M3P11 (and M4P11, M5P11) Galois Theory, Worksheet 4

Alessio Corti

9th March 2020

Q 1. Say $E \subseteq F$ is an extension of fields with $[F : E]$ finite, and M, N are both subfields of F containing E. Assume that M/E and N/E are both normal.

(i) Prove that $(M \cap N)/E$ is normal.

(ii) Prove that MN (this notation means "the smallest subfield of F containing both M and N") is normal over E as well.

Q 2 (†)**.** (a) Let $K \subset L$ be a finite field extension. A finite extension $L \subset \Omega$ is a *normal closure* of $K \subset L$ if

1. $K \subset \Omega$ is normal, and
2. Ω is generated (as a ring, or field) by $\cup_\sigma \sigma(L)$, the union over all K-embeddings $\sigma \colon L \to \Omega$.

Prove that a normal closure always exists, and that any two normal closures are isomorphic over L.

(b) Let $K \subset L \subset \Omega$ be finite field extensions. Assume:

1. Ω is generated (as a ring, or field) by $\cup_\sigma \sigma(L)$, the union over all K-embeddings $\sigma \colon L \to \Omega$.
2. The set $\mathrm{Emb}_K(L, \Omega)$ has $[L : K]_s$ embeddings.

Then $K \subset \Omega$ is normal, and hence it is a normal closure of $K \subset L$.

Q 3. Here I ask you again to go through the example of an inseparable extension given in class.

Let k be any field of characteristic p (for example $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$), and let $L = k(T)$, the field of fractions of the polynomial ring $k[T]$. This means that a typical element of L is of the form $f(T)/g(T)$ with f and g polynomials, and $g \neq 0$. You can convince yourself that this is a field by checking that the sum, product etc of such things is of the same form.

Set $K = k(T^p)$, the subfield of L consisting of ratios $f(T^p)/g(T^p)$.

(a) Convince yourself that K really is a subfield of L;

(b) Check that $L = K(T)$, the smallest subfield of L containing K and T;

(c) Check that T is algebraic over K and hence $[L : K]$ is finite;

(d) Check that $q(x) = x^p - T^p$ is an irreducible element of $K[x]$;[1]

(e) Deduce that $q(x)$ is the min poly of T over K, and is also an inseparable polynomial in $K[x]$;

(f) Deduce that L/K is not a separable extension.

Q 4. Say $E \subseteq F$, and L and M are intermediate fields (i.e. $E \subseteq L, M \subseteq F$). Let $N := LM$ denote the smallest subfield of F containing L and M.

(i) If $L = E(\alpha_1, \ldots, \alpha_n)$ then prove $N = M(\alpha_1, \ldots, \alpha_n)$.

(ii) Now assume L/E and M/E are finite and normal. Prove N/E is finite and normal. (hint: splitting field). Next assume L/E and M/E are finite, normal and separable. Prove that N/E is finite, normal and separable.

(iii) Prove that restriction of functions gives a natural injective group homomorphism from $\mathrm{Gal}(N/E)$ to $\mathrm{Gal}(L/E) \times \mathrm{Gal}(M/E)$. Is it always surjective?

Q 5. (a) Prove that the polynomials

$$f(x) = x^3 + x + 1, \quad g(x) = x^3 + x^2 + 1 \quad \in \mathbb{F}_2[x]$$

are irreducible. Consider the fields $K = \mathbb{F}_2(\alpha)$, $L = \mathbb{F}_2(\beta)$ where α, β are roots of f, g. If $\sigma\colon K \to L$ is a field isomorphism, what are the possible values of $\sigma(\alpha) \in L$ written in the basis $1, \beta, \beta^2$ of L as a $\mathbb{F}_2$-vector space? Explain why K and L are isomorphic. How many field isomorphisms $\sigma\colon K \to L$ are there?

(b) Let L be the same as in Part (a). Consider the polynomial

$$h(x) = x^4 + x + 1 \in \mathbb{F}_2[x] \, .$$

Prove that h is irreducible in $\mathbb{F}_2[x]$, or else exhibit a factorisation. Let $L \subset E$ be the splitting field of h — seen as a polynomial in $L[x]$. Is the extension $\mathbb{F}_2 \subset E$ normal? Is it separable? What is the degree $[E : \mathbb{F}_2]$? Prove that $h \in L[x]$ is irreducible, or else exhibit a factorisation.

Q 6. Show that if G is a transitive subgroup of $\mathfrak{S}_n$ containing a $(n-1)$-cycle and a transposition, then $G = \mathfrak{S}_n$.

Q 7. Consider the polynomial:

$$f(x) = x^6 - 12x^4 + 15x^3 - 6x^2 + 15x + 12$$

(a) By considering how $f(x)$ factorises in $\mathbb{F}_p[x]$ for small primes p, either prove that $f(x) \in \mathbb{Q}[x]$ is irreducible, or exhibit a factorisation.

(b) Let $\mathbb{Q} \subset K$ be the splitting field of the polynomial in (a). Determine the Galois group of the extension $\mathbb{Q} \subset K$.

[1] Hint: suppose it was reducible, and factor it in $K[x]$. The same factorization would work in $L[x]$. But $L[x]$ is a unique factorization domain. Spot that $p(x) = (x - T)^p$ in $L[x]$. By looking at constant terms, convince yourself that this gives a contradiction.

Q 8. Consider the polynomial

$$f(x) = x^4 + x^2 + x + 1 \in \mathbb{Q}[x]$$

(a) By considering how $f(x)$ factorises in $\mathbb{F}_p[x]$ for small primes p, either prove that $f(x) \in \mathbb{Q}[x]$ is irreducible, or exhibit a factorisation.

(b) Let $\mathbb{Q} \subset K$ be the splitting field of the polynomial in (a). Determine the Galois group of the extension $\mathbb{Q} \subset K$.

Q 9. Consider the polynomial

$$f(x) = x^4 + 3x + 1 \in \mathbb{Q}[x]$$

(a) Show that $f(x)$ is irreducible in $\mathbb{F}_2[x]$ and compute its prime factorisation in $\mathbb{F}_5[x]$.

(b) Show that: if G is a transitive subgroup of $\mathfrak{S}_4$ that contains a 4-cycle and a 3-cycle, then $G = \mathfrak{S}_4$.

(c) Determine the structure of the Galois group of the splitting field of f over $\mathbb{Q}$.

Q 10. (a) Show that for all prime p and all integer $n > 0$ there exists an irreducible monic polynomial of degree n in $\mathbb{F}_p[x]$.

(b) Let $g(x) \in \mathbb{F}_2[x]$ be an irreducible monic polynomial of degree n; $h(x) \in \mathbb{F}_3[x]$ an irreducible monic polynomial of degree $(n-1)$; $p > n-2$ a prime and $k(x) \in \mathbb{F}_p[x]$ an irreducible monic quadratic polynomial. Show that there is a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(x) \equiv g(x) \mod 2$, $f(x) \equiv xh(x) \mod 3$, and $f(x) \equiv x(x+1)\cdots(x+n-3)k(x) \mod p$.

[*Hint. Chinese remainder theorem.*]

(c) If f is the polynomial in (b), show that the Galois group of the splitting field over $\mathbb{Q}$ of f is $\mathfrak{S}_n$.

Q 11. In this question $\zeta = e^{\frac{2\pi \mathtt{i}}{6}}$.

(a) Factorise the polynomial $x^6 - 1 \in \mathbb{Q}[x]$. Hence or otherwise determine the degree $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.

(b) Show that the polynomial $f(x) = x^6 + 3 \in \mathbb{Q}[x]$ is irreducible. Let $\mathbb{Q} \subset K$ be the splitting field of $f(x)$. What is the degree $[K : \mathbb{Q}]$?. Determine the Galois group G of the extension $\mathbb{Q} \subset K$ and describe, perhaps by drawing some picture(s), the action of G on the set of roots of $f(x)$.

[*Hint. Consider first the field* $\mathbb{Q}(\alpha)$ *where* $f(\alpha) = 0$ *and study the intersection* $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta)$.]

(c) Let $\mathbb{Q} \subset L$ be the splitting field of the polynomial $g(x) = x^6 - 3 \in \mathbb{Q}[x]$. Compute the degree $[L : \mathbb{Q}]$, determine the Galois group G of the extension $\mathbb{Q} \subset L$ and describe, perhaps by drawing some picture(s), the action of G on the set of roots of $g(x)$.

Q 12. For all integers $3 \leq n \leq 16$, draw pictures illustrating the lattice of subgroups of the Galois group of the cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\mu_n)$. Draw the corresponding picture of subfields $\mathbb{Q} \subset F \subset \mathbb{Q}(\mu_n)$. For each of these subfields, find "natural" generators.

If you feel brave, then do the case $n = 17$. (The Galois group $(\mathbb{Z}/17\mathbb{Z})^\times = C_{16}$ is not in and of itself very complicated. The field $\mathbb{Q}(\mu_{17})$ is a tower of quadratic extensions but it takes some elbow grease to determine at each stage what you are taking the square root of; in particular this leads to a formula for $\cos\frac{2\pi}{17}$ involving just iterated square roots of rational numbers. Gauss did this calculation in his teens and it led him to a construction of the regular 17-gon with ruler and compass. You don't yourself need to get to the bitter end of the calculation: do the first couple of steps and then look up the last steps on google.)