Lecture 2-3: Galois groups and central simple algebras

February 3, 2025

I wrap up the treatment of Galois theory with an account of the relationship between Galois groups and central simple algebras; the latter were defined and studied briefly in my second lecture on tensor products last term (on October 14).

Let F be a field of characteristic 0. Recall from last term that a central simple algebra over F is an algebra A containing a copy of F as its center and admitting no proper two-sided ideals, such that A is finite-dimensional over F. Last term I showed that if A and B are two such algebras, then so is their tensor product $A \otimes_F B$ and that $A \otimes_F A^o \cong M_n(F)$, the ring of $n \times n$ matrices over F, where n is the dimension of A over F. Here A^o is the opposite algebra of A (coinciding with A as an F-vector space but with multiplication such that if $a, b \in A^o$ then $ab = ba$, computed in A). Let M be an irreducible left A-module; such exists since for example A has a left ideal L of minimal nonzero dimension over F, and then $M = L$ has no proper left subideal.

Letting D be the ring $\hom_A(M, M)$ of A-endomorphisms of M, you showed in a homework problem last term that D is a division ring, which clearly contains F. Arguing as in the proof last term that the group algebra $\mathbb{C}G$ of a finite group G is a direct sum of matrix rings over $\mathbb{C}$, one shows that A is isomorphic to the ring $M_m(D)$ of $m \times m$ matrices over D for some m. The irreducible module M is in fact essentially unique, being isomorphic to any minimal nonzero left ideal L of A, or to the space D^m of column vectors over D of length m. Any finite-dimensional A-module is isomorphic to a direct sum of copies of M.

Now replace A by D, which is again central simple over F. Enlarge F to a maximal subfield K of D (one not contained in any other). The centralizer of K in D is then equal to K. Otherwise there is $x \in D$ commuting with K but not in it, which is necessarily algebraic over K; then K and x generate a subfield of D larger than K. We know by the above that $D \otimes_F D^o \cong M_n(F), n = [D : F]$. Passing to the smaller tensor product $D \otimes_F K$ we get the ring $\hom_K(D, D)$ of K-endomorphisms of D since $D \otimes_F D^o$ is the ring $\hom_F(D, D)$ of all F-endomorphisms of F and K is its own centralizer in D.

Computing dimensions over F we get $[D:F][K:F] = [D:K][K:F]^2 = [D:K]^2[K:F]$, whence $[D=K] = [K:F]$: the degree $[D:F] = n$ is necessarily a square r^2 and $r = [K:F] = [D:K]$. The field K is then a separable extension of F (since F has characteristic 0). Let L be its Galois closure and write $s = [L:K]$. Passing from D to the matrix ring $D' = M_s(D)$, we find that $L \subset M_s(K) \subset D'$ (by looking at the action of L on itself by K-linear transformations); also $[D':F] = r^2 s^2 = [D':L]^2$. Arguing as above with D and K, we see that L is a maximal subfield of D' and equal to its own centralizer in D'.

We are almost ready to bring in Galois theory. First we need

Theorem (Skolem-Noether)

Let B be a central simple F-algebra and A a simple algebra with F central in A. Given any two F-algebra homomorphisms $f, g : A \to B$ there is an invertible $b \in B$ with $g(a) = bf(a)b^{-1}$ for all $a \in A$. In particular, any F-automorphism of B is inner (given by conjugation by some $b \in B$).

Proof.

First suppose that $B = M_n(F)$. Since A is necessarily central simple over its center, it follows by above remarks that there is only one irreducible A-module up to isomorphism and any finite-dimensional A-module is a direct sum of copies of this module. But now the space F^n of column vectors over F becomes an A-module in two different ways, via the homomorphisms f and g. Since the dimension of F^n is the same in both module structures, they are isomorphic. The isomorphism is implemented by conjugation by some invertible $b \in B$, so we are done. In general, replacing B by $B \otimes_F B^o \cong M_n(F)$ and extending f, g to maps $f \otimes 1, g \otimes 1 : A \otimes_F B_o \to B \otimes_F B^o$, where 1 is the identity map on B^o, we deduce that $f \otimes 1, g \otimes 1$ are conjugate by some invertible $c \in B \otimes_F B^o$ centralizing $1 \otimes B^o$ (since both $f \otimes 1$ and $g \otimes 1$ fix $1 \otimes B^o$), so c lies in $B \otimes 1 \cong B$. This is the desired result. □

With notation as above, let G be the Galois group of L over F. Then L embeds in D' via the inclusion map and its composition with any $g \in G$, so there is an invertible element $e_g \in D'$ such that $e_g \ell e_g^{-1} = g.\ell$ for all $\ell \in L$. Arguing as in the proof that distinct automorphisms of a field are linearly independent as maps over that field, we see that the e_g are independent under left multiplication by L as g runs over G, whence they form a basis of D' as a left L-module. Note that the e_g are not uniquely determined, since each could be multiplied by some nonzero $\ell_g \in L$. Note also that we do not necessarily have $e_g e_h = e_{gh}$ for $g, h \in G$; instead we have $e_g e_h = \ell_{g,h} e_{gh}$ for some nonzero $\ell_{g,h} \in L$.

The upshot is that our central simple algebra D' is what is sometimes called the smash product of L and G (and sometimes denoted $L * G$). It is also called a crossed product. As a left L-vector space, it is isomorphic to the group algebra LG. It also carries a natural G-action such that $g.e_h = e_{gh}$ and is isomorphic to LG as a G-module under this action. But it is not isomorphic to LG as a ring and L does not lie in its center.

Conversely, given any Galois extension L of a field F with Galois group G and an element $\ell_{g,h} \in L^*$ for every $g, h \in G$, we can define an algebra A to have basis $\{e_g : g \in G\}$ as a left L-vector space, while $e_g \ell e_g^{-1} = g.\ell$ for $\ell \in L, g \in G, e_g, e_h = \ell_{g,h} e_{gh}$ for $g, h \in G$. In order to be sure that A is associative, we must choose the $\ell_{g,h}$ suitably; we will see later that the condition amounts to a cocycle condition (which is always satisfied, for example, if we set $\ell_{g,h} = 1$ for all g, h). The change in the $\ell_{g,h}$ that results when e_g is replaced by $\ell_g e_g$ for some $\ell_g \in L^*$ amounts to a change by a coboundary. Whenever the algebra A defined by these relations is associative, it turns out to be central simple over F, by an easy argument (though typically it will not be a division algebra).

As an example, we now see that the division ring $\mathbb{H}$ of quaternions, which has dimension 4 over its center $\mathbb{R}$, predictably must contain a copy of the only proper finite extension of $\mathbb{R}$, namely $\mathbb{C}$, as well as an element such that conjugation by preserves the copy of $\mathbb{C}$ om $\mathbb{H}$, acting on it by complex conjugation (the unique nontrivial element of the Galois group G of $\mathbb{C}$ over $\mathbb{R}$). Here the element $e_1 \in \mathbb{H}$ corresponding to the identity element of G can be taken to be 1 (indeed, this can always be done in any crossed product); the other element e_2 can be taken to be j. We have $e_2^2 = -1 \in \mathbb{C}$. Had we taken $e_2^2 = 1$ instead, we would still have gotten a central simple algebra over $\mathbb{R}$, but not a division ring.

It is known, by the way, that even if the basefield F has characteristic $p > 0$, any central simple division algebra D over F admits a maximal subfield K separable over F, so that a suitable matrix ring $M_s(D)$ can always be realized as a crossed product. It is also known that D itself need not be a crossed product; the passage to a matrix ring $M_s(D)$ is sometimes essential.

I will return to central simple algebras over a field next month, applying the machinery of (Galois) group cohomology to them.