Michiel Kosters - Mathematisch Instituut, Universiteit Leiden
`mkosters@math.leidenuniv.nl`, May 16, 2011

Groups acting on rings - a theorem of Tate

1. Introduction

In this talk we would like to present a proof of a theorem of Tate, which is very elegant and gives short proofs of some useful facts.

2. The theorem

Let G be a group which has a compact topology acting on a ring A with a continuous action when A is endowed with the discrete topology through ring morphisms. This means that the map $G \times A \to A$ is continuous. Remark that for $a \in A$ the map $G \times \{a\} \to A$ is continuous and the image is compact as G is compact. This means that all orbits under the action of G are finite.

Examples 2.1. Let G be a finite group acting on a ring A. Then G is compact under the discrete topology and the action is automatically continuous. Just think for example of a Galois group acting on the ring of integers of a number field.

Let K be a field and let $G = \mathrm{Gal}(\overline{K}/K)$, the absolute Galois group of K (where $\overline{K}$ is the separable closure of K). This G has a natural topology (profinite topology) and it is a compact group under this topology. This G acts naturally on $\overline{K}$ (or on other objects) and this action is continuous.

Theorem 2.2 (Tate). *Let (G, A) be as above. Let R be a domain and let $f, f' : A \to R$ be ring morphisms. Suppose that $f|_{A^G} = f'|_{A^G}$, then there is a $g \in G$ such that $f' = f \circ g$.*

Proof. Extend the action of G to $A[Y][X]$ by letting G act on the coefficients. Let $f_0 \in A[Y]$. We extend $f, f' : A[Y][X] \to R[Y][X]$ by $X \mapsto X$, $Y \mapsto Y$. Then consider the polynomial $h = \prod_{h' \in Gf_0}(X - h') \in A^G[Y][X]$. We have

$$\prod_{h' \in Gf_0}(X - f(h')) = f(h) = f'(h) = \prod_{h' \in Gf_0}(X - f'(h')).$$

As R and hence $R[Y]$ are domains, we can compare the roots and conclude that there is a $g \in G$ such that $f'(f_0) = f(g(f_0))$. We see that for any finite $E \subseteq A$, there is a $g \in G$ such that $f'|_E = f \circ g|_E$ (take a polynomial with the elements of E as coefficients).

Now let $E \subseteq A$ be finite and consider $G_E = \{g \in G : f'|_E = f \circ g|_E\}$, which is non-empty by the above observations. We claim that G_E is closed in G. Indeed for $e \in E$ we can consider the following continous maps, whose composition is continous:

$$G \xrightarrow{(f(e),\mathrm{id},e)} R \times G \times A \xrightarrow{(\mathrm{id},(G\times A \to A))} R \times A \xrightarrow{(\mathrm{id},f')} R \times R \xrightarrow{-} R$$

whose composition σ maps g to $\sigma(g) = f(e) - f'(g(e))$. Hence $\sigma^{-1}(0) = G_{\{e\}}$ is closed. We have $G_E = \bigcap_{e \in E} G_{\{e\}}$, which is closed as well. Similarly for finite sets $E_1, \ldots, E_n$ we have $\bigcap_{i=1}^n G_{E_i} = G_{\bigcup_{i=1}^m E_i} \neq \emptyset$. By compactness of G we see that

$G_A = \{g \in G : f = f'\} = \bigcap_{E \subseteq A, E \text{ finite}} G_E \neq \emptyset$. This means that there is a $g \in G$ such that $f' = f \circ g$. □

Example 2.3. If one looks at the proof of the main theorem, one sees that one doesn't really use all the hypotheses of the theorem. The theorem holds for example also for the ring $\{f = \sum_i a_i x^i \in \mathbf{Z}[X] : 2|a_1\} \subsetneq \mathbf{Z}[X]$ with G acting trivially.

3. Corollaries

We can now deduce some nice results from the above theorem.

Corollary 3.1. *Suppose that (G, A) is as above. Let $\mathfrak{p} \subset A^G$ be prime. Then G acts transitively on the primes of A lying above $\mathfrak{p}$.*

Proof. Let $\mathfrak{q}, \mathfrak{q}' \subset A$ be primes lying above $\mathfrak{p}$. We will now construct two maps from A to $\overline{Q(A^G/\mathfrak{p})}$. The first maps $f : A \to A/\mathfrak{q} \to Q(A/\mathfrak{q}) \to \overline{Q(A^G/\mathfrak{p})}$, where we use that the extension $Q(A/\mathfrak{q}) \supseteq Q(A^G/\mathfrak{p})$ is algebraic (which follows as the orbits are finite) where the last map is the identity on $A^G/\mathfrak{p}$. Similarly one defines another map $f' : A \to A/\mathfrak{q}' \to \overline{Q(A^G/\mathfrak{p})}$. Both maps agree on A^G. Theorem 2.2 says that there is a $g \in G$ such that $f' = fg$. But taking kernels gives $\mathfrak{q} = \text{Ker}(f') = \text{Ker}(fg) = g^{-1}(\text{Ker}(f)) = g^{-1}\mathfrak{q}'$. So $g\mathfrak{q} = \mathfrak{q}'$, which finishes the proof. □

Example 3.2. Let $K \supseteq \mathbf{Q}$ be a number field which is Galois over $\mathbf{Q}$. Then G acts transitively on the primes of K (of $\mathcal{O}_K$) lying above a prime of $\mathbf{Z}$. One can also take $\overline{Q} \supset \mathbf{Q}$ and the above corollary still holds!

Example 3.3. Some conditions on G and the action of A on G are needed to make the above corollary valid. Consider the ring $A = \mathbf{F}_2[x_i : i \in \mathbf{Z}]$ with $G = \mathbf{Z}$ action with $n(x_i) = x_{i+n}$. One easily sees that $A^G = \mathbf{Z}/2\mathbf{Z}$, but that not all prime ideals of A lie in the same G-orbit. Indeed, prime ideals can have different residue fields (such as $\mathbf{F}_2, \mathbf{F}_4, \ldots$).

Now we will prove another familiar lemma (which you have seen in number theory).

Corollary 3.4. *Let (G, A) be as above. Let $\mathfrak{q} \subset A$ be a prime lying above a prime $\mathfrak{p} \subset A^G$. Let $G_{\mathfrak{q}/\mathfrak{p}} = \{g \in G : g(\mathfrak{q}) = \mathfrak{q}\}$. Let $l = Q(A/\mathfrak{q})$ and let $k = Q(A^G/\mathfrak{p})$. Then the natural map $G_{\mathfrak{q}/\mathfrak{p}} \to \text{Aut}_k(l)$ is surjective.*

Proof. Let $\sigma \in \text{Aut}_k(l)$. Consider the natural map $f : A \to Q(A/\mathfrak{q}) = l$ which restricts to the natural map $A^G \to Q(A^G/\mathfrak{p}) = k$. Let $f' = \sigma f$. Now apply Lemma 2.2 to see that there is a $g \in G$ with $\sigma f = fg$. But then for $a \in A$ we have

$$g \circ (f(a)) = f(g(a)) = \sigma f(a).$$

This means that g maps to σ. □

Of course there are other uses of this lemma (say in the theory of Galois algebras), but we will not discuss these.