M3P11 (and M4P11, M5P11) Galois Theory, Solutions to Worksheet 1

Alessio Corti

9th March 2020

Q 1. (a) Doing long division we see $x^5 + x + 1 = (x^3 - x)(x^2 + 1) + 2x + 1$ so the quotient is $x^3 - x$ and the remainder is $2x + 1$.

(b) If $x^{2019} + 32x^{53} + 8 = q(x)(x-1) + r(x)$ then either $r(x) = 0$ or $\deg(r) < \deg(x-1) = 1$ so in either case r is a constant. Evaluating the equation at $x = 1$ shows us that $r(x) = 1 + 32 + 8 = 41$.

(c)

$$\begin{aligned} 2x^3 + 2x^2 + 3x + 2 &= (2x + 2)(x^2 + 1) + x \\ x^2 + 1 &= (x)(x) + 1 \\ x &= x \times 1 + 0 \end{aligned}$$

so the last non-zero remainder is 1. Now working backwards,

$$\begin{aligned} 1 &= (x^2 + 1) - (x)(x) \\ &= (x^2 + 1) - x[2x^3 + 2x^2 + 3x + 2 - (2x + 2)(x^2 + 1)] \\ &= (2x^2 + 2x + 1)(x^2 + 1) - x(2x^3 + 2x^2 + 3x + 2) \end{aligned}$$

so, if I got it right, one possibility is $s(x) = -x$ and $t(x) = 2x^2 + 2x + 1$. If you got another solution it doesn't mean you are wrong, because there is more than one answer to this sort of question just as in the case of usual integers—for example, you can add $x^2 + 1$ to s and subtract $2x^3 + 2x^2 + 3x + 2$ from t and get a new solution that still works (another bonus question: what's the most general solution? Can you prove it?).

Bonus part: I knew they were coprime in $\mathbb{Q}[x]$ because they have no roots in common in the bigger ring $\mathbb{C}[x]$ – it's easy to check this because the roots of $x^2 + 1$ are $\pm i$ and neither of these is a root of $2x^3 + 2x^2 + 3x + 2$, as you can see by substituting in. Can you see why this is enough?

(d) Euclid again:

$$\begin{aligned} x^4 + 4 &= x(x^3 - 2x + 4) + 2x^2 - 4x + 4 \\ x^3 - 2x + 4 &= (x/2 + 1)(2x^2 - 4x + 4) + 0 \end{aligned}$$

and after that mercifully short procedure we see that the last non-zero remainder is $2x^2 - 4x + 4$. Now hcf's don't really care about constants, so $x^2 - 2x + 2$ is another hcf which is kind of nicer (in my opinion), but let's work with what we have and go backwards:

$$2x^2 - 4x + 4 = (x^4 + 4) - x(x^3 - 2x + 4)$$

oh and that's it isn't it – there are serious advantages to Euclid only taking 2 steps! So $a(x) = 1$ and $b(x) = -x$. Actually I see now that the "nicer" hcf wasn't perhaps so nice because then we would have had fractions in a and b.

(e) Just one long division gives:

$$-\frac{1}{3}(x^3 - 2) + \frac{x^2 - x + 1}{3}(x + 1) = 1$$

Q 2. (a) The previous question, part (e), suggests that we take $a = 1/3$, $b = -1/3$, $c = 1/3$.

(b) The matrix of multiplication by $A + B\xi + \xi^2$ in the basis $1, \xi, \xi^2$ is:

$$T = \begin{pmatrix} A & 2 & 2B \\ B & A & 2 \\ 1 & B & A \end{pmatrix}$$

We find a, b, c by solving the system:

$$T \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

The Cramer rule gives, setting

$$D = \det T = A^3 + 2B^3 - 6AB + 4,$$

the expressions:

$$a = \frac{A^2 - 2B}{D}, \quad b = \frac{-AB + 2}{D}, \quad c = \frac{B^2 - A}{D}$$

(What does $D = 0$ mean?)

Q 3. The hcf has the property that all other common divisors divide it. So by definition $s \mid t$ and $t \mid s$, so looking at top degree terms we deduce that the degrees of s and t must be equal, and $s = tr$ for a polynomial r of degree 0, that is, a non-zero constant.

Q 4. (a) Divide g by f in $K[x]$ and get a quotient and a remainder, and then pretend eveything is in $L[x]$ and use uniqueness of quotient and remainder to do this part immediately.

(b) First part no, e.g. $2x + 2 \mid x + 1$ in $\mathbb{Q}[x]$. Second part yes, and again prove it by figuring out $q(x)$ such that $g(x) = f(x)q(x)$ by long division and noting that you only ever have to divide by 1 when figuring out the coefficients of g.

Q 5. (a) If $\sqrt{n} = p/q$ in lowest terms (with $p, q \in \mathbb{Z}$ and $q \neq 0$) then we deduce that $nq^2 = p^2$. In particular q^2 divides p^2 – but q^2 and p^2 are coprime, so $q^2 = 1$, so $p/q \in \mathbb{Z}$.

(b) We know $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. We now prove $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ by contradiction.

If $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ then squaring both sides and tidying up, we deduce $2ab\sqrt{2} \in \mathbb{Q}$. But $\sqrt{2} \notin \mathbb{Q}$ by part (a), so $2ab = 0$, so either $a = 0$ or $b = 0$. If $b = 0$ then

$\sqrt{3} \in \mathbb{Q}$, contradicting part (a). If $a = 0$ then $\sqrt{3} = b\sqrt{2}$ and multiplying both sides by $\sqrt{2}$ we deduce $\sqrt{6} \in \mathbb{Q}$, also contradicting part (a). Either way we're there, so $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

The min poly of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ must then be x^2-3. Why? It's monic, and has coefficients in the right field, so the only issue is whether it's irreducible. And it is, because if it factored then it would have to factor into two linear factors, and one of them would be (up to a constant) $x - \sqrt{3}$, but we've just shown that this polynomial does not have coefficients in $\mathbb{Q}(\sqrt{2})$.

(c) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$. We know both extensions on the right have degree 2; for one it's clear and for the other it comes from part (b) and a result proved in class ($[K(\lambda) : K]$ is the degree of the minimal polynomial of λ over K).

Q 6. (a) If $\alpha = \sqrt{2} + \sqrt{3}$ then $\alpha^2 = 5 + 2\sqrt{6}$ and hence $\sqrt{6} = (\alpha^2 - 5)/2 \in \mathbb{Q}(\alpha)$. Hence $\beta := \sqrt{6}\alpha = \sqrt{12} + \sqrt{18} = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\alpha)$. So $\sqrt{2} = \beta - 2\alpha \in \mathbb{Q}(\alpha)$ and now $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$.

We deduce that $\mathbb{Q}(\alpha)$ contains $\sqrt{2}$ and $\sqrt{3}$, so it contains $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. The converse inclusion is obvious, so the two fields are equal.

(b) $p(x) = x^4 - 10x^2 + 1$ can be checked to be a polynomial in $\mathbb{Q}[x]$ such that $p(\alpha) = 0$. Hence it is a multiple of the minimal polynomial of α. But part (a) and $[\mathbb{Q}(\alpha) : \mathbb{Q}] =$ deg(minimal poly. of a) imply that the degree of the min poly of α is 4, so $p(x)$ must be a constant multiple of this min poly, so it must be the min poly, so it must be irreducible.

Q 7. Answer is yes! It's $\frac{1}{3}\sqrt{6}\sqrt{15}$.

Q 8. If $[L : K]$ is infinite then E has an infinite-dimensional K-subspace and hence must be infinite-dimensional over K (for any $n \geq 1$ we can choose n K-linearly independent elements of L and these give n K-linearly independent elements of E).

If $[E : L]$ is infinite, then $[E : K]$ must also be infinite, because for any n we can choose n elements of E that are L-linearly independent, and these are easily checked to also be K-linearly independent.

Q 9. (a) This is a variant of the Tower Law argument: Let $e_1, \ldots, e_n$ be a basis for L/K and $f_1, \ldots, f_m$ be a basis for V/L. Then $e_i \in L$ and $f_j \in V$, and V is an L-vector space, so $g_{ij} = e_i f_j$ makes sense. Of course the claim is that the g_{ij} form a basis for V considered as a K-vector space, and the same proof as in the tower law works: the g_{ij} span because if $v \in V$ then write v as an L-linear combination of the f_j and then write each coefficient as a K-linear combination of the e_i, and multiply out. For linear independence, if a linear combination $\sum_{i,j} \mu_{ij} g_{ij} = 0$ then write this as $\sum_j (\sum_i \mu_{ij} e_i) f_j = \sum_j \lambda_j f_j$ and by linear independence of the f_j over L we know the λ_j must be zero, and this means the μ_{ij} are all zero by linear independence of the e_i over K.

(b) So?

Q 10. Long division (for example) of $f(X)$ by $X - \alpha$ yields:

$$f(X) = (X - \alpha)\Big(X^2 + \alpha X + (-3 + \alpha^2)\Big) \in L[X]$$

The quadratic formula for $g(X)$ needs the square root of

$$\Delta = b^2 - 4ac = \alpha^2 - 4(-3+\alpha^2) = 12 - 3\alpha^2$$

which is explicitly shown to be a square in the hint.

[Note: if $\operatorname{char}(K) = 3$, then $f(x) = x^3 + 1 = (x+1)(x^2 - x + 1)$ is not irreducible.]

Q 11. (a) We have

$$u \mapsto \alpha_2 + \omega\alpha_3 + \omega^2\alpha_1 = \omega u$$

and, similarly, $v \mapsto \omega^2 v$.

(b) Using that $\omega + \omega^2 = -1$ and $\alpha_1 + \alpha_2 + \alpha_3 = 0$, we get, for example:

$$\frac{u+v}{3} = \frac{\alpha_1 + \alpha_1 - \alpha_2 - \alpha_3}{3} = \alpha_1$$

and, similarly, $\alpha_2 = \frac{\omega^2 u + \omega v}{3}$, $\alpha_3 = \frac{\omega u + \omega^2 v}{3}$.

(c) It is pretty obvious that $\tau(u) = v$ and $\tau(v) = u$. The rest of this question requires considerable work and we may return to this point later in the lectures, when we study the Galois group of splitting fields of cubic polynomials in general.

We must use the following facts from M1F:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad (\alpha_2\alpha_3 + \alpha_1\alpha_3 + \alpha_1\alpha_2) = 3p, \quad \alpha_1\alpha_2\alpha_3 = -2q$$

We will also need to use the (elementary) algebraic identity:

$$(z_1 + z_2 + z_3)(z_2z_3 + z_1z_3 + z_1z_2) = (z_1^2z_2 + z_1^2z_3 + z_1z_2^2 + z_2^2z_3 + z_1z_3^2 + z_2z_3^2) + 3z_1z_2z_3$$

We compute by brute force uv and $u^3 + v^3$: from these quantities it is easy to construct the sought-for quadratic equation. A direct calculation (using $\omega + \omega^2 = -1$!) shows that:

$$uv = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -9p$$

and:

$$\begin{aligned} u^3 + v^3 &= 2(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) - 3(\alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_1\alpha_2^2 + \alpha_2^2\alpha_3 + \alpha_1\alpha_3^2 + \alpha_2\alpha_3^2) + 12\alpha_1\alpha_2\alpha_3 = \\ &= 2(\alpha_1 + \alpha_2 + \alpha_3)^2 - 9(\alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_1\alpha_2^2 + \alpha_2^2\alpha_3 + \alpha_1\alpha_3^2 + \alpha_2\alpha_3^2) = \\ &= 27\alpha_1\alpha_2\alpha_3 = -27 \times 2q \end{aligned}$$

Now write down the quadratic equation and deduce the cubic formula!