Lecture 12-6: Preview of next quarter

December 6, 2024

I have reviewed most of the topics covered by the final exam, so in this last lecture I will give a preview of coming attractions for next quarter.

I will begin with field theory and Galois theory (Chapter 13 and 14 in Dummit and Foote); the latter is an especially beautiful combination of field theory and group theory. In it one attaches a finite group G to every finite field extension (that is, to every pair (K, L) such that K is a subfield of L and L is finite-dimensional as a vector space over K). In favorable circumstances the order of G matches the dimension of L over K and there is an inclusion-reversing bijection between subgroups of G and fields lying between K and L. The "favorable circumstances" here are quite strong, but they are satisfied in a very large number of examples.

As a totally unexpected consequence, I will derive a condition for a polynomial over a field to be solvable by radicals, meaning roughly that there are expressions for its roots involving nothing more than the field operations and taking *n*th roots for various *n*. It is important to note here that there is no a priori restriction on the roots involved; I am allowing the possibility of using 11th roots to solve cubic equations, for example. Nevertheless, there is a very strong negative answer to the question of whether every polynomial can be solved by radicals: not only is there no universal formula for doing so for any polynomial of degree at least five, but there are even particular polynomials *p*, very easy to write down explicitly, for which no formula expresses the roots just of *p*. There are also interesting and quite unexpected connections to classical problems of geometric constructions.

Solvability by radicals is clearly a field-theoretic property, having to do with roots of polynomials and how far one has to move beyond the fields generated by their coefficients to locate their roots. Nevertheless, Galois gave an amazing answer to the question of which polynomials are solvable by radicals in purely group-theoretic terms. Indeed, though some groups were known before Galois, it is not too much of a stretch to say that he invented group theory to settle this question. It was he who identified and named the group-theoretic property that characterizes solvability by radicals, calling it (naturally) solvability.

After presenting Galois theory I will turn my attention to the cohomology of finite groups, building on the homological algebra tools you have learned this quarter; this material appears in Chapter 17 of the text. Given a finite group G I will define its integral group algebra $\mathbb{Z}G$, which is an analogue over $\mathbb{Z}$ of the complex group algebra $\mathbb{C}G$ that you saw this quarter. The cohomology groups of G will be Ext groups attached to a pair of modules over $\mathbb{Z}G$. In dimensions one and two these groups have natural group-theoretic interpretations, which I will use to deduce group-theoretic information about G from knowledge of its cohomology. I will also give an alternative proof of one of the key steps in the proof of the Galois criterion for solvability of a polynomial by radicals; it turns out that this step can be proved using either canonical forms of matrices or group cohomology.

I will be spending the entire spring quarter on commutative algebra; as a warmup to this and a continuation of the classification of finitely generated modules over a PID, I will define a class of “almost PIDs” called Dedekind domains and develop their structural properties. I will concentrate on the most interesting examples, arising from extensions of $\mathbb{Q}$, but will treat general Dedekind domains in the spring, using additional tools from commutative algebras. This material appears in Chapter 16 of the text. Although not all Dedekind domains are PIDs, it turns out that there is a precise way to measure the failure of a Dedekind domain to be a PID, by means of something called its class group. This class group can be any abelian group in general, but for an important class of Dedekind domains arising in number theory it is finite. It provides an important insight into why early attempts to prove Fermat's famous Last Theorem failed and gives an inkling of what can be done to salvage some information from their faulty approaches.

With the structural theory of Dedekind domains in hand, I will classify finitely generated modules over such domains. This is similar to but somewhat more complicated than the corresponding classification over PIDs. It uses the theory of projective modules in an interesting way and points to a difference between free and torsion-free modules in general; by contrast, recall that a $\mathbb{Z}$-module is free if and only if it is projective, or if and only if it is torsion-free.

I will then give a brief account of Artinian rings and discrete valuation rings, following Chapter 16. If there is extra time I will start to get into commutative algebra (Chapter 15), getting a jump on the main material in the spring.