M3P11 (and M4P11, M5P11) Galois Theory, Solutions to Worksheet 2

Alessio Corti

10th March 2020

Q 1. (i) γ clearly satisfies $(\gamma^3-1)^2=3$, so it's a root of the polynomial $(x^3-1)^2-3$ which is x^6-2x^3-2. By the Eisenstein criterion this polynomial is irreducible, so it must be the min poly of γ, and the degree of γ over $\mathbb{Q}$ is 6.

Note that $\sqrt{3}=\gamma^3-1\in\mathbb{Q}(\gamma)$ so if $F=\mathbb{Q}(\gamma)$ and $K=\mathbb{Q}(\sqrt{3})$ we must have $\mathbb{Q}\subseteq K\subseteq F$ and the tower law gives $2[F:K]=[K:\mathbb{Q}][F:K]=[F:\mathbb{Q}]=6$, and we deduce $[F:K]=3$. Because F contains $\sqrt{3}$ it must contain K and it's not hard to deduce that $F=K(\gamma)$. By the tower law again, the degree of γ over K must then be 3.

Note that if one could show that $x^3-(1+\sqrt{3})$ were irreducible in $K[x]$ then this would be another way to do the question, but I did not explain any techniques for tackling this.

(ii) Even more evil trick question. Turns out $\delta=1+\sqrt{3}$ (cube it out to check) so the degree is 2 over $\mathbb{Q}$ and also over $\mathbb{Q}(\sqrt{2})$, the latter because we saw in some previous question that $\delta\notin\mathbb{Q}(\sqrt{2})$ (it would imply $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$).

Q 2. (a) Well $z^3=\omega^3\alpha^3=1\times 2=2$ so z is a root of $x^3-2=0$, which is irreducible over $\mathbb{Q}$ because it has no root in $\mathbb{Q}$, so x^3-2 is the min poly of z, and by what we did in class this means $[\mathbb{Q}(z):\mathbb{Q}]=3$. Although we don't need it, we can note that in fact $\mathbb{Q}(z)$ is isomorphic to, but not equal to, $\mathbb{Q}(\alpha)$, as an abstract field.

(b) We know $\omega^3=1$ but $\omega\neq 1$ so ω is a root of $(x^3-1)/(x-1)=x^2+x+1$. This polynomial is irreducible as it has no rational (because no real) roots, so $[\mathbb{Q}(\omega):\mathbb{Q}]=2$. Note also while we're here that solving the quadratic gives $\omega=\frac{-1+i\sqrt{3}}{2}$ (plus sign because the imaginary part of ω is positive; the other root is ω^2).

(c) We have $\alpha\in\mathbb{R}$. Furthermore $\overline{\omega}$ is another cube root of 1 so it must be ω^2. Hence $\overline{z}=\overline{\omega\alpha}=\omega^2\alpha=\omega z$. In particular if $\overline{z}\in\mathbb{Q}(z)$ then $\omega=\overline{z}/z\in\mathbb{Q}(z)$. This means $\mathbb{Q}(\omega)\subseteq\mathbb{Q}(z)$, and by the first two parts and the tower law we deduce $[\mathbb{Q}(z):\mathbb{Q}(\omega)]=\frac{3}{2}$, which is nonsense because the dimension of a (finite-dimensional) vector space is a whole number.

(d) If $x\in\mathbb{Q}(z)$ then $\overline{z}=-z+2x\in\mathbb{Q}(z)$, contradiction. So x is not in. If $i\in\mathbb{Q}(z)$ then $\mathbb{Q}(i)\subseteq\mathbb{Q}(z)$ and this contradicts the tower law like in part(c). Finally because the imaginary part of ω is $\sqrt{3}/2$ we see $y=\alpha\sqrt{3}/2$, so if $y\in\mathbb{Q}(\omega)$ then $y^3=3\alpha^3/8\sqrt{3}=3/4\sqrt{3}\in\mathbb{Q}(z)$, implying $\sqrt{3}\in\mathbb{Q}(z)$ which again contradicts the tower law.

Q 3. (a) We know 0 is the additive identity in R so $0+0=0$. Hence $0x=(0+0)x=0x+0x$ and subtracting $0x$ (which we can do, because $(R,+)$ is a group so $0x$ has an additive inverse) we deduce $0=0x$.

(b) If $a\neq 0$ and $b\neq 0$ then there exist multiplicative inverses a^{-1} and b^{-1}, and now $abb^{-1}a^{-1}=1\times 1=1$. However if $ab=0$ then we deduce $0(b^{-1}a^{-1})=1$ which contradicts part (a) (as $0\neq 1$ in a field).

(c) Look at top degree terms.

(d) $fh=gh$ implies $(f-g)h=0$, and if $h\neq 0$ we must have $f-g=0$ by (c).

Q 4. (i) Spot root $x=2$; so $x^3-8=(x-2)(x^2+2x+4)$ and roots of the quadratic are non-real and hence non-rational, so the quadratic must be irreducible (as any factors would be linear).

(ii) Irreducible by Eisenstein ($p=2$ or $p=3$).

(iii) The polynomial x^2-2x+2 is a factor; dividing out we see $x^4+4=(x^2-2x+2)(x^2+2x+2)$. Easy check now that both quadratics have non-real and hence non-rational roots, so must be irreducible.

(iv) Either this is irreducible over $\mathbb{Q}$, or there is a root in $\mathbb{Q}$ (because any factorization must involve a linear term). So let's substitute in $x=p/q$ in lowest terms (i.e. $\gcd(p,q)=1$) and see what happens. Clearing denominators we get

$$2p^3+5p^2q+5pq^2+3q^3=0.$$

Now p divides the first three terms of the left hand side, so must divide the fourth which is $3q^3$. But p and q are coprime! So p must divide 3. A similar argument shows that q must divide 2. So $p=\pm 1$ or ± 3 and $q=\pm 1$ or ± 2. Clearly no positive rational is a root (as all the coefficients are positive) so we are left with the possibilities $x=-1,-1/2,-3,-3/2$ and we just try all of them. Miraculously $x=-3/2$ does work! Pulling off the corresponding linear factor gives

$$2x^3+5x^2+5x+3=(2x+3)(x^2+x+1)$$

and the quadratic term has no real roots and hence no rational ones, so this is the factorization into irreducibles.

(v) This one is irreducible by Eisenstein with $p=3$.

(vi) There's an obvious factor of $x-1$ and the other factor $x^{72}+x^{71}+\cdots+x+1$ is irreducible. To see this first substitute $y=x-1$, then apply Eisenstein with $p=73$ prime.

(vii) This polynomial is obtainable from the polynomial in part (vi): start with the part (vi) polynomial, change x to $-x$ and then change the sign of the polynomial. These sorts of things do not affect things like irreducibility and factorization, so the factorization will be $(x+1)(x^{72}-x^{71}+\ldots-x+1)$ and the degree 72 polynomial will be irreducible.

(viii) Spot roots $x=1$ and $x=-1$. Over the complexes we have more roots too, like $\pm i$ and so on – how do these control factorization over the rationals? Well $(x-i)$ and $(x+i)$ are factors over the complexes, so their product x^2+1 is a factor over the complexes and hence also over the rationals. Similarly the two complex cube roots of 1 are complex conjugates and are the two roots of x^2+x+1, and the two 6th roots of 1 that we haven't mentioned yet ($e^{\frac{2\pi i}{6}}$ and its complex conjugate) are roots of $x^2 - x + 1$. So we've just spotted factors whose degrees add up to 8. Let's see what we have so far then: the factors we have spotted are

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

and so what is left is

$$\begin{aligned} &(x^{12}-1)/(x^4-1)(x^4+x^2+1) \\ &= (x^8+x^4+1)/(x^4+x^2+1) \\ &= x^4-x^2+1 \end{aligned}$$

The hardest part of this question is figuring out whether that last polynomial $x^4 - x^2 + 1$ factors.

Q 5. The min poly of α must be $x^{10} - 2$ because this is irreducible over $\mathbb{Q}$ (by Eisenstein) and has α as a root. In particular there is no non-zero polynomial of degree at most 9 with rational coefficients and α as a root, so $\{1, \alpha, \alpha^2, \ldots, \alpha^9\}$ are linearly independent elements in a vector space of dimension 10, and hence are a basis.

Q 6. (i) To check that a subset of a field is a subfield all we need to do is to check 0 and 1 are in, and that the subset is closed under addition, subtraction, multiplication, and division-by-things-that-aren't-zero. These things follow from the tower law: if α, β are algebraic then $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] < \infty$, but then

$$[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\beta) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$$

But then for all $\lambda \in \mathbb{Q}(\alpha, \beta)$ $[\mathbb{Q}(\lambda) : \mathbb{Q}] < \infty$, i.e., λ is algebraic.

(ii) Say for a contradiction that $[A : \mathbb{Q}] = n < \infty$. Let $p(x) = x^{n+1} - 2$ and let $\alpha \in \mathbb{C}$ be a root. Then α is algebraic and its min poly must be $p(x)$ as $p(x)$ is monic and irreducible. So $n = [A : \mathbb{Q}] = [A : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = (n+1)[A : \mathbb{Q}(\alpha)] \geq n+1 > n$, a contradiction.

(iii) For each n there are only countably many elements of $\mathbb{Q}[x]$ with degree at most n, and a countable union of countable sets is countable, so there are only countably many polynomials. Each algebraic number is a root of a non-zero polynomial in $\mathbb{Q}[x]$ and such a polynomial has only finitely many roots, and a countable union of finite sets is countable, so A is countable.

(iv) If $[\mathbb{C} : A]$ were finite then $\mathbb{C}$ would be isomorphic to A^n for some $n \in \mathbb{Z}_{\geq 1}$ and hence $\mathbb{C}$ would be countable, a contradiction.

Q 7. This is tedious and I am not going to do it; but I will make a few comments.

A polynomial of degree ≤ 3 in $\mathbb{F}_p[x]$ is irreducible if and only if it has no roots in $\mathbb{F}_p$, and this can be checked by evaluating at all elements $0, \ldots, p-1 \in \mathbb{F}_p$.

For example with $p = 2$ the only irreducible quadratic polynomial is:

$$x^2 + x + 1$$

and the irreducible cubic polynomials are:

$$x^3 + x + 1, \quad x^3 + x^2 + 1$$

For $p = 3$ there are 3 irreducible monic quadratic polynomials; they are:

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

On the other hand, if you understand some of what we (by now) said about finite fields, there are $(27 - 3)/3 = 8$ irreducible monic cubic polynomial, and it should not be too time-consuming to write them all down.

For $p = 5$, again if you understand the last part of the question in Test 2, there are $(25-5)/2 = 10$ irreducible monic quadratic (not too bad to list them all) and $(125-5)/3 = 40$ irreducible monic cubic polynomials in $\mathbb{F}_5[x]$ (OK so to do this by hand would be a bit ridiculous. You can write your own computer program if you wish, or find a table on the 'net).

Q 8. (a) The statement is obvious if b is a square in K so let us assume that it is not. Suppose that there are $x, y \in K$ such that

$$a = (x + y\sqrt{b})^2 = (x^2 + by^2) + 2xy\sqrt{b}$$

Since $1, \sqrt{b}$ are linearly independent over K, we must have that **either**

(i) $y = 0$, in which case $a = x^2$ is a square in K, **or**

(ii) $x = 0$, in which case $a = y^2 b$ and then $ab = (yb)^2$ is a square in K.

(b) Suppose say that $a + \beta$ is a square in L. This means that there are $x, y \in K$ such that

$$a + \beta = (x + y\beta)^2 = (x^2 + y^2 b) + 2xy\beta$$

but then $a - \beta = (x - y\beta)^2$ is also a square in L, and

$$c = a^2 - b = (a + \beta)(a - \beta) = [(x + y\beta)(x - y\beta)]^2 = [x^2 - y^2 b]^2$$

is a square in L.

(c) The roots are $\pm\sqrt{a \pm \sqrt{b}}$; so choose $\beta, \alpha, \alpha' \in L$ such that $\beta^2 = b$, $\alpha^2 = a + \beta$, ${\alpha'}^2 = a - \beta$. We work with the diagram

$$\begin{tikzcd}
 & L & \\
K(\alpha) \arrow[ur] & & K(\alpha') \arrow[ul] \\
 & K(\beta) \arrow[ul] \arrow[ur] & \\
 & K \arrow[u] &
\end{tikzcd}$$

First, $[K(\beta) : K] = 2$ since we are assuming that b is not a square in K.

Write $K_1 = K(\beta)$. I **claim** that $[K(\alpha) : K_1] = 2$. Indeed, by Part (b), if $a + \beta$ were a square in K_1, then also $a - \beta$ would be a square in K_1 and then $c = (a+\beta)(a-\beta) = a^2 - b$ is a square in K, contradicting one of our assumptions.

Similarly, also $[K(\alpha') : K_1] = 2$.

The conclusion of Part (c) follows from the tower law and the **new claim**: $K_1(\alpha) \neq K_1(\alpha')$. Indeed suppose for a contradiction that $\alpha' \in K_1(\alpha)$: this is saying that $a - \beta$ is a square in $K_1(\sqrt{a+\beta})$. From Part (a) with $u = a - \beta$ and $v = a + \beta$ in K_1, we conclude that **either**:

(i) $a - \beta$ is a square in K_1, contradicting the claim proved that $[K_1(\alpha') : K_1] = 2$, **or**:

(ii) $c = (a-\beta)(a+\beta) = a^2 - b$ is a square in K_1.

Since the first alternative led to a contradiction, it must be that c is a square in K_1. We apply Part (a) again with $u = c$, $v = b$ in K. We have c a square in $K(\sqrt{b})$, that is, either c or cb is a square in K, contradicting our assumptions. This final contradiction shows that $K_1(\alpha) \neq K_1(\alpha')$ and finishes Part (c).

Q 9. It is easy to see that (ii) implies (i) and here I focus on proving that (i) implies (ii).

The key thing to understand is this: **Claim** If $\mathrm{char}(K) \neq 2$ then every extension $K \subset L$ of degree $[L : K] = 2$ is of the form $L = K(\alpha)$ for some $\alpha \in L$ such that $\alpha^2 \in K$. I am going to leave out the proof of the Claim (hint: quadratic formula) and I will use it to answer the question.

So assume (i), then by the tower law $[L : E] = 2$ and $[E : K] = 2$ and by the Claim $L = E(\alpha)$ for some $\alpha \in L$ with $\alpha^2 \in E$. Also $E = K(\beta)$ where $\beta^2 \in K$. Hence we can write $\alpha^2 = u + v\beta$ with $u, v \in K$, so

$$(\alpha^2 - u)^2 = v^2\beta^2 \in K$$

hence α is a root of the polynomial

$$f(X) = (X^2 - u)^2 - v^2\beta^2 = X^4 - 2uX^2 + (u^2 - v^2\beta^2) \in K[X]$$

which is of the required form. If $f(X) \in K[X]$ is irreducible then we are done.

So what if $f(X)$ is not irreducible? This is *really awkward*! In that case by the tower law $[K(\alpha) : K] = 2$ and the minimal polynomial of α over K is a quadratic polynomial

$$X^2 + cX + d \in K[X]$$

and necessarily $c = 0$, otherwise $\alpha = \frac{-\alpha^2 - d}{c} \in E$, a contradiction. Hence in fact $\alpha^2 \in K$ and we have extensions:

$$\begin{tikzcd}
 & L = K(\alpha, \beta) & \\
E = K(\beta) \arrow[ur] & & F = K(\alpha) \arrow[ul] \\
 & K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

where $\beta^2 = b \in K$ and $\alpha^2 = a \in K$ BUT also, clearly, $\alpha \notin K(\beta)$ and $\beta \notin K(\alpha)$.

Remark there is a third field, $G = K(\alpha\beta)$, *distinct* from E, F, and also of degree $[G : K] = 2$. Note also that $(\alpha\beta)^2 = ab \in K$. (I leave all this to you to sort out.)

I now want to work with the element $\alpha + \beta \in L$: I claim that it has degree 4 over K, and then $L = K(\alpha + \beta)$ and, since

$$(\alpha + \beta)^2 = a + b + 2\alpha\beta \in G, \tag{1}$$

the argument above shows that the minimal polynomial of $\alpha + \beta$ has the required form.

Suppose for a contradiction that $\alpha + \beta$ satisfies a quadratic polynomial

$$X^2 + AX + B \in K[X]$$

If $A = 0$ then we have that $(\alpha + \beta)^2 = -B \in K$, and this implies (by Equation 1) that $\alpha\beta \in K$, a contradiction. If $A \neq 0$ then $\alpha + \beta = \frac{-(\alpha+\beta)^2 - B}{A} \in G$ (Equation 1 again) and the polynomial

$$g(X) = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta$$

is in $G[X]$. This polynomial is irreducible, otherwise its roots α, β already belong to G, so $L = G$ and we get a contradiction in too many ways (for instance $[L : K] = [G : K] = 2$). But then $g(X)$ equals $X^2 - a$, the minimal polynomial of α over $K[X]$, and this then leads to a contradiction in too many ways (for instance it implies that $\alpha = -\beta$).

Q 10. This is not difficult at all. Go back to your notes of the discussion of $X^3 - 2$ at the beginning of the course and make the appropriate minor changes.

Q 11. Let's start by adjoining one root of $x^4 - p$, say, α, the positive real 4^{th} root of p. We get a field $K = \mathbb{Q}(\alpha)$. By Eisenstein, $x^4 - p$ is irreducible over $\mathbb{Q}$, so $[K : \mathbb{Q}] = 4$. Is K a splitting field? No, because it's a subfield of the reals, and $x^4 - p$ has some non-real roots (namely $\pm \mathtt{i}\alpha$). However K does contain two roots of $x^4 - p$, namely $\pm\alpha$, so $x^4 - p$ must factor as $(x + \alpha)(x - \alpha)q(x)$, with $q(x) \in K[x]$ of degree 2 and irreducible (as no roots in K). If $\beta = \mathtt{i}\alpha$ is a root of $q(x)$ and $F = K(\beta)$ then $[F : K] = 2$ so $[F : \mathbb{Q}] = 8$ by the tower law. We can alternatively write $F = K(\mathtt{i})$ as $\beta = \mathtt{i}\alpha$, so $F = \mathbb{Q}(\mathtt{i}, \alpha)$.

F is a splitting field over $\mathbb{Q}$ so it's finite, normal and separable (separability isn't an issue as we're in characteristic 0). So we know $\mathrm{Gal}(F/\mathbb{Q})$ has size 8. We also know that if $\tau : F \to F$ is an isomorphism then $\tau(\alpha)$ had better be a 4^{th} root of $\tau(p) = p$, so it's $\pm\alpha$ or $\pm\mathtt{i}\alpha$; there are at most 4 choices for $\tau(\alpha)$. Similarly $\tau(\mathtt{i}) = \pm\mathtt{i}$ so there are at most 2 choices for $\tau(\mathtt{i})$. This gives at most 8 choices for τ; however we know that $\mathrm{Gal}(F/\mathbb{Q})$ has size 8, so all eight choices must work. It is not hard now to convince yourself that $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to D_8 (think of a square with corners labelled $\alpha, \mathtt{i}\alpha, -\alpha, -\mathtt{i}\alpha$).