda_g g \in Z(KG)$ , and so

$$\sum \lambda_g g = h^{-1} \left( \sum \lambda_g g \right) h = \sum \lambda_g h^{-1} g h$$

for each  $h \in G$ . So the function  $g \mapsto \lambda_g$  is a class function. Hence

$$\sum \lambda_g g = \sum_{i=1}^d \lambda_i c_i \in W.$$

## Chapter 8

# Tensor Products, Symmetrics and Exterior Squares as $KG$ -Modules

### 8.1 Review of Tensor Products

The tensor product of  $K$ -vector spaces  $U$  and  $V$  is a  $K$ -vector space  $U \otimes V$ , together with a bilinear map  $\otimes : U \times V \rightarrow U \otimes V$  with the following universal property: For each bilinear map  $g : U \times V \rightarrow W$ ,  $\exists!$  linear map  $\tilde{g} : U \otimes V \rightarrow W$  such that the following diagram commutes:

$$\begin{array}{ccc} U \times V & \xrightarrow{g} & W \\ \downarrow \otimes & \nearrow \tilde{g} & \\ U \otimes V & & \end{array}$$

The tensor product exists as is unique up to isomorphism.

If  $U$  and  $V$  are finite dimensional with bases  $\{e_1, e_2, \dots, e_m\}$  and  $\{f_1, f_2, \dots, f_n\}$ , respectively, then  $U \otimes V$  has basis  $\{e_i \otimes f_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ .  $\dim(U \otimes V) = (\dim U)(\dim V)$ .

Given linear maps  $f : U_1 \rightarrow U_2$  and  $g : V_1 \rightarrow V_2$ , then  $\exists!$  linear map  $f \otimes g : U_1 \otimes V_1 \rightarrow U_2 \otimes V_2$  such that  $(f \otimes g)(u \otimes v) = f(u) \otimes g(v) \forall u, U_1, v \in V_1$ .

#### Lemma 8.1

1.  $1_U \otimes 1_V = 1_{U \otimes V}$ .
2. Given  $f_1 : U_1 \rightarrow U_2$ ,  $f_2 : U_2 \rightarrow U_3$ ,  $g_1 : V_1 \rightarrow V_2$ , and  $g_2 : V_2 \rightarrow V_3$ , we have  $(f_1 \otimes g_1)(f_2 \otimes g_2) = (f_1 f_2) \otimes (g_1, g_2)$ .
3. Given  $\alpha : U \rightarrow U$  and  $\beta : V \rightarrow V$ , we have  $\text{tr}(\alpha \otimes \beta) = \text{tr}(\alpha)\text{tr}(\beta)$ .

**Proof**

1, 2. Show that the maps agree on the spanning set  $\{u \otimes v \mid u \in U, v \in V\}$ .

3. Choose bases  $\{e_1, e_2, \dots, e_m\}$  and  $\{f_1, f_2, \dots, f_n\}$  on  $U$  and  $V$ , respectively. Let  $\alpha(e_i) = \sum a_{ik} e_k$  and  $\beta(f_j) = \sum b_{jl} f_l \forall i, j$ . Then

$$(\alpha \otimes \beta)(e_i \otimes f_j) = \alpha(e_i) \otimes \beta(f_j) = \sum_{k,l} a_{ik} b_{jl} e_k \otimes f_l.$$

Thus  $\alpha \otimes \beta$  has matrix with rows and columns indexed by  $\{(i, j) : 1 \leq i \leq m, 1 \leq j \leq n\}$ . The entry at the intersection of row  $(i, j)$  and column  $(k, l)$  is  $a_{ik} b_{jl}$ . Thus

$$\text{tr}(\alpha \otimes \beta) = \sum_{i,j} a_{ii} b_{jj} = \text{tr}(\alpha) \text{tr}(\beta).$$

**Proposition 8.2** If  $U$  and  $V$  are finite dimensional  $KG$ -modules, then  $U \otimes V$  becomes a  $KG$ -module with action defined by  $g(u \otimes v) = g(u) \otimes g(v)$ ,  $u \in U$ ,  $v \in V$ ,  $g \in G$ . We have that  $\chi_{U \otimes V}(g) = \chi_U(g) \chi_V(g)$ , so the product of the characters is a character.

**Proof** Let  $\rho$  and  $\sigma$  be the representations of  $G$  on  $U$  and  $V$ , respectively. For each  $g \in G$ , consider the maps  $\rho(g) \otimes \sigma(g)$ . We have

$$[\rho(g_1) \otimes \sigma(g_1)][\rho(g_2) \otimes \sigma(g_2)] = (\rho(g_1)\rho(g_2)) \otimes (\sigma(g_1)\sigma(g_2)) = \rho(g_1 g_2) \otimes \sigma(g_1 g_2)$$

and  $\rho(1) \otimes \sigma(1) = 1_{U \otimes V}$ . Hence the map  $g \mapsto \rho(g) \otimes \sigma(g)$  is a representation, and  $U \otimes V$  is a  $KG$ -module. We have

$$\chi_{U \otimes V}(g) = \text{tr}(\rho(g) \otimes \sigma(g)) = \text{tr}(\rho(g)) \text{tr}(\sigma(g)) = \chi_U(g) \chi_V(g).$$

**Lemma 8.3** Let  $U$ ,  $V$ , and  $W$  be  $KG$ -modules, and regard  $K$  as a  $KG$ -module with  $G$  acting trivially. Then each of the following natural isomorphisms of a  $K$ -vector space is a  $KG$ -isomorphism:

1. The map  $\theta : K \otimes U \rightarrow U$ ,  $\lambda \otimes u \mapsto \lambda u$ .
2.  $\phi : U \otimes V \rightarrow V \otimes U$ ,  $u \otimes v \mapsto v \otimes u$ .
3.  $(U \otimes V) \otimes W \rightarrow U \otimes (V \otimes W)$ ,  $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$ .

**Proof** Check that everything works on a spanning set.

## 8.2 Symmetric and Exterior Squares

Let  $V$  be a finite dimensional  $K$ -vector space with  $\text{char}(K) \neq 2$ . Let  $\tau$  be the action on  $V \otimes V$  determined by  $u \otimes v \mapsto v \otimes u$ . So  $\tau^2 = 1$ , and  $V \otimes V$  is a  $K\langle\tau\rangle$ -module.

**Definition 8.4** Call  $t \in V \otimes V$  **symmetric** if  $\tau(t) = t$  and **antisymmetric** if  $\tau(t) = -t$ . Each  $t \in V \otimes V$  is uniquely the sum of its symmetric and antisymmetric parts:

$$t = \frac{1}{2}(t + \tau(t)) + \frac{1}{2}(t - \tau(t)).$$

So we have

$$V \otimes V = S^2(V) \oplus \lambda^2(V),$$

where  $S^2(V)$  consists of all symmetric elements and  $\lambda^2(V)$  consists of all antisymmetric elements.

**Definition 8.5**  $S^2(V)$  is the **symmetric square** of  $V$ ;  $\lambda^2(V)$  is the **exterior square** of  $V$ .

If  $\{e_1, e_2, \dots, e_n\}$  is a basis of  $V$ , then  $\{e_i \otimes e_j + e_j \otimes e_i \mid i \leq j\}$  and  $\{e_i \otimes e_j - e_j \otimes e_i \mid i < j\}$  are subsets of  $S^2(V)$  and  $\lambda^2(V)$ , respectively. Together they have  $n^2$  elements and span  $V \otimes V$ , so they are bases of  $S^2(V)$  and  $\lambda^2(V)$ , respectively. If  $V$  is a  $KG$ -module, then  $S^2(V)$  and  $\lambda^2(V)$  are  $KG$ -submodules of  $V \otimes V$ . (Check this.)

**Proposition 8.6** The characters of  $G$  on the  $KG$ -module  $S^2(V)$  and  $\lambda^2(V)$  are given by

1.  $\chi_{S^2(V)}(g) + \chi_{\lambda^2(V)}(g) = \chi_V(g)^2$ ,
2.  $\chi_{S^2(V)}(g) - \chi_{\lambda^2(V)}(g) = \chi_V(g^2)$ .

**Proof**

2. Suppose that  $\{e_1, e_2, \dots, e_n\}$  is a basis of  $V$ .  $g(e_i) = \sum a_{ik}e_k$ , say. Put  $t_{ij} = e_i \otimes e_j$ . Then  $g(t_{ij}) = \sum_{k,l} a_{ik}a_{jl}t_{kl}$ . So

$$g(t_{ij} + t_{ji}) = \sum_{k,l} a_{ik}a_{jl}(t_{kl} + t_{lk}) \tag{†}$$

for  $i \leq j$ . If  $i < j$ , then the coefficient of  $t_{ij} + t_{ji}$  on the RHS of (†) is  $a_{ii}a_{jj} + a_{ij}a_{ji}$ . Compute  $\chi_{S^2(V)}(g)$  with respect to the above basis:

$$\chi_{S^2(V)}(g) = \sum_{i < j} a_{ii}a_{jj} + \sum_{i < j} a_{ij}a_{ji} + \sum_i a_{ii}a_{ii}.$$

Similarly,

$$\chi_{\lambda^2(V)}(g) = \sum_{i < j} a_{ii}a_{jj} - \sum_{i < j} a_{ij}a_{ji},$$

for if  $i < j$ , the coefficient of  $t_{ij} - t_{ji}$  on the RHS of (†) is  $a_{ii}a_{jj} - a_{ij}a_{ji}$ . Subtracting gives

$$\chi_{S^2(V)}(g) - \chi_{\lambda^2(V)}(g) = 2 \sum_{i < j} a_{ij}a_{ji} + \sum_i a_{ii}a_{ii} \sum_{i,j} a_{ij}a_{ji} = \text{tr}((a_{ij})^2) = \chi_V(g^2).$$

Alternatively, if  $G$  is finite and  $K$  algebraically closed with  $\text{char } K = 0$  or coprime to  $|G|$ , there is a much simpler proof. If  $g \in G$  has order  $r$ , then the minimum polynomial of  $G$  on  $V$  divides  $x^r - 1$  and so has distinct roots. Hence  $\exists$  a basis  $\{e_1, e_2, \dots, e_n\}$  of eigenvectors, say  $g(e_i) = \lambda_i e_i \forall i$ . Then  $g(e_i \otimes e_j) = \lambda_i \lambda_j (e_i \otimes e_j)$ , so computing  $\chi_{S^2(V)}(g)$  with respect to the obvious basis gives  $\chi_{S^2(V)}(g) = \sum_{i \leq j} \lambda_i \lambda_j$ . Similarly,  $\chi_{\lambda^2(V)}(g) = \sum_{i < j} \lambda_i \lambda_j$ . So

$$\chi_{S^2(V)}(g) - \chi_{\lambda^2(V)}(g) = \sum_i \lambda_i^2 = \chi_V(g^2).$$

## Chapter 9

# Induced Representations

Hypotheses for Chapter 9:  $H$  is a subgroup of  $G$  of finite index  $m$ ; all representations are finite dimensional.

If  $V$  is a  $KG$ -module (corresponding to a representation  $\rho : G \rightarrow GL(V)$ ), then  $V$  is a  $KH$ -module (and the corresponding representation is the restriction  $\rho|_H$  of  $\rho$  to  $H$ ).

**Problem** Given a representation of  $H$ , find a representation of  $G$ .

**Definition 9.1** A  $KG$ -module  $V$  is **induced** from a  $KH$ -module  $W$  if

1.  $W$  is a  $KH$ -submodule of  $V$  when  $V$  is regarded as a  $KH$ -module.
2. There is a transversal  $T = \{t_1, t_2, \dots, t_m\}$  of  $H$  in  $G$  such that

$$V = \bigoplus_{i=1}^m t_i W \quad (t_i W = \{t_i(w) \mid w \in W\}).$$

**Example** Suppose that  $G$  is any finite group and  $H$  is the trivial group acting on  $W = K$ . Then the group algebra  $KG$  as a  $KG$ -module is induced from  $W$ .

**Proposition 9.2**

1. The above definition is independent of the transversal. If  $V$  is induced from  $W$ , then (2) holds for *every* transversal of  $H$  in  $G$ .
2. If  $V$  is induced from  $W$ , then the structure of  $V$  as a  $KG$ -module is entirely determined by that of  $W$  as a  $KH$ -module.

**Proof**

1. If  $T' = \{t'_1, t'_2, \dots, t'_m\}$  is another transversal numbered such that  $t_i H = t'_i H$  (i.e. numbered in the same order), then  $\exists h \in H$  such that  $t'_i = t_i h$  and  $t'_i W = t_i h W = t_i W$  (since  $W$  is a  $KH$ -module). So  $V = \bigoplus_i t'_i W = \bigoplus_i t_i W$ .
2. Let  $\rho : G \rightarrow GL(V)$  and  $\sigma : H \rightarrow GL(W)$  be the corresponding representations. We must show that the  $\sigma(h)$  ( $h \in H$ ) determine  $\rho(g)$  ( $g \in G$ ), or, as the  $t_i W$  span  $V$ , determine the maps  $\rho(g)|_{t_i W} : t_i W \rightarrow V$ . Now given  $g \in G$  and  $t_i W$ , then  $\exists t_j \in T, h \in H$  such that  $gt_i = t_j h$ . We have  $\rho(g)(t_i w) = t_j h(w) = t_j(\sigma(h)w)$ .

**Proposition 9.3** Given a  $KH$ -module  $W$ ,  $\exists$  a  $KG$ -module  $V$  induced from  $W$ . The module  $V$  is uniquely determined up to isomorphism of  $KG$ -module (by Proposition 9.2(2)) and is denoted  $\text{ind}_H^G W$ .

**Proof** Let  $t_1 = 1, t_2, \dots, t_m$  be a transversal of  $H$  in  $G$ . Let  $W_1 = W, W_2, \dots, W_m$  be a  $K$ -vector space with  $W_i \simeq W \forall i$ . Let  $\theta_i : W \xrightarrow{\sim} W_i$  be an isomorphism  $\forall i$  and  $\theta_1$  be the identity map. Set  $V = \bigoplus_{i=1}^m W_i$ . Define  $\rho(g) : V \rightarrow V$  by specifying the action on each  $W_i$ . Given  $g$  and  $t_i$ , let  $gt_i = t_j h$  ( $h \in H$ ). So  $g = t_j h t_i^{-1}$ ; then for  $w_i \in W_i$ , define  $\rho(g)w_i = \theta_j h \theta_i^{-1}(w_i)$ .

1.  $V$  becomes a  $KG$ -module. Firstly, the maps  $\rho(g)$  are linear and well-defined, as  $V = \bigoplus W_i$ . Because  $1 \cdot t_i = t_i \cdot 1$ , we have  $\rho(1)w_i = \theta_i 1 \theta_i^{-1}(w_i) = w_i$ . So  $\rho(1) = 1_V$ . Given  $g_1, g_2 \in G$  and  $t_i$ , define  $h_1, h_2, t_j$ , and  $t_k$  by  $g_1 t_i = t_j h$  and  $g_2 t_j = t_k h_2$ . Then

$$\rho(g_2)\rho(g_1)w_i = \theta_k h_2 \theta_j^{-1} \theta_j h_1 \theta_i^{-1}(w_i) = \theta_k (h_2 h_1) \theta_i^{-1}(w_i) = \rho(g_1 g_2)w_i$$

since  $g_1 g_2 t_i = g_2 t_j h_1 = t_k h_2 h_1$ .

2.  $W$  is a  $KH$ -submodule. If  $w \in W$  and  $h \in H$ , then  $h1 = 1h$ . So  $\rho(h)w = \theta_1 h \theta_1^{-1}(w) = h(w)$ .
3. Take  $g = t_i$  and  $w \in W$ . Then  $t_i(w) = \theta_i 1 \theta_i^{-1}(w) = \theta_i(w)$ . So  $t_i W = W_i$  and  $V \simeq \bigoplus_{i=1}^m t_i W$ .

**Proposition 9.4** (“Induction is Transitive”) Suppose that  $H \leq L \leq G$  and that  $W$  is a  $KH$ -module. Then  $\text{ind}_L^G \text{ind}_H^L W \simeq \text{ind}_H^G W$  (as  $KG$ -modules).

**Proof** If  $R$  is a transversal of  $H$  in  $L$  and  $S$  a transversal of  $L$  in  $G$ , then  $RS = \{rs : r \in R, s \in S\}$  is a transversal of  $H$  in  $G$ . The result now follows from Proposition 9.2.

**Note** If  $V = \text{ind}_H^G W = \bigoplus t_i W$ , then each  $gt_i W = t_i W$  iff  $t_i^{-1}gt_i \in H$  since if  $gt_i = t_j h$  ( $h \in H$ ), then  $gt_i W = t_j h W = t_j W$ .

Hypotheses for the rest of the chapter:  $G$  is finite and  $K$  is algebraically closed of characteristic zero.

How can we compute induced characters?

**Proposition 9.5** Let  $V = \text{ind}_H^G W$  and  $g \in G$ , and suppose that  $T$  is a transversal of  $H$  in  $G$ . Then

$$\chi_V(g) = \sum_{\substack{t \in T \\ t^{-1}gt \in H}} \chi_W(t^{-1}gt) = \frac{1}{|H|} \sum_{\substack{s \in G \\ s^{-1}gs \in H}} \chi_W(s^{-1}gs).$$

**Proof** Denote the corresponding representations by  $\sigma : H \rightarrow GL(W)$  and  $\rho : G \rightarrow GL(V)$ . Our strategy is to compute the trace of  $\rho(g)$  with respect to a union of the bases of  $tW$  ( $t \in T$ ). If  $g(tW) \neq tW$ , then we get zero entries on the diagonal for basis vectors in  $tW$ . So

$$\chi_V(g) = \sum_{\substack{t \in T \\ g(tW) = tW}} \text{tr}(\rho(g) |_{tW}) = \sum_{\substack{t \in T \\ t^{-1}gt \in H}} \text{tr}(\rho(g) |_{tW}).$$

If  $e_1, e_2, \dots, e_r$  is a basis of  $W$ , then  $te_1, te_2, \dots, te_r$  is a basis of  $tW$ . If  $g(te_i) = \sum_j a_{ij}te_j \forall i$ , then  $t^{-1}gt(e_i) = \sum_j a_{ij}e_j \forall i$ . So

$$\text{tr}(\rho(g) |_{tW}) = \sum a_{ii} = \text{tr}(\sigma(t^{-1}gt)).$$

Hence

$$\chi_V(g) = \sum_{\substack{t \in T \\ t^{-1}gt \in H}} \chi_W(t^{-1}gt).$$

Now write this another way: suppose that  $g' \in G$  with  $g' = t'h$  ( $t' \in T, h \in H$ ) say. Then  $g'^{-1}gg' \in H$  iff  $h^{-1}t'^{-1}gt'h \in H$  iff  $t'^{-1}gt' \in H$ . In this case,  $g'^{-1}gg'$  and  $t'^{-1}gt'$  are conjugate in  $H$ , and so  $\chi_W(g'^{-1}gg') = \chi_W(t'^{-1}gt')$ . Hence

$$\chi_V(g) = \frac{1}{|H|} \sum_{\substack{s \in G \\ s^{-1}gs \in H}} \chi_W(s^{-1}gs).$$

**Definition 9.6** Let  $H \leq G$ . If  $\phi$  is a class function on  $H$ , define

$$(\text{ind}_H^G \phi)(g) = \frac{1}{|H|} \sum_{\substack{s \in G \\ s^{-1}gs \in H}} \phi(s^{-1}gs).$$

This is a class function on  $G$ . (Check this.) (“It comes from a sum over all conjugates lying on  $H$ .”)

If  $\psi$  is a class function on  $G$ , define  $\text{res}_H \psi$  to be the restriction of  $\psi$  to  $H$ . This is a class function on  $H$ .

**Theorem 9.7** (Frobenius Reciprocity Theorem) If  $\phi$  is a class function on  $H$  and  $\psi$  is a class function on  $G$ , then

$$(\text{ind}_H^G \phi, \psi)_G = (\phi, \text{res}_H \psi)_H,$$

where  $(\cdot, \cdot)_X$  means inner product of class functions for the group  $X$ .

**Proof**

$$\begin{aligned}
(\text{ind}_H^G \phi, \psi)_G &= \frac{1}{|G|} \frac{1}{|H|} \sum_{g \in G} \sum_{s \in G} \phi(s^{-1}g^{-1}s) \psi(g) \\
&= \frac{1}{|G|} \frac{1}{|H|} \sum_{s \in G} \sum_{\substack{g \in G \\ s^{-1}gs \in H}} \phi(s^{-1}g^{-1}s) \psi(g) \\
&= \frac{1}{|G|} \frac{1}{|H|} \sum_{s \in G} \left( \sum_{h \in H} \phi(h^{-1}) \psi(shs^{-1}) \right) \text{ (setting } s^{-1}g^{-1}s = h^{-1}) \\
&= \frac{1}{|G|} \frac{1}{|H|} \sum_{s \in G} \sum_{h \in H} \phi(h^{-1}) \psi(h) \\
&= (\phi, \text{res}_H \psi)_H.
\end{aligned}$$

**Corollary 9.8** If  $\chi$  is an irreducible character of  $G$  and  $\psi$  is an irreducible character of  $H$ , then the multiplicity of  $\chi$  in  $\text{ind}_H^G \psi$  is equal to the multiplicity of  $\psi$  in  $\text{res}_H \chi$ .

**Proof** By Proposition 6.22, these are  $(\chi, \text{ind}_H^G \psi)_G$  and  $(\text{res}_H \chi, \psi)_H$ , respectively.

## 9.1 Permutation Representations

Let  $\Pi$  be a permutation representation of  $G$  on  $X = \{x_1, x_2, \dots, x_m\}$ . Let  $V$  be a  $K$ -vector space with basis in one-to-one correspondence with  $X$ , and write  $\Pi$  for the associated linear representation. Set  $H = \{g \in G : gx_1 = x_1\}$  — the stabilizer of  $x_1$  in  $G$ . Suppose that  $\Pi$  is a *transitive* representation (i.e.  $\forall i, j \exists g \in G$  with  $g(x_i) = x_j$ ). For each  $i$ , choose  $t_i \in G$  with  $x_i = t_i x_1$ . We claim that  $\{t_i : 1 \leq i \leq m\}$  is a transversal of  $H$  in  $G$ . If  $g \in G$ , then  $x_i = gx_1$  iff  $t_i x_1 = g_1$  iff  $t_1^{-1}g \in H$  iff  $g \in t_i H$ . Let  $W$  be the space spanned by  $w_1$ . Then  $HW = W$ , so  $W$  is a  $KH$ -module (i.e.  $W$  is a  $KH$ -submodule of  $V$ ). Also,  $t_i W = \langle x_i \rangle$  and

$$V = \bigoplus_{i=1}^m \langle x_i \rangle = \bigoplus_{i=1}^m t_i W.$$

Hence  $V = \text{ind}_H^G W$ , where  $W$  is a 1-dimensional subspace acted upon trivially by  $H$ .

**Nonstandard Notation**  $\chi_{(G)}^{(1)}$  is the trivial character of the group  $G$ .  $\chi_{(G)}^{(1)}(g) = 1 \forall g \in G$ .

**Proposition 9.9** Let  $\Pi$  be as above.

1.  $\chi_V(g)$  is the number of points of  $V$  fixed by  $g$
2.  $\sum_{g \in G} \chi_V(g) = |G|$ .
3.  $V$  is the direct sum  $V_1 \oplus V_2$  of the submodule  $V_1$  spanned by  $\sum_{i=1}^m x_i$  (on which  $G$  acts trivially) and the submodule

$$V_2 = \left\{ \sum_{i=1}^m \lambda_i x_i : \sum_{i=1}^m \lambda_i = 0 \right\}.$$

The character  $\chi_{V_2}$  is given by  $\chi_{V_2}(g) = \{\text{number of fixed points of } g\} - 1$ .

4. If  $\Pi$  is 2-transitive (i.e. if  $\forall i \neq j, k \neq l, \exists g \in G$  such that  $gx_i = x_k$  and  $gx_j = x_l$ ) and  $m \geq 2$ , then  $V_2$  is irreducible and not isomorphic to  $V_1$ .

### Proof

1. Compute the trace with respect to the basis  $X$ .

2.

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g) = (\chi_V, \chi_{(G)}^{(1)})_G = (\chi_{(H)}^{(1)}, \chi_{(H)}^{(1)} - H) = 1.$$

3.  $V_1$  and  $V_2$  are obviously submodules,  $V_1 \not\subseteq V_2$ ,  $\dim V_1 = 1$ , and  $\dim V_2 = \dim V - 1$ , so  $V = V_1 \oplus V_2$ .
4. First observe that  $(\chi_V, \chi_V)_G = (\chi_{(H)}^{(1)}, \phi)_H$ , where  $\phi$  is the restriction of  $\chi_V$  to  $H$ . Consider  $V$  as a  $KH$ -module. We have  $V = \langle x_1 \rangle \oplus \langle x_i : i > 1 \rangle$ . This is a direct sum of a module with character  $\chi_{(H)}^{(1)}$  and a module corresponding to a transitive permutation representation of  $H$  with character  $\psi$ , say. Applying (2) to the group  $H$  gives

$$(\chi_{(H)}^{(1)}, \psi) = \frac{1}{|H|} \sum_{h \in H} \psi(h) = 1.$$

So

$$(\chi_V, \chi_V)_G = (\chi_{(H)}^{(1)}, \phi)_H = (\chi_{(H)}^{(1)}, \chi_{(H)}^{(1)}) + (\chi_{(H)}^{(1)}, \psi)_H = 2.$$

So  $V$  is a direct sum of two nonisomorphic irreducible  $KG$ -submodules.

**Examples of 2-Transitive Representations**  $S_n$  ( $n \geq 3$ ),  $A_n$  ( $n \geq 4$ ),  $GL_n(F)$  on a 1-dimensional subspace of  $F^n$  for any field  $F$  ( $n \geq 2$ ).

Let us now redo induced representations from a different point of view: Suppose that  $H \leq G$ , and let  $T = \{t_1, t_2, \dots, t_m\}$  be a transversal of  $H$  in  $G$ . Let  $W$  be an  $FH$ -module. Recall that  $\text{ind}_H^G W = \bigoplus_{i=1}^m t_i W$ . Set  $V = FG \otimes_{FH} W$ , where  $FG$  is viewed as a *right*  $FH$ -module.

### Proposition 9.10

$$V = FG \otimes_{FH} W \simeq \bigoplus_{i=1}^m (t_i \otimes W) \simeq \bigoplus_{i=1}^m t_i W.$$

**Proof** Observe that  $G$  is a disjoint union of the sets  $t_i H$ ,  $t_i \in T$ . Hence, as a right  $FH$ -module, we have an isomorphism  $FG \simeq \bigoplus_{i=1}^m Ft_i H$ . Then we have

$$FG \otimes_{GH} W \cong \left( \bigoplus_{i=1}^m Ft_i H \right) \otimes_{FH} W \simeq \bigoplus_{i=1}^m t_i \otimes W.$$

Check that the  $FG$ -action agrees with that of Proposition 9.3.

**Example** We now compute the character table of  $GL_3(\mathbb{F}_2) = G$ .  $|G|$  is the number of ordered bases of  $\mathbb{F}_2^3$ , which is  $(8-1)(8-2)(8-4) = 168 = 2^3 \cdot 3 \cdot 7$ . Every element of  $G$  is conjugate to a matrix in rational canonical form. Thus each element of  $G$  is conjugate to one of

1.  $g_1 = 1$ ,

2.

$$g_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which has minimum polynomial  $x^2 + 1$ , characteristic polynomial  $(x^2 + 1)(x + 1)$ , and order 2,

3.

$$g_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

which has minimum polynomial  $x^2 + x + 1$ , characteristic polynomial  $(x^2 + x + 1)(x + 1)$ , and order 3,

4.

$$g_4 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

which has minimum polynomial  $x^3 + x^2 + x + 1$ , characteristic polynomial  $x^3 + x^2 + x + 1$ , and order 4,

5.

$$g_5 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

which has characteristic polynomial  $x^3 x + 1$  and order 7,

6.

$$g_6 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

which has characteristic polynomial  $x^3 + x^2 + 1$  and order 7.

Let the corresponding conjugacy classes be  $C_1, C_2, \dots, C_6$ , and write  $h_i = |C_i|$ .

1.  $C_i^{-1} = C_i$  for  $i \leq 4$  (as elements have the same order). Thus  $\chi(g_1)$  is real  $\forall i \leq 4$ .  $g_5^{-1}$  satisfies  $1 + g_5^{-2} + g_5^{-3}$ . (Check this.) Thus the minimum polynomial of  $g_5^{-1}$  divides  $x^3 + x^2 + 1$  (which is irreducible over  $\mathbb{F}_2$ ). Since  $g_5^{-1}$  has order 7, we have that  $g_5^{-1} \in C_6$ . Thus  $g_5^{-1} = C_6$ . Now  $g_5(g_5^2 + 1) = 1 = 0$ , and so  $g_5^2(g_5^4 + 1) + 1 = 0$  (squaring both sides in characteristic 2), and so  $g_5^2 \in C_5$ .
2.  $G$  acts 2-transitively on  $\mathbb{F}_2 \setminus \{0\}$ , for given two ordered pairs of distinct elements, we can complete each to an ordered basis and so can map one onto the other. So if  $\Pi$  is a permutation character of  $G$  on  $\mathbb{F}_2^3 \setminus \{0\}$  (i.e.  $\Pi(g)$  is the number of fixed points of  $G$  on  $\mathbb{F}_2^3 \setminus \{0\}$ ), then  $\Pi - 1$  is irreducible (see Proposition 9.9). Now the set of fixed points of  $g_i$  on  $\mathbb{F}_2^3$  is a subspace, and so it follows that  $\Pi(g_i)$  is 7, 3, 1, or 0.  $\Pi(g_i) = 7$  iff  $g_i = g_1 = 1$ .  $g_5$  and  $g_6$  act as 7-cycles, so  $\Pi(g_5) = \Pi(g_6) = 0$ .  $g_2$  fixes  $(0, 0, 1)$ ,  $(1, 1, 0)$ , and  $(1, 1, 1)$ , so  $\Pi(g_2) = 3$ .  $g_3$  is a product of  $r$  disjoint 3-cycles, and so  $\Pi(g_3) = 7 - 3r$ , and so  $r = 2$  and  $\Pi(g_3) = 1$ . (We can't have  $r = 1$  since then the number of fixed points of  $g_3$  on  $\mathbb{F}_2^3$  would be 5, which is a contradiction.)  $g_4(x, y, z) = (x, y, z)$  iff  $(x, y, z) = (z, x + z, y + z)$  iff  $y = 0$  and  $x = -2$ . Thus  $\Pi(g_4) = 1$ .
3. Thus far we have

	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$
	1	$h_2$	$h_3$	$h_4$	$h_5$	$h_6$
$\chi^{(1)}$	1	1	1	1	1	1
$\chi^{(2)}$	6	2	0	0	-1	-1

Rows are orthogonal. Hence  $R(2, 2) : 36 + 4h_2 + (h_5 + h_6) = 0$ .  $R(1, 2) : 6 : 2h_2 - (h_5 + h_6) = 0$ . Thus  $h_2 = 21$  and  $h_5 + h_6 = 48$ . Since  $C_6 = C_5^{-1}$ ,  $h_5 = h_6 = 24$ .

4. Consider  $S^2(\chi^{(2)})$ . We have

$$S^2(\chi^{(2)})(g) = \frac{1}{2}[\chi^{(2)}(g)^2 + \bar{\chi}^{(2)}(g^2)].$$

This yields

$$21 \quad 5 \quad 0 \quad 1 \quad 0 \quad 0.$$

This character decomposes, as  $21^2 > 168$ . Suppose that it contains  $\chi^{(1)}$   $r$  times and  $\chi^{(2)}$   $s$  times. Since  $\langle \chi^{(1)}, r\chi^{(1)} + s\chi^{(2)} \rangle = r\langle \chi^{(1)}, \chi^{(1)} \rangle$ ,  $168r = 21 + 5h_2 + h_4 = 126 + h_4$ , and so  $r = 1$  and  $h_2 = 42$ . Also,  $\langle \chi^{(2)}, r\chi^{(1)} + s\chi^{(2)} \rangle = s\langle \chi^{(2)}, \chi^{(2)} \rangle$ , and so  $168s = 21 \cdot 6 + 5h_2$ , or  $s = 2$ . Now  $\chi^{(3)} = S^2(\chi^{(2)}) - \chi^{(1)} - 2\chi^{(2)}$  is a character.

$$\chi^{(3)} = 6 \quad 0 \quad -1 \quad 0 \quad 1 \quad 1.$$

This is irreducible, as  $\langle \chi^{(3)}, \chi^{(3)} \rangle = 1$ .

5. Solve  $\sum_{i=1}^6 n_i^2 = 168$  to get degrees 7, 3, and 3 for  $\chi^{(4)}$ ,  $\chi^{(5)}$ , and  $\chi^{(6)}$ . Now  $C_5^{-1} = C_6$  implies that columns 5 and 6 are conjugate to each other. They are not real, as the character table is nonsingular. If  $\chi$  is a character, then  $\bar{\chi}$  is a character. Thus  $\chi^{(6)} = \bar{\chi}^{(5)}$ . Suppose that  $\chi^{(5)}(g_3) = s$  and  $\chi^{(6)}(g_3) = \bar{s} = s$ . (See (1):  $\chi(g_i)$  is real  $\forall i \leq 4$ .) Then  $s$  is a sum of 3 cube roots of unity since  $g_3$  is of order 3. Now  $\langle \chi^{(5)}, \chi^{(5)} \rangle = 1$ , and so we must have  $56s^2 < 168$ ,  $s$

real, and  $s$  a sum of three cube roots of unity, and so  $s = 0$ . Thus  $\chi^{(5)}(g_3) = \chi^{(6)}(g_3) = 0$ .

Now use  $C(1, 3)$  to compute column 3. Now use column 3 and orthogonality relations on *columns* to finish off  $\chi^{(4)}$ . Now  $\chi^{(5)}(g_2) = \chi^{(6)}(g_2) = -1$ . A similar argument shows that  $\chi^{(5)}(g_4) = \chi^{(6)}(g_4) = 1$ .

6. Now  $\chi(g_5) = \chi(g_6) \forall x$  (since  $C_5^{-1} = C_6$ ). If  $\chi(g_5)$  is real  $\forall x$ , then column 5 = column 6, which is a contradiction since the character table is nonsingular. Also,  $\chi$  is irreducible, so  $\bar{\chi}$  is irreducible, so the bottom right of the table is

$$\begin{array}{cc} \eta & \bar{\eta} \\ \bar{\eta} & \eta \end{array}$$

for some  $\eta \in \mathbb{C} \setminus \mathbb{R}$ . Now  $C(2, 5)$  implies that  $\eta + \bar{\eta} = -1$ , so  $\eta = -\frac{1}{2} + i\lambda$ .  $C(5, 6)$  implies that  $0 = 3 + \eta^2 + \bar{\eta}^2 = 3\frac{1}{2} - 2\lambda^2$ , and so  $\lambda = \frac{\sqrt{7}}{2}$ . This completes the calculation of the character table.

	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$
	1	21	56	42	24	24
$\chi^{(1)}$	1	1	1	1	1	1
$\chi^{(2)}$	6	2	0	0	-1	-1
$\chi^{(3)}$	8	0	-1	0	1	1
$\chi^{(4)}$	7	-1	1	-1	0	0
$\chi^{(5)}$	3	-1	0	1	$-\frac{1}{2} + i\frac{\sqrt{7}}{2}$	$-\frac{1}{2} - i\frac{\sqrt{7}}{2}$
$\chi^{(6)}$	3	-1	0	1	$-\frac{1}{2} - i\frac{\sqrt{7}}{2}$	$-\frac{1}{2} + i\frac{\sqrt{7}}{2}$

Here are some of the things we can conclude from the character table:

1.  $G$  is simple, for if not, then  $\exists i, j > 1$  with  $\chi^{(i)}(g_j) = \chi^{(i)}(1)$ . We show this in two steps:

**Lemma A** Let  $G$  be a finite group, and suppose that  $\rho : G \rightarrow GL(V)$  is a representation of degree  $m$  and character  $\chi$ . If for some  $g \in G$  we have  $|\chi(g)| = m$ , then  $\rho(g) = \omega I$ , where  $\omega$  is a root of unity. If  $\chi(g) = m$ , then  $\rho(g) = I$ , i.e.  $g \in \ker \rho$ .

**Proof** Suppose that  $g$  is of order  $k$ . Then  $\rho(g)$  satisfies the equation  $x^k - 1$ . Since this splits over  $K$ , it follows that  $\rho(g)$  is diagonalizable. Let  $\lambda_1, \lambda_2, \dots, \lambda_m$  be the eigenvalues of  $\rho(g)$  (counted with multiplicity). Then  $\lambda_1, \lambda_2, \dots, \lambda_m$  are roots of unity, and  $\chi(g) = \lambda_1 + \lambda_2 + \dots + \lambda_m$ , and so

$$|\chi(g)| \leq |\lambda_1| + |\lambda_2| + \dots + |\lambda_m| = m. \quad (*)$$

The triangle inequality implies that equality holds in  $(*)$  iff  $\lambda_1 = \lambda_2 = \dots = \lambda_m = \omega$ . This implies that  $\rho(g) = \omega I$ . Hence if  $\chi(g) = m$ , then  $\omega = 1$ , and  $\rho(g) = I$ , i.e.  $g \in \ker \rho$ .

**Lemma B** Let  $G$  be a finite group. Then  $G$  is simple iff  $\forall g \in G$  and for every irreducible character  $\chi \neq 1$ , we have that  $\chi(g) \neq \chi(1)$  if  $g \neq 1$ .

**Proof** The forward direction follows from Lemma A. For the reverse direction, suppose that  $N \triangleleft G$  with  $N \neq 1$ , and let  $\hat{\chi}$  be an irreducible character of  $G/N$ . Define  $\chi : G \rightarrow K^\times$  by

$\chi(g) = \widehat{\chi}(\bar{g})$ , where  $\bar{g}$  is the image of  $g$  in  $G/N$ . Check that  $\chi$  is an irreducible character of  $G$ . Then if e.g.  $g \in N$  with  $g \neq 1$ , we have that  $\chi(g) = \chi(1)$ .

2. Every element of order 7 lies in a unique subgroup of order 7. Thus the number of subgroups of order 7 is 8. Similarly, the number of subgroups of order 3 is 28.
3. Centralizers of elements of order 2 have order  $168/h_2 = 168/21 = 8$ . These centralizers are conjugate to each other. (Another way to see this is to note that these centralizers are Sylow 2-subgroups of  $G$ .) Observe that each element  $g$  of order 4 has  $g^2$  of order 2 and so lies in a subgroup of order 8. The centralizer of such a  $g$  has order  $168/h_4 = 168/42 = 4$ , and so it follows that the subgroups of order 8 are nonabelian.
4. If  $x$  and  $y$  are of order 2 with  $x \neq y$ , then  $C_G(x) \neq C_G(y)$ , for otherwise, we have that  $\{1, x, y, xy\} \subseteq Z(C_G(x))$ , which implies that  $C_G(x)$  is abelian, which is a contradiction. (Note that the two nonabelian groups of order 8 viz.  $D_8$  and  $H_8$  have centers of order 2.) Thus the number of subgroups of  $G$  of order 8 is 21.

## 9.2 Some Remarks on Tensor Products

We want to consider tensor products over noncommutative rings.

**Definition 9.11** Let  $R$  and  $S$  be rings (not necessarily commutative), and let  $M$  be an abelian group which is both a left  $R$ -module and a right  $S$ -module such that  $(rx)s = r(xs) \forall x \in M, r \in R, s \in S$ . Then  $M$  is said to be an  $(R, S)$ -**bimodule** (sometimes written  $R^M S$ ).

Let  $R$  be any ring,  $U$  a *right*  $R$ -module, and  $V$  a *left*  $R$ -module. For any abelian group  $W$ , consider mappings  $f : U \times V \rightarrow W$  such that

1.  $f$  is **biadditive**, i.e. additive in each argument.
2.  $f$  is  **$R$ -balanced**, i.e.  $f(ur, v) = f(u, rv) \forall u \in U, v \in V, r \in R$ .

Construct  $U \otimes_R V$  (now merely an abelian group!) universal for  $R$ -balanced, biadditive maps from  $U \times V$  to abelian groups:

$$\begin{array}{ccc} U \times V & \xrightarrow{f} & W \\ \downarrow \otimes_R & \nearrow \exists! \tilde{f} & \\ U \otimes_R V & & \end{array}$$

$\tilde{f}$  is a homomorphism of abelian groups.

**Existence**  $U \otimes_R V = A/B$ , where  $A$  is a free abelian group on  $U \times V$  and  $B$  is a subgroup generated by

$$(u + u', v) - (u, v) - (u', v), u, u' \in U$$

$$(u, v + v') - (u, v) - (u, v'), v, v' \in V$$

$$(ur, v) - (u, rv), r \in R.$$

Now suppose that  $U$  is an  $(S, R)$ -bimodule and  $V$  is an  $(R, T)$ -bimodule. Then  $U \otimes_R V$  may be viewed as an  $(S, T)$ -bimodule in the following way: Suppose that  $s \in S$ , and consider  $\lambda_s : U \times V \rightarrow U \otimes_R V$ ,  $(u, v) \mapsto su \otimes v$ . Then  $\lambda_s$  is biadditive and  $R$ -balanced. (Check this.) Thus  $\lambda_s$  induces a homomorphism  $\widetilde{\lambda}_s : U \otimes_R V \rightarrow U \otimes_R V$  (which we just denote by “ $s$ ”):

$$s \left( \sum u_i \otimes v_i \right) = \sum su_i \otimes v_i.$$

We thus obtain a left  $S$ -module structure on  $U \otimes_R V$ . Similarly, by considering  $\mu_t : U \times V \rightarrow U \otimes_R V$ , we obtain a right  $T$ -module structure on  $U \otimes V$ . Hence  $U \otimes V$  is an  $(S, T)$ -bimodule.

**Example** Let  $G$  be a finite group and  $H \leq G$ . Suppose that  $W$  is a  $KH$ -module. Then  $FG$  is an  $(FG, FH)$ -bimodule,  $W$  is an  $(FH, (0))$ -bimodule (i.e. a left  $FH$ -module). Thus  $FG \otimes_{FH} W = \text{ind}_H^G W$  is a left  $FG$ -module.

### 9.3 Tensor, Symmetric, and Exterior Algebras

**Definition 9.12** Let  $K$  be a field. A  $K$ -algebra is a  $K$ -vector space  $A$  which is also a ring (associated with a 1) such that the multiplication map  $A \times A \rightarrow A$  is  $K$ -bilinear. A  $K$ -algebra homomorphism  $f$  is a  $K$ -linear ring homomorphism (so  $f(1) = 1$ ), e.g.  $M_n(K)$ ,  $\text{end}_K(V)$ ,  $K[x_1, x_2, \dots, x_n]$ , and  $KG$ .

Let  $V_1, V_2, \dots, V_n$  be  $K$ -vector spaces. Define  $V_1 \otimes V_2 \otimes \dots \otimes V_n$  inductively by

$$v_1 \otimes v_2 \otimes \dots \otimes v_n = (v_1 \otimes v_2 \otimes \dots \otimes v_{n-1}) \otimes v_n.$$

(There's a canonical isomorphism from  $v_1 \otimes v_2 \otimes \dots \otimes v_n$  to the iterated tensor product with any other bracketing.) If  $V_1, V_2, \dots, V_n$  are finite dimensional, then  $V_1 \otimes V_2 \otimes \dots \otimes V_n$  has basis  $\{x_1 \otimes x_2 \otimes \dots \otimes x_n\}$  with the  $x_i$  running independently through a basis of the  $V_i$ .

Define  $\bigotimes^n V = \underbrace{V \otimes V \otimes \dots \otimes V}_n$  to be the  $n^{\text{th}}$  tensor power of  $V$ . Define

$$T(V) = \bigoplus_{n=0}^{\infty} \left( \bigotimes^n V \right)$$

( $\bigotimes^0$  means  $K$ ). Then  $T(V)$  is a  $K$ -vector space. To define a  $K$ -bilinear product, it suffices to define a  $K$ -bilinear map  $(\bigotimes^m V) \times (\bigotimes^n V) \rightarrow T(V) \forall m, n$ . Use the isomorphism

$$\left( \bigotimes^m V \right) \otimes \left( \bigotimes^n V \right) \simeq \bigotimes^{m+n} V.$$

Make the product of  $h \in \bigotimes^m V$  and  $k \in \bigotimes^n V$  the image of  $h \otimes k$  in  $\bigotimes^{m+n} V$ .

**Definition 9.13**  $T(V)$  is the **tensor algebra** on  $V$ . Let  $i : V \rightarrow T(V)$  be the natural inclusion map.

**Theorem 9.14** If  $f : V \rightarrow A$  is a  $K$ -linear map from  $V$  to a  $K$ -algebra  $A$ , then  $\exists!$   $K$ -algebra homomorphism  $\widehat{f} : T(V) \rightarrow A$  so that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{f} & A \\ \downarrow i & \nearrow \widehat{f} & \\ T(V) & & \end{array}$$

**Proof** For such an  $\widehat{f}$ , we need  $\widehat{f}(1) = 1$  and  $\widehat{f}(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = f(v_1)f(v_2)\cdots f(v_n)$ . So if  $\widehat{f}$  exists, then it is unique, as  $T(V)$  is spanned by 1 and elements of the form  $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ . We proceed inductively: Define  $\widehat{f}(1) = 1$ ,  $\widehat{f}|_V = f$ . Suppose that  $\widehat{f}|_{\otimes^r V}$  is defined (and is  $K$ -linear) for  $r < n$ . Consider the map

$$\begin{aligned} \left(\bigotimes^{n-1} V\right) \times V &\rightarrow A \\ (t, v_n) &\mapsto \widehat{f}(t)f(v_n). \end{aligned}$$

This map is  $K$ -bilinear, and so it factors through  $\left(\bigotimes^{n-1} V\right) \otimes V$  to give a  $K$ -linear map  $\widehat{f}|_{\otimes^n V}$ . So we obtain a linear map  $\widehat{f} : T(V) \rightarrow A$  so that  $f = \widehat{f} \circ i$  and

$$\widehat{f}(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = \widehat{f}(v_1 \otimes v_2 \otimes \cdots \otimes v_{n-1})f(v_n) = \cdots = f(v_1)f(v_2)\cdots f(v_n) \quad \forall v_1, v_2, \dots, v_n \in V.$$

So we have

$$\begin{aligned} \widehat{f}[(u_1 \otimes u_2 \otimes \cdots \otimes u_m)v_1 \otimes v_2 \otimes \cdots \otimes v_n] &= \widehat{f}(u_1 \otimes u_2 \otimes \cdots \otimes u_m \otimes v_1 \otimes v_2 \otimes \cdots \otimes v_n) \\ &= f(u_1)f(u_2)\cdots f(u_m)f(v_1)f(v_2)\cdots f(v_n) \\ &= \widehat{f}(u_1 \otimes u_2 \otimes \cdots \otimes u_m)\widehat{f}(v_1 \otimes v_2 \otimes \cdots \otimes v_n). \end{aligned}$$

Hence  $T(V)$  is spanned by elements  $h$  for which  $\widehat{f}(h_1 h_2) = \widehat{f}(h_1)\widehat{f}(h_2)$ . Hence  $\widehat{f}$  is a ring homomorphism via linearity.

Let  $I$  be the ideal of  $T(V)$  generated by all  $\{u \otimes v - v \otimes u \mid u, v \in V\}$ . (So  $I$  consists of sums of elements  $t_1 - t_2$ ,  $t_1, t_2 \in T(V)$ ).  $I$  is a subspace as well as an ideal.

**Definition 9.15** The algebra  $S(V) := T(V)/I$  is the **symmetric algebra on  $V$** . Let  $i' : V \xrightarrow{i} T(V) \xrightarrow{\text{quotient}} S(V)$ .

**Theorem 9.16**

1.  $S(V)$  is commutative. If  $f : V \rightarrow A$  is a linear map and  $A$  is a commutative algebra, then  $\exists!$   $K$ -algebra homomorphism  $\widehat{f} : S(V) \rightarrow A$  such that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{f} & A \\ \downarrow i' & \nearrow \exists! \widehat{f} & \\ S(V) & & \end{array}$$

2. If  $x_1, x_2, \dots, x_m$  is a basis of  $V$ , then  $S(V)$  is just the polynomial algebra  $K[x_1, x_2, \dots, x_m]$ .

**Proof**

- The elements  $v \in V$  commute with each other, and they generate  $S(V)$ . So  $S(V)$  is commutative. Theorem 9.14 implies  $\exists! f_1 : T(V) \rightarrow A$  such that  $f = f_1 \circ i$ . But each  $u \otimes v - v \otimes u \in \ker f_1$  since  $A$  is commutative. So  $I \leq \ker f_1$ , and so  $f_1$  factors through  $S(V) = T(V)/I$ .
- $S(V)$  is generated by products of the  $x_i$ s, and so each element in  $S(V)$  is a polynomial in the  $x_i$ . But the identity map  $V \rightarrow V \leq K[x_1, x_2, \dots, x_n]$  extends to a unique homomorphism  $S(V) \rightarrow K[x_1, x_2, \dots, x_n]$  by (1) above, which must be the identity. (Alternatively,  $K[x_1, x_2, \dots, x_n]$  satisfies the right universal property.)

Suppose that  $\text{char } K \neq 2$ . Let  $I$  be the ideal of  $T(V)$  generated by all of the elements  $v \otimes v$ ,  $v \in V$  (equivalently generated by all elements  $u \otimes v + v \otimes u$ ,  $u, v \in V$ ).

**Definition 9.17** The algebra  $\Lambda(V) := T(V)/I$  is the **exterior algebra** of  $V$ . Let  $i''$  be the map

$$i'' : V \xrightarrow{i} T(V) \xrightarrow{\text{quotient}} \Lambda(V).$$

**Theorem 9.18** Let  $A$  be any  $K$ -algebra. If  $f : V \rightarrow A$  is a  $K$ -linear map such that  $f(v)f(v) = 0 \forall v \in V$ , then  $\exists! \widehat{f} : \Lambda(V) \rightarrow A$  such that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{f} & A \\ \downarrow i'' & \nearrow \exists! \widehat{f} & \\ \Lambda(V) & & \end{array}$$

**Proof** Similar to Theorem 9.16(1).

**Definition 9.19** The  $n^{\text{th}}$  **symmetric** and **exterior powers** of  $V$ ,  $S^n(V)$  and  $\lambda^n(V)$ , are the images of  $\otimes^n V$  in  $S(V)$  and  $\Lambda(V)$ , respectively (and so are the subspaces generated by products of  $n$  elements of  $V$ ). ( $S^n(V)$  and  $\lambda^n(V)$  have universal properties with respect to  $n$ -linear symmetric

and skew-symmetric forms.)

If  $V$  is a  $KG$ -module, then  $T(V)$ ,  $S(V)$ , and  $\Lambda(V)$  are naturally  $KG$ -modules, and  $S^n(V)$  and  $\lambda^n(V)$  are submodules. If  $\{x_1, x_2, \dots, x_m\}$  is a basis of  $V$ , then  $S^n(V)$  consists of homogeneous polynomials of degree  $n$  in  $x_1, x_2, \dots, x_m$ . Hence we can compute the trace of  $g \in G$  acting on  $S^n(V)$  with respect to the basis consisting of all monomials

$$\{x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m} \mid \sum r_i = n\}.$$

Work in the exterior algebra: Let  $v_1, v_2, \dots, v_n \in V$ . Then  $v_i v_{i+1} + v_{i+1} v_i = 0$ . So

$$v_1 v_2 \cdots v_{i-1} v_i v_{i+1} \cdots v_n + v_1 v_2 \cdots v_{i-1} v_{i+1} v_i \cdots v_n = 0.$$

Hence

$$v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} = \epsilon(\sigma) v_1 v_2 \cdots v_n \quad \forall \sigma \in S_n. \quad (*)$$

Since also  $vv = 0 \forall v \in V$ , it follows that  $\lambda^n(V)$  is spanned by  $x_{i_1} x_{i_2} \cdots x_{i_n}$  with  $i_1 < i_2 < \cdots < i_n$ . (In particular,  $\lambda^n(V) = 0$  if  $n > m$ , and  $\dim \Lambda(V)$  is finite if  $\dim V$  is finite.)

**Theorem 9.20** The  $x_{i_1} x_{i_2} \cdots x_{i_n}$  with  $i_1 < i_2 < \cdots < i_n$  form a basis of  $\lambda^n(V)$ .

**Proof** Define a  $K$ -linear map  $\phi : T(V) \rightarrow K$  by specifying the image of a basis:  $\phi(1) = 0$ , and for  $i_1, i_2, \dots, i_t \in \{1, 2, \dots, m\}$ ,

$$\phi(x_{i_1} \otimes x_{i_2} \otimes \cdots \otimes x_{i_t}) = \begin{cases} \text{sgn}(\prod_{i < k} (i_j - i_k)) & \text{if the product is nonempty,} \\ 0 & \text{otherwise.} \end{cases}$$

Now  $\Lambda(V) = T(V)/J$ , where  $J$  is generated as an ideal by elements of the form  $x_r \otimes x_s + x_s \otimes x_r$ . Thus  $J$  is generated as a  $K$ -vector space by all elements  $h \otimes x_r \otimes x_s \otimes k + h \otimes x_s \otimes x_r \otimes k$ , where  $h$  and  $k$  run through a basis of  $T(V)$ . It is easy to check that  $\phi(J) = 0$ . Now suppose  $\exists$  a nontrivial relation,

$$\sum_{l=1}^r \lambda_l P_l = 0,$$

where  $\lambda_l \in K$ , and each  $P_l$  is of the form  $x_{i_1} x_{i_2} \cdots x_{i_{m_l}}$ , with  $i_1 < i_2 < \cdots < i_{m_l}$ . Choose the  $P_l$ s to make  $r$  as small as possible. If  $r > 1$ , then some  $x_j$  appears in some but not all of the  $P_l$ s. Thus

$$0 = \left( \sum_{l=1}^r \lambda_l P_l \right) x_j = \sum_{l=1}^r \lambda_l (P_l x_j).$$

Now rearrange using (\*) to contradict the minimality of  $r$ . So  $r = 1$ , and we have a relation of the form  $x_{i_1} x_{i_2} \cdots x_{i_n} = 0$ ,  $i_1 < i_2 < \cdots < i_n$ . Thus  $x_{i_1} x_{i_2} \cdots x_{i_n} \in J$ , which is a contradiction from the definition of  $\phi$ . In particular, if  $\dim V = m$ , then  $\dim \lambda^m(V) = 1$ ,  $\alpha \in \text{end}(V)$  induces scalar multiplication by  $\det(\alpha)$  on  $\lambda^m(V)$ .

**Caveat** If  $n > 2$ , it is not true that

$$\bigotimes^n V = S^n(V) \oplus \lambda^n(V).$$

To check this, just compute dimensions!

Now we can compute characters. Let  $\mu_1, \mu_2, \dots, \mu_n \in K$  and  $\sigma_1, \sigma_2, \dots, \sigma_n$  be the elementary symmetric functions on the  $\mu_i$ s. (So  $\sigma_r$  is the sum of the product of the  $\mu_i$ s taken  $r$  at a time.) Then

$$\prod_{i=1}^m (x - \mu_i) = \sum_{r=0}^m (-1)^r x^{m-r} \sigma_r, \quad \sigma_0 = 1. \quad (\dagger)$$

$\exists P_n(x_1, x_2, \dots, x_m) \in \mathbb{Z}[x_1, x_2, \dots, x_m]$  so that  $\mu_1^n + \mu_2^n + \dots + \mu_m^n = P_n(\sigma_1, \sigma_2, \dots, \sigma_m)$  (c.f. p. 190–191 of Lang's *Algebra*).

**Theorem 9.21** Let  $G$  be a finite group, and suppose that  $V$  is a  $\mathbb{C}G$ -module. Then the character  $\chi$  of  $\lambda^r(V)$  evaluated at  $g \in G$  is

1.  $\sigma_r(\mu_1, \mu_2, \dots, \mu_m)$ , where  $\mu_1, \mu_2, \dots, \mu_m$  are the eigenvalues of  $g$  on  $V$ .
2.  $(-1)^r \times$  (coefficient of  $x^{m-r}$  in the characteristic polynomial of  $G$  on  $V$ ).

**Proof**

1. Let  $(x_1, x_2, \dots, x_m)$  be a basis of eigenvectors of  $g$  on  $V$ . Compute the trace with respect to the  $x_{i_1} x_{i_2} \dots x_{i_r}$ s, where  $i_1 < i_2 < \dots < i_r$ . The contribution from  $x_{i_1} x_{i_2} \dots x_{i_r}$  is  $\mu_{i_1} \mu_{i_2} \dots \mu_{i_r}$ . Hence (1) holds.
2. This follows immediately from (1) and  $(\dagger)$ .

Let  $G$  be a finite group. The set of complex characters is closed with respect to sums and products and is contained in the ring of class functions. The **character ring**  $R_G$  of  $G$  is the subring (of the ring of class functions) generated by the characters. Each element of  $R_G$  is of the form  $\chi - \phi$ , where  $\chi$  and  $\phi$  are characters; each element is uniquely expressible as a  $\mathbb{Z}$ -linear combination of irreducible characters (uniqueness follows from the fact that irreducible characters are linearly independent). The elements of  $R_G$  are called **virtual characters**.

**Theorem 9.22** If  $n \in \mathbb{N}$  is fixed and  $\chi$  is a complex character, then  $g \mapsto \chi(g^n)$  is a virtual character.

**Proof** Suppose that  $\chi$  corresponds to a  $\mathbb{C}G$ -module  $V$  of dimension  $m$ . Then

$$\Pi = P_n(\chi_{\lambda^1(V)}, \chi_{\lambda^2(V)}, \dots, \chi_{\lambda^m(V)})$$

is a virtual character. If  $g \in G$  has eigenvalues  $\mu_1, \mu_2, \dots, \mu_m$  of  $V$ , then

$$\begin{aligned} \Pi(g) &= P_n(\sigma_1(\mu_1, \mu_2, \dots, \mu_m), \sigma_2(\mu_1, \mu_2, \dots, \mu_m), \dots, \sigma_m(\mu_1, \mu_2, \dots, \mu_m)) \\ &= \mu_1^n + \mu_2^n + \dots + \mu_m^n \\ &= \chi(g^n). \end{aligned}$$

(In fact, this works for  $n \in \mathbb{Z}$  since  $g \mapsto \chi(g^{-1})$  is a character, the **contragredient** of  $\chi$ . If  $\chi$  corresponds to  $\rho$ , then  $g \mapsto \rho(g^{-1})^t$  is a representation and has character  $g \mapsto \chi(g^{-1})$ .)

# Chapter 10

## Character Degrees: The $p^\alpha q^\beta$ Theorem

**Hypotheses**  $G$  is a finite group, and representations are over  $\mathbb{C}$ .

### 10.1 Algebraic Integers

**Definition 10.1** An element  $\alpha \in \mathbb{C}$  is an **algebraic integer** if it satisfies a polynomial equation  $\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$ , all  $c_i \in \mathbb{Z}$ , e.g. elements of  $\mathbb{Z}$ , roots of unity, etc.

#### Proposition 10.2

1. The set of algebraic integers is a ring. So character values are algebraic integers.
2. If  $\gamma \in \mathbb{Q}$  and  $\gamma$  is an algebraic integer, then  $\gamma \in \mathbb{Z}$ . ( $\gamma = \frac{r}{s}$ , say, with  $(r, s) = 1$ , and  $\gamma^n + a_1\gamma^{n-1} + \cdots + a_n = 0$ , so  $r^n - s(a_1r^{n-1} + a_2r^{n-2}s + \cdots + a_ns^{n-1})$  implies that  $s \mid r^n$ , and so  $s = \pm 1$ .)
3. If  $y_1, y_2, \dots, y_n \in \mathbb{C}$  are not all zero and  $\gamma$  satisfies

$$\sum_{j=1}^N a_{ij}y_j = \gamma y_i \quad (i = 1, 2, \dots, N),$$

then  $\gamma$  is an algebraic integer provided all  $a_{ij} \in \mathbb{Z}$ . ( $\sum_{j=1}^N (a_{ij} - \gamma\delta_{ij})y_j = 0$ , each  $i$  is nonzero, and not all  $a_{ij}$ s are 0. So we have  $0 = \det(a_{ij} - \gamma\delta_{ij})$ , this is a monic polynomial equation in  $\gamma$  with integer coefficients.)

#### Proof

1. We claim that if  $f(X, Y) \in \mathbb{Z}[X, Y]$  and  $\alpha$  and  $\beta$  are algebraic integers, then so is  $f(\alpha, \beta)$ . Suppose that  $\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = \beta^m + d_1\beta^{m-1} + \cdots + d_m = 0$ . Let  $y_1, y_2, \dots, y_N =$

$\{\alpha^i \beta^j \mid 0 \leq i \leq n, 0 \leq j \leq m\}$ . Then every  $\alpha^i \beta^j$  with  $i, j \geq 0$  is a  $\mathbb{Z}$ -linear combination of these. (This follows via induction on  $i$  and  $j$ , e.g. if  $i \geq n$ , we can use

$$\alpha^n = -c_1 \alpha^{n-1} - \dots$$

to express  $\alpha^i \beta^j$  in terms of  $\alpha^k \beta^l$  already considered.) Hence  $f(\alpha, \beta) = \gamma$  is a  $\mathbb{Z}$ -linear combination of  $y_1, y_2, \dots, y_N$ . So is  $\gamma y_i$ ,  $1 \leq i \leq N$ . Suppose  $\gamma y_i = \sum_{j=1}^N a_j y_j$ . Now the result follows from (3).

Character values are algebraic integers since they are sums of roots of unity.

**Notation**  $G$  is finite, with conjugacy classes  $C_1 = \{1\}, C_2, \dots, C_d, g_i \in C_i$ .

**Theorem 10.3** Let  $\chi$  be a character of an irreducible representation  $\rho$  of degree  $n$  of  $G$ .

1.  $\frac{|C_i|}{n} \chi(g_i)$  is an algebraic integer.
2.  $n$  divides  $|G|$ .

**Proof**

2.

$$\frac{|G|}{n} = \frac{|G|}{n} \langle \chi, \chi \rangle = \sum_{g \in G} \chi(g^{-1}) \left( \frac{\chi(g)}{n} \right) = \sum_{i=1}^d \chi(g_i^{-1}) \left( |C_i| \frac{\chi(g_i)}{n} \right).$$

1. (Recall Proposition 7.10.) Let  $c_k = \sum_{g \in C_k} g \in$  center of  $\mathbb{C}G$  for  $k = 1, 2, \dots, d$ . Recall that the elements  $c_1, c_2, \dots, c_k$  form a basis for the center of  $\mathbb{C}G$ . So for fixed  $i$  and for each  $k$ , we have

$$c_i c_k = \sum_{j=1}^d a_{ik}^{(j)} c_j,$$

$a_{ik}^{(j)} \in \mathbb{Z}$ ,  $j = 1, 2, \dots, d$ . Now  $\rho : G \rightarrow GL(V)$  extends to a ring homomorphism  $\rho : \mathbb{C}G \rightarrow \text{end}(V)$ . Since  $\rho(c_k)$  commutes with each  $\rho(g)$  ( $g \in G$ ), it follows that  $\rho(c_k)$  is a  $\mathbb{C}G$ -module homomorphism. Thus Schur's Lemma implies that  $\rho(c_k)$  is multiplication by a scalar,  $\gamma_k$ , say. Write  $I \in \text{end } V$  for the identity map. Then

$$(\gamma_i \gamma_k) I = (\gamma_i I)(\gamma_k I) = \rho(c_i) \rho(c_k) = \rho(c_i c_k) = \left( \sum_{j=1}^d a_{ik}^{(j)} \gamma_j \right) I.$$

So

$$\gamma_i \gamma_k = \sum_{j=1}^d a_{ik}^{(j)} \gamma_j, \quad k = 1, 2, \dots, d.$$

Now all the  $\gamma_k$ s are zero, e.g.  $\gamma_1 = 1$ . Thus Proposition 10.2(3) implies that  $\gamma_i$  is an algebraic integer. Now taking traces gives  $n \gamma_i = \text{tr}(\rho(c_i)) = \sum_{g \in C_i} \chi(g)$ , and this implies the result.

**Lemma 10.4** Suppose that  $\alpha = \frac{1}{n} \sum_{k=1}^n \omega_k$ , where each  $\omega_k$  is a root of unity. If  $\alpha$  is also an algebraic integer, then  $\alpha = 0$  or  $\omega_1 = \omega_2 = \cdots = \omega_n$  (so  $\alpha$  is a root of unity).

**Proof**  $\exists$  a root of unity  $\omega$  such that each  $\omega_k$  is a power of  $\omega$ . Let  $f$  be the minimum (monic) polynomial of  $\alpha$  over  $\mathbb{Z}$ . Then  $f$  is the minimum polynomial of  $\alpha$  over  $\mathbb{Q}$ . The roots are precisely the images  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$  of  $\alpha$  under the action of  $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ . Thus each  $\alpha_i$  is of the form  $\frac{1}{n}$ (sum of roots of unity). So  $|\alpha_i| \leq 1$ , and unless all  $\omega_j$ s are equal,  $|\alpha| < 1$ , and  $\prod_i |\alpha_i| < 1$ . But  $\pm \prod_i \alpha_i$  is the constant coefficient in  $f$ . So  $\prod_i \alpha_i \in \mathbb{Z}$ , whence  $\prod_i \alpha_i = 0$ , and so  $\alpha = 0$ .

**More Notation**  $\chi^{(1)} - 1, \chi^{(2)}, \dots, \chi^{(d)}$  are the irreducible characters of  $G$ .  $\rho_1 = 1, \rho_2, \dots, \rho_d$  are the corresponding representations of degrees  $n_1 = 1, 2, \dots, d$ . Proposition 10.3(1) implies that

$$\frac{|C_j|}{n_i} \chi^{(i)}(g_j)$$

are algebraic integers  $\forall i, j$ .

**Proposition 10.5** If  $n_i$  and  $|C_j|$  are coprime, then either  $\chi^{(i)}(g_j) = 0$  or  $\rho_i(g_j)$  is multiplication by a root  $\omega$  of unity (so  $\chi^{(i)}(g_j) = n_i \omega$ ).

**Proof** Since  $n_i$  and  $|C_j|$  are coprime,  $\exists a, b \in \mathbb{Z}$  so that  $an_i + b|C_j| = 1$ . Let  $\omega_1, \omega_2, \dots, \omega_n$  be the eigenvalues of  $\rho_i(g_j)$ . Then

$$\frac{1}{n} \sum_{k=1}^n \omega_k = \frac{1}{n_i} \chi^{(i)}(g_j) = a \chi^{(i)}(g_j) + b \left( \frac{|C_j|}{n_i} \right) \chi^{(i)}(g_j).$$

So  $\frac{1}{n} \chi^{(i)}(g_j)$  is an algebraic integer. Lemma 10.4 implies that either  $\chi^{(i)}(g_j) = 0$  or  $\omega_1 = \omega_2 = \cdots = \omega_n$ . So since  $\exists$  a basis of eigenvectors,  $\rho_i(g_j)$  is multiplication by  $\omega_1$ .

**Proposition 10.6** If  $|C_j|$  is a power of a prime  $p$  for some  $j > 1$ , then  $G$  is not nonabelian simple.

**Proof** Suppose that  $G$  is nonabelian simple. If  $i > 1$  and  $(p, n_i) = 1$ , then by Proposition 10.5, either

1.  $\chi^{(i)}(g_j) = 0$
2.  $\rho_i(g_j)$  is multiplication by a scalar.

(2) implies  $\rho_r(g_j)$  is in the center of  $\rho_i(G)$ . Since  $G$  is nonabelian simple,  $\ker \rho_i = \{1\}$  (since  $i > 1$ ), and the center of  $\rho_i(G)$  is trivial. So  $\rho_i(g_j) = 1$ , and so  $g_j = 1$ , which is a contradiction. Hence for  $i > 1$ , either  $\chi^{(i)}(g_j) = 0$  or  $p \mid n_i$ . Now orthogonality of column 1 and column  $j$  gives

$$0 = \sum_{i=1}^d \chi^{(i)}(1) \chi^{(i)}(g_j) = 1 + \sum_{i=2}^d n_i \chi^{(i)}(g_j).$$

Thus

$$-\frac{1}{p} = \sum_{i=2}^d \frac{n_i}{p} \chi^{(j)}(g_j).$$

Each summand on the RHS is either 0 (if  $p \nmid n$ ) or an algebraic integer (if  $p \mid n$ ), which is a contradiction. (See Proposition 10.2(2).)

### Recall

1. If  $|Q| = p^m$ , where  $p$  is prime and  $m \geq 1$ , then the center of  $Q$  is nontrivial.
2. (Sylow) If  $|G| = p^m r$  with  $(p, r) = 1$ , then  $G$  has a subgroup of order  $p^m$ .

**Theorem 10.7** (Burnside's  $p^\alpha q^\beta$  Theorem) If  $|G| = p^\alpha q^\beta$ , where  $p$  and  $q$  are prime and  $\alpha, \beta \in \mathbb{N}$ , then  $G$  cannot be nonabelian simple.

**Proof**  $G$  has a subgroup  $Q$  of order  $q^\beta$ . Let  $z \neq 1$ ,  $z \in$  center of  $Q$ . The number of conjugates of  $z$  in  $G$  is  $|G : C_G(z)|$ , and  $Q \leq C_G(z)$ . So

$$p^\alpha = \frac{|G|}{|Q|} = |G : C_G(z)| \frac{|C_G(z)|}{Q} = |G : C_G(z)| |C_G(z) : Q|.$$

Now the result follows from Proposition 10.6.