Lecture 12-4: Review, continued

December 4, 2024

I continue with review, recalling the classification of finitely generated modules over PIDs, its applications to matrices, and representation theory.

Let R be a PID. Any finitely generated module M over R is then a direct sum of quotients of R. More precisely, we can write M as a direct sum $\bigoplus_{i=1}^{m} R/(a_i)$, where the elements $a_i \in R$ can be chosen so that either $a_1|a_2|\cdots|a_m$ (elementary divisor decomposition; we allow $a_i = 0$ here) or $a_i = p_i^{n_i}$, where $p_i \in R$ is either prime or 0 and n_i is a positive integer (primary decomposition version). In the elementary divisor decomposition, the a_i are unique up to unit multiples; in the primary decomposition, the primes p_i are likewise unique up to unit multiples and the exponents are unique up to reordering exponents of the same prime. The module M is free over R if and only if it is torsion-free (so that $rm = 0$ for $r \in R, m \in M$ if and only if $r = 0$ or $m = 0$). In particular, any submodule of a free module is free and M is free if and only if it is projective. I noted last time that M (not now assumed finitely generated) is injective if and only if it is divisible as an R-module.

In particular, any finitely generated abelian group is a direct product of cyclic groups, some of which might have infinite order. The ones of finite order can either be arranged so the order of each divides that of the next *or* each has prime-power order (where the primes involved might or might not differ from one cyclic factor to the next). Any finite subgroup of the multiplicative group of a field (in particular, the full multiplicative group of a finite field) is cyclic.

Applying the classification to the case $R = K[x]$ (the ring of polynomials in one variable over a field K) and $M = V$ is a finite-dimensional vector space over K on which the variable x acts by a linear transformation T, we can rewrite V as the direct sum of proper quotients $R/(q_i)$ of R, taking the q_i to be monic polynomials such that either $q_1|q_2 \cdots$ or $q_i = p_i^{n_i}$ for some irreducible polynomial p_i. Choosing a basis of V for each quotient $R/(q_i)$ consisting of powers of x, we find that the matrix of T with respect to this basis is block diagonal with the block corresponding to the quotient $R/(q_i)$ equal to the companion matrix attached to q_i (ones below teh diagonal, negatives of the nonleading coefficients of q_i in the right column, all other entries 0). This is the rational canonical form of (any matrix of) T. If the basefield K contains all the eigenvalues of T, then we can replace this form by the Jordan form, in which the blocks have all diagonal entries equal and ones above the diagonal.

The minimal and characteristic polynomials of T are easy to read off from its rational canonical form: if the blocks are companion matrices of $q_1, \ldots, q_m$, then the minimal polynomial of T is the least common multiple of the q_i while its characteristic polynomial is the product of the q_i (up to sign). In particular, up to similarity, there are only finitely many matrices of a fixed size over a field K with a specified minimal polynomial, or with a specified characteristic polynomial. The transformation T (or the matrix of it with respect to any basis) is diagonalizable if and only if the minimal polynomial of T is the product of distinct linear factors. Also any square matrix over K is similar to its transpose.

Turning now to the representation theory of finite groups G, we begin with the basic definition that a representation of G (over a field K) is a homomorphism $\pi : G \to GL_n(K)$ for some n, where $GL_n(K)$ denotes the group of invertible $n \times n$ matrices over K. Two representations π, π', both with range in the same $GL_n(K)$, are equivalent if there is $x \in GL_n(K)$ with $\pi(g) = x\pi'(g)x^{-1}$ for all $g \in G$. Equivalently, one can speak of G-modules: these are finite-dimensional vector spaces V over K such that G acts on V by K-linear transformations. The group algebra KG, consisting by definition of all K-linear combinations $\sum_{g \in G} k_g g$ with the $k_g \in K$ with multiplication given by multiplication in G together with the distributive law, provides a handy ring R such that R-modules are the same thing as G-modules over K.

If the characteristic of the field K does not divide the order n of G, then any G-module V is a direct sum of irreducible G-modules W, none of them admitting any G-submodule apart from 0 and W, If moreover K is algebraically closed, then KG is isomorphic as a K-algebra to a direct sum of finitely many rings $M_i = M_{n_i}(K)$ of $n_i \times n_i$ matrices over K. Any irreducible G-module is then isomorphic to the space K^{n_i} of column vectors of length n_i over K for a unique index i, on which M_i acts by matrix multiplication and M_j acts by 0 for $j \neq i$. In particular, G has only finitely many irreducible representations up to equivalence; more precisely, the number of such representations equals the number of conjugacy classes in G.

Restricting for simplicity to the case $K = \mathbb{C}$, it turns out that any representation π of G is determined up to equivalence by its character χ, defined by $\chi(g) = \text{tr}\, \pi(g)$, where tr denotes the trace of a matrix. The characters χ, χ' of inequivalent irreducible representations π, π' satisfy the orthogonality relation $\sum_{g \in G} \chi(g)\bar{\chi}'(g) = 0$, where the bar denotes complex conjugation; if instead $\chi' = \chi$, then $\sum_{g \in G} \chi(g)\bar{\chi}(g) = n = |G|$. We also have orthogonality relations for the columns of a character table: if $g, h \in G$ are not conjugate in G, then $\sum_i \chi_i(g)\bar{\chi}_i(h) = 0$, where the sum takes place over the irreducible characters of G. If g and h are conjugate in G, then $\sum_i \chi_i(g)\bar{\chi}_i(h) = \sum_i \chi_i(g)\bar{\chi}_i(g) = \frac{n}{|c_g|}$, where $|c_g|$ denotes the size of the conjugacy class of g. The values $\chi(g)$ of any character are algebraic integers; more precisely, they are sums of roots of 1 in $\mathbb{C}$. The dimension d of any irreducible representation divides the order n of G.

If G is abelian, its representation theory is especially simple: all of its irreducible representations over $\mathbb{C}$ are one-dimensional and there are as many such representations as elements of G. Just as a warning, this is not true even for cyclic groups of order n if the basefield K does not contain n distinct nth roots of 1; over the rational field $\mathbb{Q}$, for example, irreducible representations of cyclic groups can have arbitrarily large degree.

Using characters one can show that if a finite group G has a nonidentity conjugacy class C whose order is a power of a prime, then G is not simple. From this it easily follows that any group whose order is the product of two prime powers is nonsimple (Burnside's $p^a q^b$ Theorem).

You should be familiar with small character tables like those of the symmetric group S_3, the dihedral group D_4 of order 8, and the alternating group A_4. Most of the entries in these tables can be worked out from the orthogonality relations, rather than actually having to compute traces.