SECTION 50, PROBLEM 22

SEBASTIAN CASALAINA-MARTIN

Abstract. Here is a solution to the problem.

Introduction

Lemma 0.1 (Section 50, Problem 22)**.** *Let F be a field and let $f(x) \in F[x]$ be a polynomial. If E is a splitting field for $f(x)$ over F, then $G(E/F)$ is isomorphic to a subgroup of the group of permutations on the set of distinct roots of $f(x)$ in E.*

Proof. Let $n = \deg(f)$. Let us fix an algebraic closure $\bar{F}$ and consider all extensions to be subfields of $\bar{F}$. We may assume without loss of generality that $f(x)$ is monic. Now let $f(x) = f_1(x) \dots f_r(x)$ be a factorization of $f(x)$ into (monic) irreducibles. Note that the roots of $f(x)$ in $\bar{F}$ are in bijection with the roots of $f_1(x), \dots, f_r(x)$ in $\bar{F}$. Let us list these roots as say $\{\alpha_1, \dots, \alpha_m\} \subseteq \bar{F}$ for some $m \leq n$.

Our goal is to show that there is an injective homomorphism

$$\Phi : G(E/F) \to \Sigma_m.$$

(Σ_m is the group of permutations of $\alpha_1, \dots, \alpha_m$.)

To begin, let us observe that for $\sigma \in G(E/F)$ we have $\sigma(\alpha_i) \in \{\alpha_1, \dots, \alpha_m\}$ for all $i = 1, \dots, m$. Indeed, we have seen that α_i is a root of (at least) one of the $f_1(x), \dots, f_r(x)$; let us say it is a root of $f_j(x)$. Now given $\sigma \in G(E/F)$, we get by restriction a homomorphism

$$\sigma|_{F(\alpha_i)} : F(\alpha_i) \to E \subseteq \bar{F}$$

fixing F. We have seen in our theorem on simple extensions that such homomorphisms send roots of the irreducible polynomial $f_j(x) = \mathrm{Irr}(\alpha_i, F)$ to other roots of $f_j(x)$, which, as we mentioned above, are in the set $\{\alpha_1, \dots, \alpha_m\}$. Thus $\sigma(\alpha_i) = \sigma|_{F(\alpha_i)}(\alpha_i) \in \{\alpha_1, \dots, \alpha_m\}$. Moreover, from the fact that σ is an isomorphism, we can conclude that $\sigma(\alpha_i) \neq \sigma(\alpha_j)$ for $i \neq j$.

Now let us define Φ. For $\sigma \in G(E/F)$ we set

$$\Phi(\sigma) := \begin{bmatrix} \alpha_1 & \dots & \alpha_m \\ \sigma(\alpha_1) & \dots & \sigma(\alpha_m) \end{bmatrix}$$

From the paragraph above, this is indeed a permutation, and so we have defined a map of sets. Let us check that it is a homomorphism. Given $\sigma, \tau \in G(E/F)$, we have

$$\Phi(\tau \circ \sigma) = \begin{bmatrix} \alpha_1 & \dots & \alpha_m \\ \tau \circ \sigma(\alpha_1) & \dots & \tau \circ \sigma(\alpha_m) \end{bmatrix}$$

$$= \begin{bmatrix} \alpha_1 & \dots & \alpha_m \\ \tau(\alpha_1) & \dots & \tau(\alpha_m) \end{bmatrix} \circ \begin{bmatrix} \alpha_1 & \dots & \alpha_m \\ \sigma(\alpha_1) & \dots & \sigma(\alpha_m) \end{bmatrix} = \Phi(\tau) \circ \Phi(\sigma),$$

Date: April 9, 2010.

and thus Φ is a homomorphism.

Now we will show that Φ is injective. So suppose that $\Phi(\sigma)$ is the identity permutation. Then we must show that σ is the identity automorphism of E. We can do this using induction by observing that $E = F(\alpha_1, \ldots, \alpha_m)$. Indeed, we know that σ acts by the identity on F. Now assume that we have shown that σ acts by the identity on $F(\alpha_1, \ldots, \alpha_k)$ for all $0 \leq k \leq N$. We will show it acts by the identity on $F(\alpha_1, \ldots, \alpha_{N+1})$. To do this, we view $F(\alpha_1, \ldots, \alpha_{N+1}) = F(\alpha_1, \ldots, \alpha_N)(\alpha_{N+1})$. By assumption σ acts by the identity on α_{N+1}, and by induction, it acts by the indentity on $F(\alpha_1, \ldots, \alpha_N)$. From our theorem on simple extensions (or by an easy direct argument), we have that σ acts by the identity on $F(\alpha_1, \ldots, \alpha_{N+1})$.

Thus, in conclusion, $\Phi : G(E/F) \to \Sigma_m$ is an injective homomorphism. $\square$

University of Colorado at Boulder, Department of Mathematics, Campus Box 395, Boulder, CO 80309-0395, USA

E-mail address: casa@math.colorado.edu