SOLUTIONS TO PROBLEM SET 3

MATTI ÅSTRAND

The General Cubic Extension

Denote $L = k(\alpha_1, \alpha_2, \alpha_3)$, $F = k(a_1, a_2, a_3)$ and $K = F(\alpha_1)$. The polynomial

$$f(x) = x^3 - a_1x^2 + a_2x - a_3 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

is irreducible in $F[x]$. The symmetric group S_3 acts on L by permuting the α_i, and fixes the field F.

Problem 2. The field $K = F(\alpha_1)$ is generated over F by the element α_1, which is a root of the irreducible polynomial $f(x) \in F[x]$, so $K \cong F[t]/(f(t))$ and has a basis $\{1, \alpha_1, \alpha_1^2\}$ over F. Thus $\dim_F K = 3$.

Let's now consider $f(x)$ as a polynomial in $K[x]$. It has a linear factor corresponding to the root $\alpha_1 \in K$, so it factors as

$$f(x) = (x - \alpha_1)g(x),$$

where $g(x)$ is a quadratic polynomial in $K[x]$. (Note: actually $g(x) = (x-\alpha_2)(x-\alpha_3)$, but this factoring takes place in $L[x]$.)

We get L from K by adding the roots of the quadratic polynomial $g(x)$. Thus the extension is either quadratic (if the roots of $g(x)$ are not in K) or trivial, i.e. $L = K$ (if $g(x)$ has roots already in K).

Turns out that L is a quadratic extension of K: for this we need to show that the two fields are not equal. Let $\sigma = (23)$ be the transposition swapping α_2 and α_3. Denote by L^σ the fixed field of σ. Since σ obviously doesn't fix every element of L (e.g. it doesn't fix α_2) we see that $L^\sigma \subsetneq L$. On the other hand, σ does fix everything in F and also α_1, so it fixes everything in K. We then have

$$K \subseteq L^\sigma \subsetneq L.$$

(Note that this also proves that K is exactly the fixed field L^σ.)

Now we know that $\dim_K L = 2$, and L has a basis $\{1, \alpha_2\}$ over K. Then a basis for L over F would be

$$\{1, \alpha_1, \alpha_1^2, \alpha_2, \alpha_1\alpha_2, \alpha_1^2\alpha_2\}.$$

(See problem 1 below)

Problem 3. We saw in problem 2 above that $\dim_F K = 3$, so we only need to show that the automorphism group $\mathrm{Aut}(K/F)$ is trivial. To see this, let $\sigma \in \mathrm{Aut}(K/F)$ be such an automorphism. Since $f(x)$ is a polynomial in $F[x]$, the automorphism σ has to permute the roots of $f(x)$, so $\sigma(\alpha_1)$ has to be a root of $f(x)$. But in problem 2 above we saw that K doesn't contain the other roots α_2 and α_3 of $f(x)$, so $\sigma(\alpha_1) = \alpha_1$.

Let K^σ be the fixed field of σ. Since σ has to fix F, we know that $F \subseteq K^\sigma$. But since $\sigma(\alpha_1) = \alpha_1$, we get $\alpha_1 \in K^\sigma$. Thus $K^\sigma \supseteq F(\alpha_1) = K$, so σ fixes all of K, which means that $\sigma = \mathrm{id}$. Thus $\mathrm{Aut}(K/F) = \{\mathrm{id}\}$.

Problem 4. The roots of the polynomial $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ are exactly $\{\alpha_1, \alpha_2, \alpha_3\}$. The field L is by definition the smallest field containing the roots of $f(x)$ (and k), so it's the smallest field where $f(x)$ splits into linear factors.

The Cyclic Cubic Extension

Let k be a field, and $\xi \in k$ an element such that the polynomial $\kappa(t) = t^3 - \xi$ is irreducible.

Problem 1. Let $k_\kappa = k[t]/(\kappa(t))$ be the Kronecker construction. Denote by α the equivalence class of t in k_κ, so that $k_\kappa = k(\alpha)$ and $\alpha^3 = \xi$.

Assume first that $k(\alpha)$ doesn't contain a cube root of unity. Let $\sigma \in \text{Aut}(k(\alpha)/k)$ be an automorphism. Then $\sigma(\alpha)$ is also a root of $\kappa(t)$, since σ permutes the roots of the polynomial $\kappa(t) \in k[t]$. But now we have

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)^3 = \frac{\sigma(\alpha)^3}{\alpha^3} = \frac{\xi}{\xi} = 1.$$

Since $k(\alpha)$ doesn't have a (nontrivial) third root of unity, we have $\frac{\sigma(\alpha)}{\alpha} = 1$, so $\sigma(\alpha) = \alpha$. But if the fixed field of σ contains both k and α, it has to be the whole field $k(\alpha)$, so $\sigma = \text{id}$.

Assume now that $k(\alpha)$ does contain a cube root of unity μ. We have that

$$(\mu\alpha)^3 = \mu^3\alpha^3 = 1 \cdot \xi = \xi,$$

so $\mu\alpha$ is another root of $\kappa(t)$. Similarly $\mu^2\alpha$ is a root of $\kappa(t)$. Thus $\kappa(t)$ has three roots in $k(\alpha)$, and

$$\kappa(t) = (t - \alpha)(t - \mu\alpha)(t - \mu^2\alpha).$$

Since both α and $\mu\alpha$ are roots of the irreducible polynomial $\kappa(t)$, we have two isomorphisms $k[t]/(\kappa(t)) \cong k(\alpha)$: one sending the equivalence class of t to α, and another sending it to $\mu\alpha$. Composing the first isomorphism with the inverse of the second one, we get an isomorphism from $k(\alpha)$ to itself, sending α to $\mu\alpha$:

$$k(\alpha) \to k[t]/(\kappa(t)) \to k(\alpha)$$

This is a nontrivial automorphism of $k(\alpha)$ over k, so $\text{Aut}(k(\alpha)/k)$ is nontrivial. In fact, $\text{Aut}(k(\alpha)/k) = \{\text{id}, \sigma, \sigma^2\}$ is a cyclic group of order 3. (For details of why this is true, see problem 3 of the last section.)

Finally, if $k(\alpha)$ contains a cube root of unity, I claim that it has to be already in k. Otherwise μ is a root of the irreducible polynomial

$$\frac{t^3 - 1}{t - 1} = t^2 + t + 1,$$

so the extension $k(\mu)/k$ has degree 2. But by problem 1 below, an extension of degree 3 cannot have a subextension of degree 2, since 3 is odd.

Problem 2. Let $C_3 = \{1, \sigma, \sigma^2\}$ be a cyclic group of order 3.

Define a k-algebra homomorphism $\phi\colon k[t] \to k[C_3]$ by sending t to

$$\phi(t) = \sigma \in k[C_3].$$

Then $\phi(t^3) = \sigma^3 = 1$, so $t^3 - 1 \in \mathrm{Ker}(\phi)$. Thus we can define a homomorphism

$$\overline{\phi}\colon k[t]/(t^3-1) \to k[C_3]$$

by $\overline{\phi}([g(t)]) = \phi(g(t))$ for any polynomial $g(t) \in k[t]$.

Let's show that $\overline{\phi}$ is an isomorphism. The ring $k[t]/(t^3-1)$ has a k-basis $\{1, t, t^2\}$, which is sent to $\{1, \sigma, \sigma^2\}$. Thus $\overline{\phi}$ sends a k-basis of $k[t]/(t^3-1)$ to a k-basis of $k[C_3]$, so it is bijective. This means that $\overline{\phi}$ is an isomorphism between the two rings.

Assume that k has a cube root of unity μ. Since the polynomial $t^3 - 1$ splits into coprime factors as

$$t^3 - 1 = (t-1)(t-\mu)(t-\mu^2),$$

we get

$$\begin{aligned} k[C_3] \cong k[t]/(t^3-1) &\cong k[t]/(t-1) \times k[t]/(t-\mu) \times k[t]/(t-\mu^2) \\ &\cong k \times k \times k. \end{aligned}$$

The automorphism from $k[t]/(t^3-1)$ to $k \times k \times k$ sends a polynomial $p(t)$ to the triple $(p(1), p(\mu), p(\mu^2))$. We want e_1 to be sent to $(0, 1, 0)$, and we can notice that such a polynomial is

$$\frac{(t-1)(t-\mu^2)}{(\mu-1)(\mu-\mu^2)} = \frac{1}{3}(\mu\, t^2 + \mu^2 t + 1).$$

Thus the desired element $e_1 \in k[C_3]$ is

$$e_1 = \frac{\mu\sigma^2 + \mu^2\sigma + 1}{3}.$$

Problem 3. Let k be a field of characteristic 3. In $k[t]$, the polynomial $t^3 - 1$ factors as $(t-1)^3$. Thus, the only root of $t^3 - 1$ is 1.

Last 5 problems

Let k be a field containing a cube root of unity μ, K be a field extension with $\dim_k K = 3$, and $\sigma \in \mathrm{Aut}(K/k)$ a nontrivial automorphism.

Problem 1. Suppose that $\dim_K L = m$ and $\dim_L M = n$. Choose $\{a_1, \ldots, a_m\}$ to be a K-basis of L and $\{b_1, \ldots, b_n\}$ to be an L-basis of M. I claim that now the mn elements in

$$\{a_i b_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$$

are a K-basis for M. In particular, $\dim_K M = mn$.

To prove that the $(a_i b_j)$ span M over K, let $\alpha \in M$. Now α can be written as

$$\alpha = \sum_{j=1}^{n} c_j b_j$$

for some $c_j \in L$. Also the elements c_j can be written as

$$c_j = \sum_{i=1}^{m} x_{ij} a_i$$

for some $x_{ij} \in K$. Thus we have

$$\alpha = \sum_{j=1}^{n} \sum_{i=1}^{m} x_{ij} a_i b_j,$$

so the elements $a_i b_j$ generate M over K.

Finally, let's show that $a_i b_j$ are linearly independent over K. Suppose that a linear combination

$$\sum_{j=1}^{n} (\sum_{i=1}^{m} x_{ij} a_i) b_j = 0$$

for $x_{ij} \in K$. But this is a linear combination in b_j with the coefficients $\sum_{i=1}^{m} x_{ij} a_i$ in the field L, so we must have

$$\sum_{i=1}^{m} x_{ij} a_i = 0 \quad \text{for all } i.$$

But this means that $x_{ij} = 0$, since a_i are linearly independent.

Problem 2. Pick an element $\alpha \in K$, such that $\alpha \notin k$. Now by the above problem 1 we see that $K = k(\alpha)$, since

$$3 = (\dim_k k(\alpha))(\dim_{k(\alpha)} K),$$

and $\dim_k k(\alpha) \neq 1$. (With similar reasoning you can show that $K^\sigma = k$.)

Let $f(t) \in k[t]$ be the minimal polynomial of α over k. Now σ permutes the roots of $f(t)$.

An automorphism is determined by where it maps α, in the following sense: If σ and τ are two automorphisms in $\mathrm{Aut}(K/k)$ such that $\sigma(\alpha) = \tau(\alpha)$, then $\sigma = \tau$. This is because the fixed field of $\tau^{-1}\sigma$ contains k and α, so it is all of K, i.e. $\tau^{-1}\sigma = \mathrm{id}$. Since α has to map to one of the roots of $f(t)$, there are at most 3 automorphisms in $\mathrm{Aut}(K/k)$.

If σ had order 2, then the polynomial

$$(t - \alpha)(t - \sigma(\alpha))$$

has its coefficients in $K^\sigma = k$, and it has degree 2. This is a contradiction with the fact that the minimal polynomial of α has degree 3.

Problem 3. The solution of problem 2 proves that $\mathrm{Aut}(K/k)$ is cyclic group of order 3.

Problem 4. Let $\alpha \in K$ be a root of $f(t)$. Then $k(\alpha)$ is a subfield of K which contains k but is not equal to k. By our standard dimension argument, we see that $K = k(\alpha)$, and

$$\deg(f(t)) = \dim_k k(\alpha) = \dim_k K = 3.$$

The (distinct) elements $\alpha, \sigma(\alpha)$ and $\sigma^2(\alpha)$ are roots of $f(t)$, so $f(t)$ is divisible by

$$(t - \alpha)(t - \sigma(\alpha))(t - \sigma^2(\alpha)).$$

Because we already saw that $\deg f(t) = 3$, we know that $f(t)$ is constant multiple of the above polynomial.

Problem 5. The elements $e_i \in k[C_3]$ for $i = 0, 1, 2$ satisfy

$$\begin{aligned} e_0 + e_1 + e_2 &= 1 \\ (\sigma - \mu^i)e_i &= 0 \\ e_i^2 &= e_i \\ e_i e_j &= 0 \quad \text{for } i \neq j. \end{aligned}$$

We identify the group $\mathrm{Aut}(K/k) = \{\mathrm{id}, \sigma, \sigma^2\}$ with C_3. Then the elements of the group ring $k[C_3]$ give maps $K \to K$, which are linear over k. The properties above imply that

$$K = \mathrm{Im}(e_0) \oplus \mathrm{Im}(e_1) \oplus \mathrm{Im}(e_2),$$

and that $\mathrm{Im}(e_0) \subseteq K^\sigma = k$. This means that $\mathrm{Im}(e_0)$ is (at most) 1-dimensional, so $\mathrm{Im}(e_i)$ has to be nonzero for either $i = 1$ or $i = 2$.

Now, let $\eta \in \mathrm{Im}(e_i)$ be nonzero. Then $\sigma(\eta) = \mu^i \eta \neq \eta$, so $\eta \notin k$. This implies that $K = k(\eta)$ (by the standard dimension argument). Also,

$$\sigma(\eta^3) = (\sigma(\eta))^3 = \mu^{3i}\eta^3 = \eta^3,$$

so $\eta^3 \in K^\sigma = k$.