MATH 702 – SPRING 2024
LOW LYING FRUIT – MARCH 13, 2024

(1) **Let R be a (commutative) domain, I be an ideal in R, K be the quotient field of R, and $\phi : I \to R$ be an R-module homomorphism. Prove that there exists a K-module homomorphism $\Phi : K \to K$ such that $\Phi|_I = \phi$.**

If I is the zero ideal, then take Φ to be identically zero. Henceforth, we assume that I is not the zero ideal. Fix an nonzero element x in I. Define $\Phi : K \to K$ by $\Phi(u) = u\frac{\phi(x)}{x}$. Observe that $\Phi : K \to K$ is a K-module homomorphism. (Or if you prefer, K is a one-dimensional vector space over K and Φ is a linear transformation from this vector space to itself.)

We still must show that the restriction of Φ to I is equal to ϕ. Let $y \in I$. We must show that $\Phi(y)$ is equal to $\phi(y)$ in K. We must show that $y\frac{\phi(x)}{x}$ is equal to $\phi(y)$ in K. We must show that $y\phi(x)$ is equal to $x\phi(y)$ in R. Of course, this is true. Indeed, $\phi : I \to R$ is an R-module homomorphism; hence

$$y\phi(x) = \phi(yx) = x\phi(y).$$

The first equality holds because $y \in R$ and $x \in I$. The second equality holds because $x \in R$ and $y \in I$.

(2) **Suppose $\boldsymbol{k} \subset E$ and $E \subseteq K$ are both finite dimensional Galois extensions. Does $\boldsymbol{k} \subseteq K$ have to be a Galois extension? Prove or give a counter example.**

NO! The extensions $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[4]{2}]$ each have dimension two; hence each extension is Galois by (5a). However, the extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[4]{2}]$ is not Galois because three of the roots of the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ are not in $\mathbb{Q}[\sqrt[4]{2}]$.

(3) **Let $\boldsymbol{k} \subset K$ be a Galois extension of fields with $\dim_{\boldsymbol{k}} K = p^2$, for some prime integer p. Suppose E is a field with $\boldsymbol{k} \subseteq E \subseteq K$. Prove that $\boldsymbol{k} \subseteq E$ is a Galois extension.**

Let G be the Galois group $\operatorname{Aut}_{\boldsymbol{k}} K$. The Fundamental Theorem of Galois Theory guarantees that the order of G is equal to $\dim_{\boldsymbol{k}} K = p^2$. Every group of order p^2 is Abelian. So every subgroup of G is a normal subgroup. If E is an intermediate field, then $E = K^H$ for some subgroup H of G. The fact that $H \lhd G$ ensures (again by the Fundamental Theorem of Galois Theory) that $\boldsymbol{k} \subseteq K^H$ is a Galois extension.

(4) **Give an example of a fields $\boldsymbol{k} \subseteq E \subseteq K$ with $\boldsymbol{k} \subseteq K$ a Galois extension of dimension p^3 for some prime integer p, but $\boldsymbol{k} \subseteq E$ not a Galois extension.**

Recall the Dihedral group D_4 which is the group of order 8 generated by σ and ρ with $\sigma^2 = \mathrm{id}$, $\rho^4 = \mathrm{id}$ and $(\sigma\rho)^2 = \mathrm{id}$. The subgroup $\langle\sigma\rangle$ is not normal in D_4.

I want a Galois extension $\boldsymbol{k} \subseteq K$ with Galois group equal to D_4. Then $\boldsymbol{k} \subseteq K^{\langle\sigma\rangle}$ is an intermediate extension which is not Galois.

Here is the first example that comes to my mind; but this is cheating because you don't know it yet – but you will. Let F be a field and $K = F(x_1, x_2, x_3, x_4)$ be the field of rational functions over F. The symmetric group $S_4 = \mathrm{Sym}\{x_1, x_2, x_3, x_4\}$ acts on the variables x_1, x_2, x_3, x_4 and hence on the field K. The subfield K^{S_4} is equal to $F(s_1, s_2, s_3, s_4)$ where

$$\begin{aligned}
s_1 &= x_1 + x_2 + x_3 + x_4 \\
s_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
s_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
s_4 &= x_1x_2x_3x_4
\end{aligned}$$

are the four elementary symmetric polynomials in four variables. The extension $K^{D_4} \subseteq K$ is Galois with Galois group D_4 and the intermediate extension

$$K^{D_4} \subseteq K^{\langle\sigma\rangle}$$

is not Galois. (So, take $\boldsymbol{k} = K^{D_4}$ and $E = K^{\langle\sigma\rangle}$).

For another example of a Galois extension with Galois group D_4, consider

$$\boldsymbol{k} = \mathbb{Q} \subseteq K = \mathbb{Q}[\sqrt[4]{2}, i].$$

The field K is the splitting field of the polynomial $x^4 - 2$; so the extension is Galois. There are four embeddings of $\mathbb{Q}[\sqrt[4]{2}]$ into K (namely send $\sqrt[4]{2}$ to $i^\ell\sqrt[4]{2}$ with $0 \le \ell \le 3$). For each of these embeddings, there are two extensions to an automorphism of K (namely send i to $\pm i$). So $\mathrm{Aut}_{\boldsymbol{k}} K$ is the eight element group $\langle\rho, \sigma\rangle$ where $\rho(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\rho(i) = i$ and $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$ and $\sigma(i) = -i$. Observe that $\mathrm{Aut}_{\boldsymbol{k}} K$ is a copy of D_4 and $\mathbb{Q}[\sqrt[4]{2}] = K^{\langle\sigma\rangle}$ is an intermediate field with $\mathbb{Q} \subseteq K^{\langle\sigma\rangle}$ is not a Galois extension.

(5) **Let $\boldsymbol{k}$ be a field of characteristic not equal to 2, $\boldsymbol{k} \subseteq K$ be a field extension with $\dim_{\boldsymbol{k}} K = 2$, and u be an element of K which is not in $\boldsymbol{k}$. Then the following statements hold.**

(a) **The field extension $\boldsymbol{k} \subseteq K$ is Galois and the Automorphism group $\mathrm{Aut}_{\boldsymbol{k}} K$ is cyclic of order two.**

(b) **The minimal polynomial of u over $\boldsymbol{k}$ is**

$$x^2 - (u + \tau(u))x + u\tau(u)$$

in $\boldsymbol{k}[x]$, where τ is the non-identity element of $\mathrm{Aut}_{\boldsymbol{k}} K$.

(c) **The field K is equal to $\boldsymbol{k}(\Delta)$, with $\Delta^2 \in \boldsymbol{k}$, for $\Delta = u - \tau(u)$.**

The fact that $\boldsymbol{k} \subsetneq \boldsymbol{k}(u) \subseteq K$, with $\dim_{\boldsymbol{k}} K = 2$ forces $\boldsymbol{k}(u) = K$. The minimal polynomial f of u over $\boldsymbol{k}$ has degree 2; thus, $f(x) = x^2 + \alpha_1 x + \alpha_2$, for some α_1 and α_2 in $\boldsymbol{k}$. The derivative, $f'(x) = 2x + \alpha_1$, is not identically zero (since the characteristic of $\boldsymbol{k}$ is not two); hence f is a separable polynomial and the splitting field of f over $\boldsymbol{k}$ is a Galois extension of $\boldsymbol{k}$.

Observe that K is the splitting field of f over K. Indeed, $f \in K[x]$ and the element u of K is a root of f. It follows that $(x-u)$ is a factor of f in $K[x]$. The other factor is monic and linear. Thus, there is an element $u' \in K$ with $f = (x-u)(x-u')$ in $K[x]$.

At this point all of assertion (5a) has been established. It is also clear that the non-identity element τ of $\operatorname{Aut}_{\boldsymbol{k}} K$ must carry u to u'. Now assertion (5b) is also clear.

We prove (5c). We first show that $\boldsymbol{k}[u] = \boldsymbol{k}[u-u']$. We already saw that $u' \in \boldsymbol{k}[u]$; thus $\boldsymbol{k}[u] \supseteq \boldsymbol{k}[u-u']$. On the other hand,

$$u = \tfrac{1}{2}\Big(\underbrace{(u+u')}_{\in \boldsymbol{k}} + (u-u')\Big) \in \boldsymbol{k}[u-u'];$$

hence, $\boldsymbol{k}[u] \subseteq \boldsymbol{k}[u-u']$; and $\boldsymbol{k}[u] = \boldsymbol{k}[u-u']$. Finally, observe that

$$(u-u')^2 = (\underbrace{u+u'}_{\in \boldsymbol{k}})^2 - 4(\underbrace{uu'}_{\in \boldsymbol{k}}) \in \boldsymbol{k}.$$

It might be helpful to realize that Δ^2 is the usual discriminant $b^2 - 4ac$ for the quadratic polynomial $ax^2 + bx + c$ with $a = 1$, $b = u + u'$ and $c = uu'$.

(6) **Let $\boldsymbol{k} \subseteq K$ be a finite dimensional Galois extension of fields with $\operatorname{Aut}_{\boldsymbol{k}} K$ a cyclic group. Let σ be a generator of $\operatorname{Aut}_{\boldsymbol{k}} K$. Suppose that $E_1 \subseteq E_2$ are fields with**

$$\boldsymbol{k} \subseteq E_1 \subseteq E_2 \subseteq K$$

and $\dim_{E_1} E_2 = 2$. If $u \in E_2 \setminus E_1$, then the minimal polynomial of u over E_1 is $(x-u)(x-\sigma(u))$.

The field extension $\boldsymbol{k} \subseteq K$ is Galois with an Abelian Galois group. Every subgroup of an Abelian group is normal; consequently, the fundamental theorem of Galois Theory guarantees that $E_1 \subseteq E_2$ is a Galois extension and that the non-identity element[1] of $\operatorname{Aut}_{E_1} E_2$ is $\sigma|_{E_2}$. Thus, u and $\sigma(u)$ are the roots of the minimal polynomial of u over E_1 and the minimal polynomial of u over E_1 is $(x-u)(x-\sigma(u))$ in $E_2[x]$.

[1]This assertion is the proof of the fourth part of the fundamental theorem of Galois Theory; it is not recorded as part of the statement.