MODERN ALGEBRA (MATH 210) THANKSGIVING LEFTOVERS: PROOF OF TUESDAY'S THEOREM

RAVI VAKIL

Here is the proof of the theorem that I was in the process of proving at the end of class.

Theorem. If $\sigma_1, \ldots, \sigma_n$ is a *group* of automorphisms of E, and if F is the fixed field, then $[E : F] = n$. In particular, E/F is Galois.

Proof. We use linear algebra again. Suppose $[E : F] \geq n + 1$. Say σ_1 is the identity. Then let $\alpha_1, \ldots, \alpha_{n+1}$ be elements of E that are linearly independent with respect to F. By linear algebra, there is a nontrivial solution $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ in E to the system of equations

$$\begin{aligned} x_1\sigma_1(\alpha_1) + x_2\sigma_1(\alpha_2) + \cdots + x_{n+1}\sigma_1(\alpha_{n+1}) &= 0 \\ x_1\sigma_2(\alpha_1) + x_2\sigma_2(\alpha_2) + \cdots + x_{n+1}\sigma_2(\alpha_{n+1}) &= 0 \\ &\vdots \\ x_1\sigma_n(\alpha_1) + x_2\sigma_n(\alpha_2) + \cdots + x_{n+1}\sigma_n(\alpha_{n+1}) &= 0. \end{aligned}$$

The solution can't lie in F (i.e. all x_i can't lie in F) or else the first equation would be a dependence over F.

Among all nontrivial solutions $(x_1, \ldots, x_n)$, we choose one with the least number of nonzero elements. We'll get a contradiction out of this. We may suppose this solution is $(a_1, \ldots, a_r, 0, \ldots, 0)$, where the first r are non-zero. Also, dividing by a_r, we may assume $a_r = 1$. So we have:

$$\begin{aligned} a_1\sigma_1(\alpha_1) + a_2\sigma_1(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0 \\ a_1\sigma_2(\alpha_1) + a_2\sigma_2(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0 \\ &\vdots \\ a_1\sigma_n(\alpha_1) + a_2\sigma_n(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0. \end{aligned} \tag{1}$$

Note that $r \neq 1$. We may also assume a_1 is in E, but not in F (as not all a_i can lie in F, as observed above). Thus there is an automorphism σ_k for which $\sigma_k(a_1) \neq a_1$. Apply σ_k to

Date: Tuesday, November 26, 2002. *Revised Dec. 5, patching an error caught by Oren.*

(1) to get

$$\begin{aligned}
\sigma_k(a_1)\sigma_k\sigma_1(\alpha_1) + \sigma_k(a_2)\sigma_k\sigma_1(\alpha_2) + \cdots + \sigma_k\sigma_1(\alpha_r) &= 0 \\
\sigma_k(a_1)\sigma_k\sigma_2(\alpha_1) + \sigma_k(a_2)\sigma_k\sigma_2(\alpha_2) + \cdots + \sigma_k\sigma_1(\alpha_r) &= 0 \\
&\vdots \\
\sigma_k(a_1)\sigma_k\sigma_n(\alpha_1) + \sigma_k(a_2)\sigma_k\sigma_n(\alpha_2) + \cdots + \sigma_k\sigma_1(\alpha_r) &= 0.
\end{aligned}$$

Using the fact that $\sigma_1, \ldots, \sigma_n$ form a group (this is where we use the hypothesis!), we see that $\sigma_k \cdot \sigma_1, \ldots, \sigma_k \cdot \sigma_2, \ldots, \sigma_k \cdot \sigma_n$ is a permutation of $\sigma_1, \ldots, \sigma_k$. Thus we can rearrange the rows to get

$$\begin{aligned}
\sigma_k(a_1)\sigma_1(\alpha_1) + \sigma_k(a_2)\sigma_1(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0 \\
\sigma_k(a_1)\sigma_2(\alpha_1) + \sigma_k(a_2)\sigma_2(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0 \\
&\vdots \\
\sigma_k(a_1)\sigma_n(\alpha_1) + \sigma_k(a_2)\sigma_n(\alpha_2) + \cdots + \sigma_1(\alpha_r) &= 0.
\end{aligned}$$

Subtracting these from (1), we get

$$\begin{aligned}
(a_1 - \sigma_k(a_1))\sigma_1(\alpha_1) + (a_2 - \sigma_k(a_2))\sigma_1(\alpha_2) + \cdots + 0\sigma_1(\alpha_r) &= 0 \\
(a_1 - \sigma_k(a_1))\sigma_2(\alpha_1) + (a_2 - \sigma_k(a_2))\sigma_2(\alpha_2) + \cdots + 0\sigma_1(\alpha_r) &= 0 \\
&\vdots \\
(a_1 - \sigma_k(a_1))\sigma_n(\alpha_1) + (a_2 - \sigma_k(a_2))\sigma_n(\alpha_2) + \cdots + 0\sigma_1(\alpha_r) &= 0.
\end{aligned}$$

Thus we have a solution with a fewer number of nonzero entries. Contradiction! □

E-mail address: vakil@math.stanford.edu