Representations of Finite Groups.

1. Semi-simplicity. If G is a group and F is a field, an *FG-module* M is a vector space over F with a linear G-action $G \times M \to M$, i.e., one that satisfies

$$\sigma(ax+by) = a\sigma(x) + b\sigma(y)\,, \qquad \sigma \in G\,, x, y \in M\,, a, b \in F\,. \tag{1}$$

Thus, every $\sigma \in G$ acts on M as a linear transformation $\Delta(\sigma)$. Instead of considering the FG-module M, we could equivalently speak of the *representation* Δ, which is a homomorphism $G \to \mathrm{Aut}_F(M)$.

CONVENTION: In this course, the groups G to be represented are tacitly assumed to have finite order, and all FG-modules, to have finite dimension over F.

THEOREM (Maschke): *Suppose that the order $|G|$ is prime to the characteristic of F, and let $N \subseteq M$ be FG-modules. Then $M = N \oplus N'$, where $N' \subseteq M$ is an FG-module.*

Proof. We need a left inverse ("retraction") $p \in \mathrm{Hom}_{FG}(M, N)$ for the inclusion $N \hookrightarrow M$. It is easy to produce such a thing, say f, in $\mathrm{Hom}_F(M, N)$. Take it and define

$$p(x) = \frac{1}{|G|} \sum_G \sigma f(\sigma^{-1}x). \tag{2}$$

For $x \in N$, we have $f(x) = x$ and hence $p(x) = x$, so p is still a left inverse. Moreover, $p(\tau x) = \tau p(x)$ for all $\tau \in G$, q.e.d.

By induction, every FG-module M splits into a direct sum $L_1 \oplus \cdots \oplus L_t$ of FG-modules which are *irreducible* in the sense that they have no FG-submodules. The uniqueness of the irreducible components L_i, up to isomorphism, follows at once from general theorems (e.g. Jordan-Hölder or Krull-Schmidt), but we shall soon see it more directly.

Henceforth assume that the characteristic of F is prime to $n = |G|$.

The *group algebra FG* consists of all "polynomials" $\alpha = \sum_G a_\sigma \sigma$, with products $\alpha\beta$ defined by the distributive law and the multiplication in G.

LEMMA 1.1: *Let L and N be irreducible FG-modules with $L \subseteq FG$ a left ideal. Then $LN = 0$ unless L and N are isomorphic.*

Proof. For every $x \in N$, the product Lx is either O or N, since it is an FG-submodule of N. In case $Lx = N$, the surjection $L \to N$ by $\lambda \mapsto \lambda x$ is an isomorphism, q.e.d.

COROLLARY: *Let $FG = L_1 \oplus \cdots \oplus L_t$ be a complete decomposition of FG as a (left) FG-module. Then every irreducible FG-module N is isomorphic to a suitable L_j.*

Proof. Since $(FG)N = N$, we must have $L_j N \neq 0$ for some j. Then $L_j \simeq N$ by the Lemma; q.e.d.

Now collect the aforementioned L_j into isomorphism classes, say $\mathcal{I}_1, \ldots, \mathcal{I}_s$, and let M_i be the direct sum of all the L_j which belong to $\mathcal{I}_i$. Thus

$$FG = M_1 \oplus \cdots \oplus M_s\,, \tag{3}$$

with each M_i a sum of (say m_i) irreducible components of the same isomorphism type. *Note:* by the Lemma, $i \neq j$ implies $M_i M_j = 0$.

LEMMA 1.2: *If $\pi_i : FG \to M_i \subseteq FG$ is the obvious projection, $\pi_i(\alpha) = \pi_i(1) \cdot \alpha$, for all $\alpha \in FG$.*

Proof.

$$\pi_i(1)\alpha = \sum_j \pi_i(1)\pi_j(\alpha) = \pi_i(1)\pi_i(\alpha) = \sum_j \pi_j(1)\pi_i(\alpha) = 1 \cdot \pi_i(\alpha)\,, \quad \text{q.e.d.}$$

It is customary to abbreviate $\pi_i(1) = e_i$. Since M_i is a left FG-module, it is obvious that $\pi_i(\alpha) = \alpha e_i$, that $e_i e_j = \delta_{ij} e_i$ (Kronecker's δ), and that $1 = e_1 + \cdots + e_s$. The force of the lemma is that the e_i are *central*. In particular, $(\alpha e_i)(\beta e_i) = \alpha\beta e_i$ shows each M_i to be a *ring* with unity e_i.

2. Characters. In this section, we keep the notation of the preceding one. In particular, $\mathcal{I}_1, \ldots, \mathcal{I}_s$ are the available isomorphism classes of irreducible FG-modules, and $e_1, \ldots, e_s$ are the corresponding central idempotents of FG. An irreducible L in $\mathcal{I}_i$ is annihilated by all e_j, except for e_i which acts on it as the identity. Let us once and for all choose a set $L_1, \ldots, L_s$ of representatives for $\mathcal{I}_1, \ldots, \mathcal{I}_s$.

Let $\Delta : G \to \mathrm{Aut}_F(M)$ be the representation associated with an FG-module M. If $\chi(\sigma)$ denotes the trace of $\Delta(\sigma)$, the map $\chi : G \to F$ is called the *character* of Δ or of M. We use the same name and notation for the associated linear functional $FG \to F$.

LEMMA 2.1: *The FG-modules M and M' have the same character if they are isomorphic. The converse holds for F of characteristic* 0.

Proof. Any isomorphism $T : M \to M'$ must satisfy $T\Delta(\sigma) = \Delta'(\sigma)T$, i.e., $\Delta'(\sigma) = T\Delta(\sigma)T^{-1}$, for all $\sigma \in G$; hence $\chi = \chi'$. In particular, each isomorphism class $\mathcal{I}_i$ corresponds to a single character χ_i.

Now imagine a decomposition $M = N_1 \oplus \cdots \oplus N_u$ into irreducibles. Then $\chi(e_i) = \mu_i d_i$, where μ_i is the multiplicity with which members of $\mathcal{I}_i$ occur among these components. If F has characteristic 0, this makes $\chi = \chi'$ imply $\mu_i = \mu_i'$, for all i, so that M is isomorphic to M', q.e.d.

The next lemma shows how to compute the central idempotents $e_1, \ldots, e_s$. Remember that $M_i = (FG)e_i$ splits into m_i irreducible components, so that its character equals $m_i\chi_i$.

LEMMA 2.2:
$$e_i = \frac{m_i}{n} \sum_{\sigma \in G} \chi_i(\sigma^{-1})\sigma \,. \tag{4}$$

Proof. Let χ_∞ be the character of FG itself. Then $\chi_\infty(1) = n$, and $\chi_\infty(\sigma) = 0$ whenever $1 \neq \sigma \in G$. For $\alpha = \sum_\tau a_\tau \tau$, this means that $\chi_\infty(\sigma^{-1}\alpha) = na_\sigma$. On the other hand, $\chi_\infty = \sum_j m_j\chi_j$ by (3), whence $na_\sigma = \sum_j m_j\chi_j(\sigma^{-1}\alpha)$.

For $\alpha = e_i$, this becomes $na_\sigma = \sum_j m_j\chi_j(\sigma^{-1}e_i) = m_i\chi_i(\sigma^{-1})$. The last equality is due to the fact that left multiplication by $\sigma^{-1}e_i$ annihilates M_j, for $i \neq j$, and acts on M_i like σ^{-1}; q.e.d.

Evaluating $\chi_j(e_i)$ in (4), while keeping in mind that e_i acts like I_{d_i} on L_i and like 0 on all the other L_j, we obtain the "first orthogonality relations":

$$\frac{1}{n} \sum_{\sigma \in G} \chi_i(\sigma^{-1})\chi_j(\sigma) = \begin{cases} 0 & \text{if } i \neq j \\ d_i/m_i & \text{if } i = j \,. \end{cases} \tag{5}$$

To get a handle on the total number s of irreducible characters, we study the centre $Z(FG)$. Breaking up G into its conjugacy classes $C_1, \ldots, C_r$, we let $\gamma_\nu \in FG$ stand for the sum over all $\sigma \in C_\nu$. Clearly, $\alpha = \sum_\sigma a_\sigma \sigma \in FG$ is central if and only if it is fixed under conjugation by all $\tau \in G$. This means that its coefficients a_σ must be constant on each C_ν, and hence α is linear combination of the γ_ν. It follows that $\gamma_1, \ldots, \gamma_r$ is a *basis* of $Z(FG)$. On the other hand, $e_1, \ldots, e_s$ is a linearly independent set in $Z(FG)$: any relation $c_1e_1 + \cdots + c_se_s = 0$ would yield $c_ie_i = 0$ when multiplied by e_i. Hence

$$s \leq r \quad \text{and} \quad n = m_1d_1 + \cdots + m_sd_s \,, \tag{6}$$

where d_i denotes the F-dimension of a typical L in $\mathcal{I}_i$. Together, these relations are helpful for tracking down the possible types of irreducible FG-modules.

Exercise: If F has characteristic 0, show that $m_i \mid n$. (Hint: The eigenvalues of any $\Delta(\sigma)$ are of the form ζ^ν, where ζ is a primitive n-th root of 1. Let V_i be the $\mathbf{Z}$-module generated by the elements $\zeta^\nu\sigma e_i$, for $\sigma \in G$ and $\nu = 1, \ldots, n$. Multiplying (4) by $(n/m_i)e_i$, obtain a relation which says that $(n/m_i)V_i \subseteq V_i$. Using determinants, conclude that n/m_i is the root of a certain monic polynomial over $\mathbf{Z}$.)

3. Matrices. This section is in three parts: an abstract examination of matrices, some consequences for the components M_i of FG in the sum (3), and finally another version of the orthogonality relations (5).

I. Let R be any ring, V a (left) R-module, $E = \mathrm{End}_R(V)$ its ring of endomorphisms. Then the ring $\mathcal{M}_m(E)$ of $m \times m$ matrices over E is naturally isomorphic to $\mathrm{End}_R(W)$, where $W = V \oplus \cdots \oplus V$ has m components. Indeed, a matrix (a_{ij}) with entries in E defines the endomorphism $\alpha : W \to W$ mapping $w = (v_1, \ldots, v_m)$ to the m-tuple whose i-th component is $\sum_j a_{ij} v_j$. Conversely, the matrix entry $a_{ij} \in E$ can be retrieved by following the obvious j-th injection $V \to W$ by a given $\alpha : W \to W$ and the i-th projection $W \to V$. Finally, it can be checked that the composite $\beta\alpha$ of two endomorphisms corresponds to the matrix product obtained by summing the composites $b_{ik} a_{kj}$ over k.

Let R^o the "opposite" of R, i.e., a ring with the same elements as R but with the order of multiplication reversed. R^o is naturally identifiable with the ring of right multiplications in R, and this, in turn, is canonically isomorphic to $\mathrm{End}_R(R)$, the endomorphisms of R as a left R-module.

LEMMA 3.1: *Suppose that R, as a left R-module, is isomorphic to the direct sum $V \oplus \cdots \oplus V$ of m copies of some R-module V. Then R is isomorphic to the ring $\mathcal{M}_m(E^o)$, where $E = \mathrm{End}_R(V)$.*

Proof. By the preceding discussion, $R^o \simeq \mathcal{M}_m(E)$. To finish the proof, we note that the matrix transpose yields an isomorphism $\mathcal{M}_m(E)^o \to \mathcal{M}_m(E^o)$, a verification we leave to the reader, q.e.d.

II. Recall from Section 1, that FG is the Cartesian product of rings $M_1, \ldots, M_s$, each M_i being the direct sum of m_i left ideals all isomorphic to a single L_i. Since L_i is irreducible, all its non-zero endomorphisms are invertible (their kernels must be trivial, their images all of L_i), and hence $\mathrm{End}_{FG}(L_i)^o$ is a division algebra D_i over F. Applying Lemma 3.1 to $R = M_i$, we therefore have a ring isomorphism

$$M_i \simeq \mathcal{M}_{m_i}(D_i) \tag{7}$$

for every $i = 1, \ldots, s$. Letting δ_i denote the F-dimension of D_i, we conclude moreover that

$$\dim_F M_i = m_i^2 \delta_i\,, \quad d_i = \dim_F L_i = m_i \delta_i\,, \quad \text{and} \quad n = m_1^2 \delta_1 + \cdots + m_s^2 \delta_s\,. \tag{8}$$

Since every element of any D_i generates a finite field extension of F, we have $D_i = F$ and $\delta_i = 1$ for all i, whenever F is algebraically closed.

III. The quotient d_i/m_i appearing in the orthogonality relations (5) has thus been unmasked as δ_i. Since characters are obviously constant on conjugacy classes we can rewrite these relations in the form

$$\frac{1}{n\delta_j} \sum_{\nu=1}^{r} \chi_i(C_\nu)\chi_j(C_\nu^*) h_\nu = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j\,, \end{cases} \tag{9}$$

with $h_\nu = |C_\nu|$ and $C_\nu^* = \{\sigma \mid \sigma^{-1} \in C_\nu\}$. This can be interpreted as saying that the identity matrix I_s is the product of the $s \times r$ matrix $\big(\chi_i(C_j)\big)$ and the $r \times s$ matrix $\big(\chi_j(C_i^*) h_i / n\delta_j\big)$, where i and j always denote the row and column indices, respectively. If these matrices are square, the product of the factors can be reversed. In other words,

$$\frac{h_i}{n} \sum_{\nu=1}^{s} \chi_\nu(C_i^*)\chi_\nu(C_j)/\delta_\nu = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j\,, \end{cases} \tag{10}$$

provided that $s = r$. These are the "second orthogonality relations".

The proviso $r = s$ is always satisfied if F is algebraically closed: in that case, each M_i is a full matrix ring over F, and $Z(FG) = Z(M_1) \oplus \cdots \oplus Z(M_s)$ is the Cartesian product of s copies of F. As a futher bonus, the δ_ν then disappear from the formula.