Math 154, Frobenius' surjectivity theorem

1. Motivation

Let A be a Dedekind domain with fraction field F, and F'/F a finite Galois extension with Galois group G. Let A' be the integral closure of A in F' (so A' is a finitely generated A-module, stable under the G-action) and let $\mathfrak{m}'$ be a maximal ideal of A' and $\mathfrak{m} = \mathfrak{m}' \cap A$ the maximal ideal that it lives over in A (so $\mathfrak{m}'$ contains $\mathfrak{m}A'$ and hence appears in the factorization of $\mathfrak{m}A'$). Recall that we define the *decomposition group* $D(\mathfrak{m}'|\mathfrak{m}) \subseteq G$ to consist of all $\sigma \in G$ such that $\sigma(\mathfrak{m}') = \mathfrak{m}'$. Recall that we saw in class that G acts on the set of maximal ideals of A' over $\mathfrak{m}$, even transitively. Thus, we can say that $D(\mathfrak{m}'|\mathfrak{m})$ is the stabilizer at $\mathfrak{m}'$ of the G-action on the set of primes of A' over $\mathfrak{m}$.

We also saw in class that elements $\sigma \in D(\mathfrak{m}'|\mathfrak{m})$ naturally induces automorphisms of the field $A'/\mathfrak{m}'$ over the field $A/\mathfrak{m}$ by the rule $\overline{\sigma}(a' \bmod \mathfrak{m}') = \sigma(a') \bmod \mathfrak{m}'$. (This "makes sense" because if $a'_1 - a'_2 \in \mathfrak{m}'$ then $\sigma(a'_1) - \sigma(a'_2) \in \sigma(\mathfrak{m}') = \mathfrak{m}'$.) We see from this definition that $\overline{\sigma\tau} = \overline{\sigma} \circ \overline{\tau}$, so $\overline{\sigma^{-1}}$ is the inverse to $\overline{\sigma}$ and more generally the map

$$D(\mathfrak{m}'|\mathfrak{m}) \to \mathrm{Aut}_{A/\mathfrak{m}}(A'/\mathfrak{m}') \tag{1}$$

is a homomorphism of (finite) groups. The kernel $I(\mathfrak{m}'|\mathfrak{m})$ is called the *inertia group* at $\mathfrak{m}'$, and by definition it consists of those $\sigma \in G$ that fix $\mathfrak{m}'$ (i.e., lie in $D(\mathfrak{m}'|\mathfrak{m})$) *and* satisfy the additional requirement that $\overline{\sigma}$ is the identity automorphism; i.e., $\overline{\sigma}(x) = x$ for all $x \in A'/\mathfrak{m}'$. In particular, if $\sigma \in I(\mathfrak{m}'|\mathfrak{m})$ then $\sigma(a') \equiv a' \bmod \mathfrak{m}'$ for all $a' \in A'$. The converse is also true: if $\sigma \in G$ satisfies $\sigma(a') \equiv a' \mathfrak{m}'$ for all $a' \in A'$ then necessarily $\sigma \in I(\mathfrak{m}'|\mathfrak{m})$. The only thing we have to check is that necessarily $\sigma \in D(\mathfrak{m}'|\mathfrak{m})$, which is to say that $\sigma(\mathfrak{m}') = \mathfrak{m}'$. Since containments between maximal ideals are necessarily equalities (why?), it is the same to say that $\sigma(\mathfrak{m}') \subseteq \mathfrak{m}'$, and that in turn follows from our congruence hypothesis since if $a' \equiv 0 \bmod \mathfrak{m}'$ then the congruence hypothesis implies that $\sigma(a') \equiv \sigma(0) = 0 \bmod \mathfrak{m}'$. On HW8, you will compute several examples of decomposition groups and inertia groups for Galois extensions of number fields.

The map (1) is very interesting, because it relates a group of automorphisms of F' to a group of automorphisms of $A'/\mathfrak{m}'$. For instance, if A is the ring of integers of a number field then we are relating some automorphisms in characteristic 0 to automorphisms in characteristic p! It is a fundamental fact, to be proved below, that (1) is always *surjective*; i.e., all $A/\mathfrak{m}$-automorphisms of $A'/\mathfrak{m}'$ *lift* to automorphisms of F' over F (fixing $\mathfrak{m}'$). This is the result that we aim to prove in this handout, following a classical argument of Frobenius. In class we saw that this has striking consequences when the residue fields are finite and $\mathfrak{m}$ is unramified in F'.

2. Main result

Here is Frobenius' theorem:

Theorem 2.1 (Frobenius)**.** *The natural map* (1) *is surjective.*

Proof. Since A' is finitely generated as an A-module, we may choose a finite A-linear spanning set $\{a'_1, \ldots, a'_N\}$ (i.e., $A' = \sum Aa'_i$); beware that $\{a'_i\}$ may not be A-linearly independent (i.e., perhaps not an A-basis of A'; there may be no A-basis at all). We pick $g \in \mathrm{Aut}_{A/\mathfrak{m}}(A'/\mathfrak{m}')$ and seek $\sigma \in G$ satisfying

$$\sigma(a') \bmod \mathfrak{m}' = g(a' \bmod \mathfrak{m}') \tag{2}$$

for all $a' \in A'$. Indeed, by taking $a' \in \mathfrak{m}'$ it would follow from (2) that $\sigma(a') \bmod \mathfrak{m}'$ vanishes for such a', which is to say that $\sigma(\mathfrak{m}') \subseteq \mathfrak{m}'$, and so $\sigma(\mathfrak{m}') = \mathfrak{m}'$. Thus, (2) would force $\sigma \in D(\mathfrak{m}'|\mathfrak{m})$, and then (2) says exactly that $\overline{\sigma} = g$ (i.e., (1) carries σ to g).

To establish (2), note that both sides have the same A-linear behavior in a' (since g is $A/\mathfrak{m}$-linear and the hypothetical σ is A-linear). That is, to prove (2) for some $\sigma \in G$ it is sufficient to consider just a' varying through the A-linear spanning set $\{a'_i\}$. In other words, we seek $\sigma \in G$ satisfying

$$\sigma(a'_i) \bmod \mathfrak{m}' = g(a'_i \bmod \mathfrak{m}')$$

for all $1 \leq i \leq N$. Now comes the brilliant idea: consider the multivariable polynomial

$$h(Y, X_1, \ldots, X_N) = \prod_{\sigma \in G} (Y - \sum_i \sigma(a_i')X_i) \in A'[Y, X_1, \ldots, X_N].$$

Note that although the definition of h takes place over A', under the natural G-action on polynomials over A' via G-action on the coefficients the polynomial h is *invariant*. Indeed, this G-action is compatible with multiplication and addition of polynomials (why?), and it clearly permutes the factors in the definition of h, so it carries h back to itself. Thus, the coefficients of h really lie in $(A')^G = A' \cap {F'}^G = A' \cap F = A$! So we may and do consider h as an element of $A[Y, X_1, \ldots, X_N]$ (though in this ring we cannot express h as a product in the way that we do over A', much as in Galois theory where we can express a separable polynomial usefully as a product of linear terms over a splitting field but typically not over the original ground field).

The polynomial $h \in A[Y, X_1, \ldots, X_N]$ satisfies the identity

$$h(\sum a_i' X_i, X_1, \ldots, X_N) = 0$$

in $A'[X_1, \ldots, X_N]$ since over A' the definition of h involves a factor of $Y - \sum a_i' X_i$ (corresponding to $\sigma = 1$). Passing to the reduction modulo $\mathfrak{m}'$ and letting $\overline{a}' = a' \bmod \mathfrak{m}'$ in $A'/\mathfrak{m}'$ for $a' \in A'$, we likewise have that the reduction $\overline{h} \in (A/\mathfrak{m})[Y, X_1, \ldots, X_N]$ satisfies

$$\overline{h}(\sum \overline{a}_i' X_i, X_1, \ldots, X_N) = 0 \tag{3}$$

in $(A'/\mathfrak{m}')[X_1, \ldots, X_N]$. (Make sure you understand this step.) The key point is that in this latter identity, the polynomial $\overline{h}$ has its coefficients in the subfield $A/\mathfrak{m} \subseteq A'/\mathfrak{m}'$ (since h has its coefficients in the subring $A \subseteq A'$). Thus, if we let the $A/\mathfrak{m}$-automorphism g of $A'/\mathfrak{m}'$ act on $(A'/\mathfrak{m}')[X_1, \ldots, X_N]$ through its action on coefficients then this action is a compatible with addition and multiplication of polynomials (why?) and has no effect on the coefficients of $\overline{h}$ (!), so applying g to both sides of (3) yields that

$$\overline{h}(\sum g(\overline{a}_i') X_i, X_1, \ldots, X_N) = 0$$

in $(A'/\mathfrak{m}')[X_1, \ldots, X_N]$.

But by the construction of h as a product over A', we see that $\overline{h}$ viewed over $A'/\mathfrak{m}'$ is also a product:

$$\overline{h}(Y, X_1, \ldots, X_N) = \prod_{\sigma \in G} (Y - \sum \overline{\sigma(a_i')} X_i)$$

in $(A'/\mathfrak{m}')[Y, X_1, \ldots, X_N]$. Hence, substituting $\sum_i g(\overline{a}_i')X_i$ in place of Y in this identity yields that

$$0 = \overline{h}(\sum g(\overline{a}_i')X_i, X_1, \ldots, X_N) = \prod_{\sigma \in G} (\sum_i g(\overline{a}_i')X_i - \sum_i \overline{\sigma(a_i')} X_i, X_1, \ldots, X_N)$$

in $(A'/\mathfrak{m}')[X_1, \ldots, X_N]$. In other words, we have shown that the linear polynomials

$$\sum_i (g(\overline{a}_i') - \overline{\sigma(a_i')}) X_i$$

over the field $A'/\mathfrak{m}'$ for varying $\sigma \in G$ have product equal to 0 (as a multivariable polynomial)! This forces one of these linear polynomials to vanish, and that in turn happens if and only if the coefficients all vanish. In other words, for some $\sigma \in G$ we must have $\overline{\sigma(a_i')} = g(\overline{a}_i')$ for all i. But that is precisely the collection of equalities which we have seen is sufficient to deduce (2), so we are done. ■