

# Galois Theory Problem Set 1

Austin Mohr

October 12, 2009

## 1 Problem 5

**Proposition 1.1.** *Let  $\mathbf{E}$  and  $\mathbf{F}$  be fields.  $\mathbf{E}$  is an algebraic closure of  $\mathbf{F}$  if and only if  $\mathbf{E}$  is an algebraic extension of  $\mathbf{F}$  and, for every algebraic extension  $\mathbf{K}$  of  $\mathbf{F}$ , there is an embedding of  $\mathbf{K}$  into  $\mathbf{E}$  that fixes each element of  $\mathbf{F}$ .*

*Proof.* ( $\Rightarrow$ ) Suppose that  $\mathbf{E}$  is an algebraic closure of  $\mathbf{F}$ . Let  $\mathbf{K}$  be any algebraic extension of  $\mathbf{F}$ . We know that  $\mathbf{K}$  itself has an algebraically closed extension (call it  $\overline{\mathbf{K}}$ ). Now,  $\overline{\mathbf{K}}$  is also an algebraic extension of  $\mathbf{F}$  that is algebraically closed, and so  $\overline{\mathbf{K}}$  is an algebraic closure of  $\mathbf{F}$ . By the uniqueness of algebraic closures, we have that  $\mathbf{E} \cong \overline{\mathbf{K}}$ .

Next, we seek an embedding of  $\mathbf{K}$  into  $\mathbf{E}$  that fixes each element of  $\mathbf{F}$ . To this end, define the functions

$f : \mathbf{K} \rightarrow \overline{\mathbf{K}}$  the natural embedding of  $\mathbf{K}$  into  $\overline{\mathbf{K}}$ ; and

$\phi : \overline{\mathbf{K}} \rightarrow \mathbf{E}$  the isomorphism between  $\overline{\mathbf{K}}$  and  $\mathbf{E}$ .

The monomorphism  $f$  fixes  $\mathbf{K}$  (and so fixes  $\mathbf{F}$ ) in  $\overline{\mathbf{K}}$  and the isomorphism identifies isomorphic copies of  $\mathbf{F}$  in  $\overline{\mathbf{K}}$  and  $\mathbf{E}$ . Therefore, the function  $\phi \circ f$  is the desired embedding of  $\mathbf{K}$  into  $\mathbf{E}$ .

( $\Leftarrow$ ) Suppose that  $\mathbf{E}$  is an algebraic extension of  $\mathbf{F}$  and, for every algebraic extension  $\mathbf{K}$  of  $\mathbf{F}$ , there is an embedding of  $\mathbf{K}$  into  $\mathbf{E}$  that fixes each element of  $\mathbf{F}$ . In particular, take  $\mathbf{K}$  to be the splitting field of  $\mathbf{F}$ . By hypothesis, there is an embedding of  $\mathbf{K}$  into  $\mathbf{E}$  that fixes  $\mathbf{F}$ . Identifying  $\mathbf{K}$  with its isomorphic copy in  $\mathbf{E}$ , we see that every polynomial in  $\mathbf{F}[x]$  splits in  $\mathbf{E}$  (since it splits in  $\mathbf{K}$ ), and so  $\mathbf{E}$  is in fact an algebraic closure of  $\mathbf{F}$ .  $\square$

## 2 Problem 6

**Proposition 2.1.** *Let  $\mathbf{E}$  and  $\mathbf{F}$  be fields. If  $\mathbf{E}$  extends  $\mathbf{F}$  and  $[\mathbf{E} : \mathbf{F}] = 2$ , then  $\mathbf{E}$  is a normal extension of  $\mathbf{F}$ .*

*Proof.* Let  $f(x) \in \mathbf{F}[x]$  be irreducible over  $\mathbf{F}$  with a root  $\alpha \in \mathbf{E}$ . Denote the minimal polynomial of  $\alpha$  over  $\mathbf{F}$  by  $\mu_\alpha(x)$ . We know that

$$\begin{aligned} \alpha \text{ is a root of } f(x) &\Rightarrow \mu_\alpha(x) \text{ divides } f(x) \\ &\Rightarrow \mu_\alpha(x) = f(x) \quad (\text{since } f(x) \text{ is irreducible over } \mathbf{F}[x]). \end{aligned}$$

Now, since  $[\mathbf{E} : \mathbf{F}] = 2$ , the degree of  $\mu_\alpha(x)$  is 2, and so the degree of  $f(x)$  is 2. As  $\alpha$  is a root of  $f(x)$ , one of its factors is  $x - \alpha$ , and so  $f(x) = (x - \alpha)(x - r)$ , for some  $r \in \mathbf{F}$  (since  $\alpha \cdot r \in \mathbf{F}$ ). Therefore,  $f(x)$  splits over  $\mathbf{E}$ , as desired.  $\square$

### 3 Problem 7

**Proposition 3.1.** *Let  $\mathbf{E}$  be a field extending the field  $\mathbf{F}$ . Let  $\mathbf{L}$  and  $\mathbf{M}$  be intermediate fields such that  $\mathbf{L}$  is the splitting field of a separable polynomial in  $\mathbf{F}[x]$ . Let  $\mathbf{L} \vee \mathbf{M}$  denote the smallest subfield of  $\mathbf{E}$  that extends both  $\mathbf{L}$  and  $\mathbf{M}$ . Under all these conditions,  $\mathbf{L} \vee \mathbf{M}$  is a finite, normal, separable extension of  $\mathbf{M}$  and  $\text{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M}) \cong \text{Aut}_{\mathbf{M} \cap \mathbf{L}} \mathbf{L}$ .*

*Proof.* We first show that  $\mathbf{L} \vee \mathbf{M}$  is the splitting field of a separable polynomial from  $\mathbf{M}[x]$  and then invoke the Key Theorem, which states that this is equivalent to being a finite, normal, separable extension of  $\mathbf{M}$ .

**Claim 1.**  $\mathbf{L} \vee \mathbf{M} = \mathbf{M}[r_0, \dots, r_{n-1}]$

*Proof.* ( $\subset$ ) As  $\mathbf{L} \vee \mathbf{M}$  is the *smallest* subfield of  $\mathbf{E}$  that extends both  $\mathbf{L}$  and  $\mathbf{M}$ , it will certainly be contained in  $\mathbf{M}[r_0, \dots, r_{n-1}]$  if  $\mathbf{M}[r_0, \dots, r_{n-1}]$  is indeed an extension of both  $\mathbf{L}$  and  $\mathbf{M}$ . It is evidently an extension of  $\mathbf{M}$ , and we see that it is also an extension of  $\mathbf{L}$  since

$$\begin{aligned} \mathbf{L} &= \mathbf{F}[r_0, \dots, r_{n-1}] \\ &\subset \mathbf{M}[r_0, \dots, r_{n-1}] \end{aligned} \quad (\text{since } \mathbf{M} \text{ is an extension of } \mathbf{F}).$$

( $\supset$ ) Let  $a \in \mathbf{M}[r_0, \dots, r_{n-1}]$ . We see that

$$a = c + \sum_{i=0}^{n-1} c_i r_i \quad c, c_i \in \mathbf{M}.$$

Observe also that, since  $\mathbf{L} = \mathbf{F}[r_0, \dots, r_{n-1}]$ , the  $r_i$  all belong to  $\mathbf{L}$  for all  $i$ . As  $\mathbf{L} \vee \mathbf{M}$  is an extension of both  $\mathbf{L}$  and  $\mathbf{M}$ , it follows that  $c, c_i$ , and  $r_i$  belong to  $\mathbf{L} \vee \mathbf{M}$  for all  $i$ . Hence, the linear combination  $a$  belongs to  $\mathbf{L} \vee \mathbf{M}$ , as desired.  $\square$

By the above, we conclude that  $\mathbf{L} \vee \mathbf{M}$  is a finite, separable, normal extension of  $\mathbf{M}$ .

Next, define the function

$$\begin{aligned} \phi : \text{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M}) &\rightarrow \text{Aut}_{\mathbf{F}} \mathbf{L} \\ \phi(\sigma) &= \sigma|_{\mathbf{L}}. \end{aligned}$$

We show that  $\phi$  has trivial kernel and that its image is  $\text{Aut}_{\mathbf{M} \cap \mathbf{L}} \mathbf{L}$ . Given these facts, the Homomorphism Theorem will allow us to conclude that  $\text{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M}) \cong \text{Aut}_{\mathbf{M} \cap \mathbf{L}} \mathbf{L}$ .

**Claim 2.** *The kernel of  $\phi$  is trivial.*

*Proof.*

$$\begin{aligned}\sigma \in \ker \phi &\Rightarrow \phi(\sigma) = \text{id} \upharpoonright_{\mathbf{L}} \\ &\Rightarrow \sigma \upharpoonright_{\mathbf{L}} = \text{id} \upharpoonright_{\mathbf{L}}\end{aligned}$$

Hence,  $\sigma$  fixes all elements of  $\mathbf{L}$ . As  $\sigma \in \text{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M})$ ,  $\sigma$  also fixes all elements of  $\mathbf{M}$ , and so  $\sigma$  fixes  $\mathbf{M}[r_0, \dots, r_{n-1}] = \mathbf{L} \vee \mathbf{M}$ . Hence,  $\sigma$  is the identity on its domain, and so the kernel of  $\phi$  is trivial.  $\square$

**Claim 3.**  $\text{Inv}(\text{im}\phi) = \mathbf{L} \cap \mathbf{M}$

*Proof.* Let  $H = \text{im}\phi$  and  $K = \text{Inv}H$ . We have that

$$\begin{aligned}H &\leq \text{Aut}_{\mathbf{F}}\mathbf{L} \\ &= \text{Gal}\left(\frac{\mathbf{L}}{\mathbf{F}}\right).\end{aligned}$$

Since  $H$  is finite, the Key Theorem implies that

$$H = \text{Aut}_{\mathbf{K}}\mathbf{L}.$$

Hence, it suffices to show that  $\mathbf{K} = \mathbf{L} \cap \mathbf{M}$ . To that end, let  $a \in \mathbf{L} \cap \mathbf{M}$ . Observe that

$$\begin{aligned}\phi(\sigma)(a) &= \sigma \upharpoonright_{\mathbf{L}}(a) \\ &= a\end{aligned}\quad (\text{since } a \in M).$$

Hence,  $\mathbf{L} \cap \mathbf{M} \subset \mathbf{K}$ .

For the reverse inclusion, let  $a \in \mathbf{K}$ . As before,

$$\begin{aligned}\phi(\sigma)(a) &= \sigma \upharpoonright_{\mathbf{L}}(a) \\ &= a\end{aligned}\quad (\text{since } a \in K),$$

and so  $a \in L$ . We also have

$$\begin{aligned}\sigma \upharpoonright_{\mathbf{L}}(a) &= a \\ \Rightarrow \sigma(a) &= a,\end{aligned}$$

and so  $a \in \text{Inv}(\text{Aut}(\mathbf{L} \vee \mathbf{M}))$ , but this is just  $M$  (by the Key Theorem). Hence,  $a \in \mathbf{L} \cap \mathbf{M}$ .  $\square$

Finally, the Homomorphism Theorem gives that  $\text{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M}) \cong \text{Aut}_{\mathbf{M} \cap \mathbf{L}}\mathbf{L}$ , thus completing the proof.  $\square$

## 4 Problem 8

**Proposition 4.1.** *Let  $\mathbf{L}$  and  $\mathbf{M}$  be fields. View the collection of functions from  $\mathbf{L}$  into  $\mathbf{M}$  as a vector space over  $\mathbf{M}$  with addition defined in the usual way. The collection of field embeddings from  $\mathbf{L}$  into  $\mathbf{M}$  is a linearly independent set in this vector space.*

*Proof.* Suppose, for the purpose of contradiction, that the collection of field embeddings from  $\mathbf{L}$  into  $\mathbf{M}$  is not linearly independent set. Choose minimal  $k$  such that

$$c_0\phi_0 + \cdots + c_k\phi_k = 0 \quad c_i \in \mathbf{M}, \phi_i \text{ field embeddings from } \mathbf{L} \text{ into } \mathbf{M}$$

with  $c_i \neq 0$  for all  $i$ . Without loss of generality, there exists  $x'$  such that  $\phi_0(x') \neq \phi_1(x')$  and further that  $\phi_0(x') \neq 0$ . It follows that

$$\begin{aligned} 0 &= \phi_0(x')(c_0\phi_0 + \cdots + c_k\phi_k) \\ &= c_0\phi_0(x')\phi_0 + \cdots + c_k\phi_0(x')\phi_k. \end{aligned}$$

Consider the evaluation at  $xx'$ .

$$\begin{aligned} 0 &= c_0\phi_0(xx') + \cdots + c_k\phi_k(xx') \\ &= c_0\phi_0(x)\phi_0(x') + \cdots + c_k\phi_k(x)\phi_k(x') \end{aligned}$$

Hence,

$$\begin{aligned} 0 &= (c_0\phi_0(x')\phi_0 + \cdots + c_k\phi_0(x')\phi_k) - (c_0\phi_0(x)\phi_0(x') + \cdots + c_k\phi_k(x)\phi_k(x')) \\ &= c_1(\phi_0(x') - \phi_1(x'))\phi_1(x) + \cdots + c_k(\phi_0(x') - \phi_k(x'))\phi_k(x), \end{aligned}$$

which is a shorter nontrivial linear combination, contradiction the minimality of  $k$ . Therefore, we conclude that the collection of field embeddings from  $\mathbf{L}$  into  $\mathbf{M}$  is indeed a linearly independent set in this vector space.  $\square$

## 5 Problem 9

**Proposition 5.1.** *Let  $\mathbf{F}$  be a field. We use  $\mathbf{F}^\times$  to denote the group of nonzero elements of  $\mathbf{F}$  under multiplication and the formation of multiplicative inverses. Every finite subgroup of  $\mathbf{F}^\times$  is a cyclic group.*

*Proof.* Let  $\mathbf{G}$  be a finite subgroup of  $\mathbf{F}^\times$ . Since  $\mathbf{F}$  is a field, we know that  $\mathbf{G}$  is Abelian. By the Fundamental Theorem of Finite Abelian Groups,  $\mathbf{G} \cong \mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_k}^{n_k}$  where the  $p_i$  are distinct primes and the  $n_i$  are positive integers.

If  $n_i = 1$  for all  $i$ , the Chinese Remainder Theorem gives that the element  $(1, \dots, 1)$  generates  $\mathbf{G}$  (as the  $p_i$  are relatively prime), and so  $\mathbf{G}$  is cyclic.

Suppose now, for the purpose of contradiction, that  $n_j \geq 2$  for some  $j$ , then  $\mathbf{G}$  has  $\mathbb{Z}_{p_j} \times \mathbb{Z}_{p_j}$  as a subgroup. For any  $a, b \in \mathbb{Z}_{p_j}$ , Lagrange's Theorem gives that  $(a, b)^{p_j} = 1$ . In other words, there are  $p_j^2$  roots of  $x^{p_j} - 1$ , which is a contradiction. Hence,  $n_i = 1$  for all  $i$ , and so  $\mathbf{G}$  is cyclic by the previous argument.  $\square$