PS8 - Separable extensions and Galois groups

Math146 - George McNinch

2025-04-13

K denotes a field.

1. Let L_1 and L_2 be splitting fields over K of the polynomial $f \in K[T]$. We have seen before that $L_1 \simeq L_2$. More precisely, there is an isomorphism $\phi : L_1 \to L_2$ for which $\phi(a) = a$ for all $a \in K$.

   Use ϕ to show that there is an isomorphism $\mathrm{Gal}(L_1/K) \xrightarrow{\sim} \mathrm{Gal}(L_2/K)$. (Be sure to show that the mapping you exhibit is in fact an isomorphism).

2. For $n \in \mathbf{Z}_{\geq 0}$, let $\mathscr{P}_n = \{f \in K[T] \mid \deg f < n\}$, and note that $\dim_K \mathscr{P}_n = n$.

   Fix non-zero polynomials $A, B \in K[T]$ with $\deg A = d$ and $\deg B = e$.

   a. For polynomials $P \in \mathscr{P}_e$ and $Q \in \mathscr{P}_d$ form the polynomial $\Phi(P,Q) = AP + BQ$. Explain why Φ determines a linear mapping

   $$\Phi : \mathscr{P}_e \times \mathscr{P}_d \to \mathscr{P}_{d+e}$$

   (You might prefer to write $\mathscr{P}_e \times \mathscr{P}_d$ as $\mathscr{P}_e \oplus \mathscr{P}_d$ – it is the *direct sum* of vector spaces.)

   Consider the basis $\mathscr{B} = \{(T^i, 0) \mid 0 \leq i < e\} \cup \{(0, T^i) \mid 0 \leq i < d\}$ of $\mathscr{P}_e \oplus \mathscr{P}_d$ and the basis $\mathscr{C} = \{T^i \mid 0 \leq i < d+e\}$ of $\mathscr{P}_{e+d}$, let M be the matrix of Φ with respect to these bases, and let $R(f,g) = \det(M) \in K$ be the *determinant* of M. The quantity $R(f,g)$ is known as the *resultant* of f and g.

   For example, if $d = 2$ and $e = 2$, and if $A = aT^2 + bT + c$ and $B = dT^2 + eT + f$ for $a, b, c, d, e, f \in K$ then

   $$M = \begin{pmatrix} c & 0 & f & 0 \\ b & c & e & f \\ a & b & d & e \\ 0 & a & 0 & d \end{pmatrix}$$

   Let's use a computer to find a formula for the resultant $R(f,g)$ in this case:

```
RR.<a,b,c,d,e,f>=PolynomialRing(ZZ)
M = matrix([[c,0,f,0],[b,c,e,f],[a,b,d,e],[0,a,0,d]])
(M,det(M))
```

```
(
[c 0 f 0]
[b c e f]
[a b d e]
[0 a 0 d],

c^2*d^2 - b*c*d*e + a*c*e^2 + b^2*d*f - 2*a*c*d*f - a*b*e*f + a^2*f^2
)
```

In this case, we find that

$$R(A,B) = c^2d^2 - bcde + ace^2 + b^2df - 2acdf - abef + a^2f^2$$

b. Show that there are polynomials $u \in \mathscr{P}_e$ and $v \in \mathscr{P}_d$ not both 0 for which

$$Au + Bv = R(A,B).$$

Hint: If M denotes the matrix of ϕ for the above bases, then finding polynomials $u = \sum_{i=0}^{e-1} u_i T^i$ and $v = \sum_{i=0}^{d-1} v_i T^i$ as above amounts to solving the matrix equation

$$M \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{e-1} \\ v_0 \\ \vdots \\ v_{d-1} \end{pmatrix} = \begin{pmatrix} R(A,B) \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

If $R(A,B) \neq 0$ this is possible since M is invertible. If $R(A,B) = 0$ then M is singular and there is a non-zero vector in its null space.

c. Prove that A, B have a common factor in $K[T]$ if and only if $R(A,B) = 0$.

Hint: Using b., since $R(A,B) = Au + Bv$, if A and B have a common factor of positive degree, it must divide the constant $R(A,B)$ which must therefore by 0. Conversely, if $R(A,B) = 0$, then b. shows that there are non-zero polynomials $u \in \mathscr{P}_e$ and $v \in \mathscr{P}_d$ for which $Au = -Bv$. Now consider a splitting field L for $Au = -Bv$ over K. It suffices to argue that A and B have a common root in L. But this follows from unique factorization in $L[T]$ since $\deg(v) < d = \deg(A)$.

Remark: Let L be a splitting field for $A \cdot B$ over K, and write $A = \prod_{i=1}^{d}(T - \alpha_i)$ and $B = \prod_{i=1}^{e}(T - \beta_i)$ for $\alpha_i, \beta_j \in L$. Then one can argue that

$$R(A,B) = \prod_{i,j}(\alpha_i - \beta_j).$$

3. Let $K = \mathbf{C}(X)$ be the field of rational functions over $\mathbf{C}$ (i.e. K is the field of fractions of the polynomial ring $\mathbf{C}[X]$).

   Fix a natural number $n \in \mathbf{Z}_{\geq 0}$ and consider the polynomial $P(T) = T^n - X \in K[T]$, and let $L = K[T]/\langle P(T)\rangle = K(\alpha)$ where $\alpha^n = X$.

a. Let $\omega = \exp(2\pi i/n) \in \mathbf{C}$ so that ω is a root of $T^n - 1$ and ω has multiplicative order n. Then $\omega\alpha$ is a root of $P(T)$. Explain why there is an automorphism $\sigma : L \to L$ such that $\sigma(\alpha) = \omega\alpha$.

b. Show that $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ is a cyclic group of order n.

c. Suppose that $n = 4$, and let σ be the generator for $\mathrm{Gal}(L/k)$ as before. What is the fixed field L^H where $H = \langle\sigma^2\rangle$?

Hint: Every element x of L may be written uniquely in the form

$$x = a + b\alpha + c\alpha^2 + d\alpha^3$$

and we know that

$$\sigma(x) = a + b\omega\alpha + c\omega^2\alpha + d\omega^3\alpha^3 = a + ib\alpha - c\alpha^2 - id\alpha^3$$

(since when $n = 4$, $\omega = i \in \mathbf{C}$). Now express $\sigma^2(x)$ as a linear combination of $\{\alpha^j\}$. What is the condition that $x = \sigma^2(x)$?