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

Alessio Corti

28th April 2020

Q 1. (i) If $p(x)$ is irreducible over E and has a root in $M \cap N$, then it has a root in M and a root in N, and hence splits completely in both M and N. So all the roots of $p(x)$ in F are in both M and N, and hence in $M \cap N$. Hence $M \cap N$ is normal.

(ii) If M is the splitting field of $f(x)$ and N is the splitting field of $g(x)$ then MN is the splitting field of $f(x)g(x)$ (not hard to check). Hence MN is normal.

Q 2. This is an unreasonably difficult question, but let's at least see what I can do.[1]

(a) Pick $\lambda_1, \dots, \lambda_n \in L$ such that $L = K(\lambda_1, \dots, \lambda_n)$. For all $i = 1, \dots, n$, let $f_i(x) \in K[x]$ be the minimal polynomial of λ_i over K, let

$$f(x) = \prod_{i=1}^{n} f_i(x) \in K[x]$$

and let $L \subset \Omega$ be the splitting field of $f(x)$ now thought of as a polynomial in $L[x]$. Composing $K \subset L$ and $L \subset \Omega$ we have $K \subset \Omega$ and It is pretty clear that this is also the splitting field of $f(x)$ over K. (Why?) I claim that $L \subset \Omega$ is a normal closure of $K \subset L$.

To check this I need to verify the two defining properties of a normal closure. The first is just saying that $K \subset \Omega$ is normal, and it is because it is a splitting field.

It remains to verify that Ω is generated over K by the set:

$$\Lambda = \{\sigma(\lambda_i) \mid i = 1, \dots, n,\ \sigma \in \mathrm{Emb}_K(L, \Omega)\}$$

(Please convince yourselves that this is so.) On the other hand we know that Ω is generated over K by the set of the roots of $f(x)$:

$$Z = \{\mu \in \Omega \mid f(\mu) = 0\}$$

so we will be done if we show that $\Lambda = Z$. Now we know that if λ is a root of f and $\sigma \in \mathrm{Emb}_K(L, \Omega)$ then $\sigma(\lambda)$ is also a root of f, that is, $\Lambda \subset Z$. Let us now show that $Z \subset \Lambda$.

[1] Don't worry too much if you don't follow the proof. I forbid you to spend more than five hours trying to understand this.

Let $\mu \in \Omega$ be a root of f. Then for some $i = 1, \dots, n$ μ is a root of f_i. We know that there is an embedding

$$\begin{tikzcd} K(\lambda_i) \arrow[r, "\varphi"] & \Omega \\ K \arrow[u] \arrow[ur] & \end{tikzcd}$$

such that $\varphi(\lambda_i) = \mu$; and by Lemma 16 (B) this φ extends to $\widetilde{\varphi}\colon \Omega \to \Omega$:

$$\begin{tikzcd} \Omega \arrow[dr, "\widetilde{\varphi}"] & \\ K(\lambda_i) \arrow[u] \arrow[r, "\varphi"] & \Omega \\ K \arrow[u] \arrow[ur] & \end{tikzcd}$$

Now consider $\sigma = \widetilde{\varphi}_{|L} \in \mathrm{Emb}_K(L, \Omega)$; by construction $\sigma(\lambda_i) = \mu$. This shows that $\mu \in \Lambda$ and that $Z \subset \Lambda$ and finishes Part(a).

(b) We need to show that $K \subset \Omega$ is normal.

Claim For all $\lambda \in L$ let $f(x) \in K(x)$ be its minimal polynomial: then $f(x) \in \Omega[x]$ splits completely.

The claim and property 1. imply: Choose $\lambda_1, \dots, \lambda_n$ such that $L = K(\lambda_1, \dots, \lambda_n)$ and call $f_i \in K[x]$ the minimal polynomial of λ_i, then Ω is the splitting field of $f = \prod_{i=1}^n f_i$[2], and hence $K \subset \Omega$ is normal.

Let us prove the claim. We don't yet know that $K \subset \Omega$ is normal, but we can always make a bigger field $\Omega \subset \widetilde{\Omega}$ such that $K \subset \widetilde{\Omega}$ is a normal extension. Now here comes the key point. Composing with the inclusion $\Omega \to \widetilde{\Omega}$ we obtain a natural inclusion

$$\mathrm{Emb}_K(L, \Omega) \to \mathrm{Emb}_K(L, \widetilde{\Omega})$$

and this inclusion is a bijection because by 2. the two sets have the same number $[L : K]_s$ of elements. In other words (and this is the key point): *every K-embedding $\sigma\colon L \to \widetilde{\Omega}$ in fact lands in* Ω. Now we are ready to prove the claim. We know that $f(x)$ splits completely in $\widetilde{\Omega}$. Thus, it is enough to show that if $\mu \in \widetilde{\Omega}$ is a root of$f$, then in fact $\mu \in \Omega$. Arguing as in Part (a) we can construct an embedding $\sigma\colon L \to \widetilde{\Omega}$ such that $\sigma(\lambda) = \mu$. But as we said $\sigma(L) \subset \Omega$ so in fact $\mu = \sigma(\lambda) \in \Omega$ and we are done.

Q 3. (a) It's the field of fractions of $k[T^p]$. Or, check explicitly that if $S = T^p$ then this is just the field of fractions of $k[S]$. Or check that it's a subset containing 0 and 1 and closed under $+ - \times /$.

(b) In fact any subfield of L containing k and T must contain $f(T)$ for any polynomial $f \in k[T]$ and hence it must contain $f(T)/g(T)$ if g is a non-zero polynomial. Hence $L = k(T)$ in the sense that it's the smallest subfield of L containing k and T, so $L = k(T) \subseteq K(T) \subseteq L$ and all inclusions are equalities.

[2]this requires some argument that I am not spelling out: please convince yourself that this is true

(c) T is a root of the polynomial $x^p - T^p \in K[x]$.

(d) If $q(x) = x^p - T^p$ factored in $K[x]$ into two factors f and g of degrees a and b, with $a + b = p$ and $0 < a, b < p$, then by rescaling we can assume both factors are monic. Now consider the factorization $q(x) = (x - T)^p$ in $L[x]$. This is the factorization of $q(x)$ into primes in $L[x]$, and there's only one prime involved, namely $x - T$. Because $q = fg$ in $L[x]$, we must have $f(x) = (x - T)^a$ and $g(x) = (x - T)^b$ – anything else would contradict unique factorization. But this means the constant term of $f(x)$ is $\pm T^a$ and because $0 < a < p$ we know a isn't a multiple of p and hence $\pm T^a \notin K$ and so $f(x) \notin K[x]$, a contradiction.

(e) $q(x)$ is irreducible in $K[x]$ and T is a root, so it's the min poly. It's not separable because it is irreducible over K but has repeated roots in L (namely T, p times).

(f) $T \in L$ is not separable over K because its min poly isn't. Hence L/K is not separable, because L contains an element which is not separable over K.

Q 4. (i) If $L = E(\alpha_1, \ldots, \alpha_n)$ then for $E \subseteq K \subseteq F$ we have that K contains L iff K contains all the α_i. So if $E \subseteq K \subseteq F$ then E contains N iff E contains M and the α_i iff E contains M and L; hence N is the smallest subfield of F containing M and L.

(ii) If L is the splitting field of $p(x) \in E[x]$ and M is the splitting field of $q(x) \in E[x]$ (these polynomials exist by normality) then I claim N is the splitting field of $p(x)q(x)$; indeed if the α_i are the roots of p and β_j are the roots of q then by the first part N is the field generated by the α_i and the β_j. Now N is finite and normal; moreover each of the α_i and the β_j are separable over E (as each is contained in either L or M) and hence each time we adjoin one we get a separable extension; finally a separable extension of a separable extension is separable (by comparing degrees and separable degrees).

(iii) If $g \in \mathrm{Gal}(N/E)$ then $g(L) = L$ by 6.7 and hence the restriction of g to L is in $\mathrm{Gal}(L/E)$. Similar for M/E. So we get a map $\mathrm{Gal}(N/E) \to \mathrm{Gal}(L/E) \times \mathrm{Gal}(M/E)$. This is easily checked to be a group homomorphism. It's injective because anything in the kernel fixes L and M pointwise, so fixes LM pointwise; but $LM = N$.

It's not always surjective though – for example if $L = M$ then it hardly ever is. More generally if $L \cap M \neq E$ then there will be problems. However if $L \cap M = E$ then the map is a bijection.

Q 5. (a) The two polynomials have degree 3 and have no roots in $\mathbb{F}_2$ (just plug $x = 0, 1$) hence they are irreducible.

If $\sigma \colon K \to L$ then $\sigma(\alpha)$ is a root of $f(x)$ in L; and $f(x)$ has three roots in L:

$$\beta + 1; \quad \beta^2 + 1; \quad \beta^2 + \beta$$

indeed, for example, we can check directly that:

$$(\beta + 1)^3 = \beta^3 + \beta^2 + \beta + 1 = (\beta^2 + 1) + \beta^2 + \beta + 1 = \beta = (\beta + 1) + 1$$

that is, $\beta + 1$ is a root of $f(x)$. The other roots of f are $\mathrm{Fr}_2(\beta + 1) = \beta^2 + 1$ and $\mathrm{Fr}_2(\beta^2 + 1) = \beta^4 + 1 = \beta(\beta^2 + 1) + 1 = \beta^2 + 1 + \beta + 1 = \beta^2 + \beta$. (But one can also check directly.)

A basic result about fields states that a morphism from K to L is the same as a root of $f(x)$ in L and there are 3 of these. As f and g are irreducible we know that K and L

have degree 3 over $\mathbb{F}_2$ and we have shown in class that any two finite fields of the same degree over the base field are isomorphic. Since both fields have degree 3 over the base field $\mathbb{F}_2$, all morphisms from K to L are isomorphisms hence there are 3 of these. (This gives another reason why K and L are isomorphic.)

(b) $h(x) \in \mathbb{F}_2[x]$ is irreducible because: it has no roots (plug $x = 0$ and $x = 1$) in $\mathbb{F}_2$ AND it is not divisible by $x^2 + x + 1$, the only irreducible degree two polynomial in $\mathbb{F}_2[x]$ — as can be checked by performing long division in $\mathbb{F}_2[x]$.

Let $L \subset E$ be the splitting field of $h(x)$ as a polynomial in $L[x]$. The extension $\mathbb{F}_2 \subset E$ is normal and separable because ALL finite extensions of finite fields are. Clearly E contains the splitting field $\mathbb{F}_2 \subset F$ of $h(x) \in \mathbb{F}_2[x]$:

$$\begin{tikzcd}
 & E \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash, "3"'] & & F \arrow[dl, dash, "2"] \\
 & \mathbb{F}_4 &
\end{tikzcd}$$

We know that $h(x) \in \mathbb{F}_2[x]$ is irreducible; hence if $\gamma \in F$ is a root of h, then $[\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 4$. We know that every finite extension of a finite field is normal and separable, therefore $\mathbb{F}_2 \subset F$ is normal and hence (by a known characterisation of normal extensions) $h(x)$ splits completely in $\mathbb{F}_2(\gamma)[x]$ — because it is irreducible over $\mathbb{F}_2$ and has a root in $\mathbb{F}_2(\gamma)$ — hence actually $F = \mathbb{F}_2(\gamma)$ and then, as indicated in the diagram, $[F : \mathbb{F}_2] = [\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 4$.

The tower law implies that $3|[E : \mathbb{F}_2]$ and $4|[E : \mathbb{F}_2]$ hence $12|[E : \mathbb{F}_2]$. But clearly also $E = L(\gamma)$ and then $[E : L]$ is the degree of the minimal polynomial of γ over L, which is a factor of h, hence $[E : \mathbb{F}_2] = [E : L][L : \mathbb{F}_2] \leq 12$. So in fact $[E : \mathbb{F}_2] = 12$; $[E : L] = 4$, $h \in L[x]$ is the minimal polynomial of γ and it is therefore irreducible.

Q 6. (This is a pure algebra question.) The $(n-1)$-cycle c must fix an element of $[n]$[3] which we may well assume to be 1, and then after re-labelling the elements of $[n]$ we may assume that $c = (23 \dots n)$. Let t be the transposition; then:

Either t involves 1, and then by further relabelling elements we may assume $c = (23 \cdots n)$, $t = (12)$, and it is easy to conclude from here;

Or $t = (ab)$ where $1 < a < b$: this is what we assume from now on.

Because G is transitive, it must contain an element σ such that $\sigma(a) = 1$, but then $\sigma t \sigma^{-1} = (1\sigma(b))$ and we are back in the previous case.

Q 7. We look at the polynomial modulo small primes:[4] Modulo $p = 2$ we get:

[3]Notation: $[n] = \{1, 2, \dots, n\}$ is the set with n elements.

[4]In this and the next questions we use the following result which was proved in class: **THEOREM** Let $f(X) \in \mathbb{Z}[X]$ be monic of degree n, $p \geq 1$ a prime such that the reduction mod p $\overline{f}(X) \in \mathbb{F}_p[X]$ has distinct roots and factors as a product of irreducible factors of degree $n_1, \dots, n_k$. Then the Galois group G of the splitting field $\mathbb{Q} \subset L$ of f contains a permutation of the roots of f whose cycle decomposition is $(n_1)(n_2) \cdots (n_k)$.

$$f(x) = x^6 - 12x^4 + 15x^3 - 6x^2 + 15x + 12 \equiv x(x^5 + x^2 + 1) \mod 2$$

where the second polynomial $r(x) = x^5 + x^2 + 1$ is irreducible because if it weren't it would split an irreducible degree two polynomial, but the only such polynomial is $x^2 + x + 1$ which does not divide into $r(x)$ (direct inspection). By the theorem in the footnote, the Galois group G contains a 5-cycle.

Eisenstein at $p = 3$ shows that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and in turn this implies that G is transitive.

Next:

$$f(x) \equiv (x+1)(x+2)(x+3)(x+4)(x^2+3) \mod 5$$

thus by the theorem in the footnote G contains a transposition.

By Question 6 $G = \mathfrak{S}_6$.

Q 8. (a) Let us first consider the polynomial in $\mathbb{F}_2[x]$. Clearly $x = 1$ is a root of $f(x)$ and a small calculation shows

$$x^4 + x^2 + x + 1 = (x+1)(x^3 + x^2 + 1) \quad \text{in} \quad \mathbb{F}_2[x]$$

and then $x^3 + x + 1 \in \mathbb{F}_2[x]$ is irreducible because it has no roots in $\mathbb{F}_2$ (just plug in $x = 0$ and $x = 1$).

Next, we work in $\mathbb{F}_3[x]$. A quick inspection shows that $f(x)$ has no roots in $\mathbb{F}_3$: just plug $x = 0, 1, -1$. To show that the polynomial $f(x) \in \mathbb{F}_3[x]$ is irreducible, we show that it is not divisible by any of the three irreducible degree 2 polynomial in $\mathbb{F}_3[x]$: these are:

$$x^2 + 1, \quad x^2 + x - 1, \quad x^2 - x - 1$$

Performing three long divisions in $\mathbb{F}_3[x]$ we see:

$$\begin{aligned} x^4 + x^2 + x + 1 &= (x^2+1)(x^2) + x + 1 \\ x^4 + x^2 + x + 1 &= (x^2+x-1)(x^2-x) + 1 \\ x^4 + x^2 + x + 1 &= (x^2-x-1)(x^2+x) - x + 1 \end{aligned}$$

these calculations show that f is irreducible in $\mathbb{F}_3[x]$.

(b) A result proved in class implies that the Galois group G of the splitting field $\mathbb{Q} \subset K$ contains a 3-cycle and a 4-cycle. If a subgroup G of $\mathfrak{S}_4$ contains a 3-cycle and a 4-cycle then $G = \mathfrak{S}_4$. (See Question 9 below.) Therefore, $G = \mathfrak{S}_4$.

Q 9. (a) First, working modulo 2,

$$f(X) \equiv X^4 + 3X + 1 \in \mathbb{F}_2[X]$$

is irreducible. Indeed, by inspection, it does not have a root in $\mathbb{F}_2$, and it is not divisible by the only irreducible degree 2 monic polynomial $x^2 + x + 1 \in \mathbb{F}_2[X]$. In fact long division gives

$$X^4 + X + 1 = (X^2 + X + 1)(X^2 + X) + 1$$

Next, it is easy to factor $f(X)$ mod 5:[5]

$$f(X) \equiv (X-1)(X^3+X^2+X-1) \in \mathbb{F}_5[X]$$

where the degree 3 factor is irreducible because, by inspection, it has no root in $\mathbb{F}_5$.

(b) Suppose that $G \subset \mathfrak{S}_4$ contains a 4-cycle and a 3-cycle. Let the 4-cycle be $s = (abcd)$. Note that we can write $s = (dabc)$, etc. Thus, we may assume that the 3-cycle t fixes the last letter d in the 4-cycle. Now either $t = (abc)$ or $t = (acb)$, but then $t^2 = (abc)$. The conclusion is that we may assume $s = (1234)$, $t = (123)$. You take it from here.

(c) By Part (a) and the theorem in the footnote, the Galois group contains a 4-cycle and a 3-cycle hence, by Part (b) it must be all of $\mathfrak{S}_4$.

Q 10. With all the hints and the examples, this should not be too hard. You do it (or else ignore this question).

Q 11. (a) $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$ and

$$\zeta = \frac{1+\mathtt{i}\sqrt{3}}{2} \quad \text{is a root of} \quad \Phi_6(x) = x^2 - x + 1 \in \mathbb{Q}[x]$$

Since $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ is the splitting field of $\Phi_6(x)$, we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.

(b) The polynomial $x^6+3 \in \mathbb{Q}[x]$ is irreducible by the Eisenstein criterion. By an elementary fact on fields, if $\alpha \in K$ is a root, that is $\alpha^6 = -3$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Now $\beta = \alpha^3$ satisfies:

$$\beta^2 = -3,$$

in other words, $\beta = \pm\mathtt{i}\sqrt{3}$ and we have a tower of fields:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta) = \mathbb{Q}(\mathtt{i}\sqrt{3}) \subset \mathbb{Q}(\alpha)$$

Since $K = \mathbb{Q}(\zeta, \alpha)$ and $\zeta \in \mathbb{Q}(\alpha)$, we have in fact $K = \mathbb{Q}(\alpha)$, so from above $[K : \mathbb{Q}] = 6$. The Galois group G permutes the roots of $f(x) = x^6+3$ so consider $\sigma \in G$, then $\sigma(\alpha) = \zeta^k\alpha$ for a unique $k \in \mathbb{Z}/6\mathbb{Z}$, and — ideally — I would like you to have checked that the assignment $\sigma \mapsto k$ is an isomorphism $G \cong \mathbb{Z}/6\mathbb{Z}$. (It is an injective group homomorphism and $|G| = 6$.)

(c) As before $x^6 - 3 \in \mathbb{Q}[x]$ is irreducible. Let $\alpha \in \mathbb{R}$, $\alpha^6 = 3$. As before $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ but now, because $\mathbb{Q}(\alpha) \subset \mathbb{R}$, $\zeta \notin \mathbb{Q}(\alpha)$ and $\Phi_6(x)$ remains irreducible in $\mathbb{Q}(\alpha)$. We have a diagram of fields

$$\begin{tikzcd}
 & K \arrow[dl, dash, "2"'] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "6"'] & & \mathbb{Q}(\mathtt{i}\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

[5] Working mod 3 is not going to lead to useful information: it is clear by inspection that $f(X)$ has no root in $\mathbb{F}_3$ and then either $f(X)$ is irreducible (no useful conclusion) or it splits into two quadratic polynomials (again no useful conclusion).

The diagram shows that $[K : \mathbb{Q}] = 12$. The situation at this point is similar to $x^4 - 2 \in \mathbb{Q}[x]$ — which was discussed at length in class — and you can treat it in a similar fashion: an element $\sigma \in G$ is completely determined once you know: $\sigma(\alpha)$ (6 possibilities) and $\sigma(\zeta)$ (two possibilities) for a total of 12 possibilities. Because $|G| = 12$ all these possibilities are realised, and it is not hard to see that one gets the dihedral group $\mathbb{D}_{12}$.

Q 12. I am sorry, I can't write this down for you. You do it: it is fun!