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

Alessio Corti

10th January 2020

Q 1. This question is designed to get you up to speed with arithmetic in $\mathbb{Q}[x]$.

(a) Find the quotient and remainder when $x^5 + x + 1$ is divided by $x^2 + 1$.

(b) Find the remainder when $x^{2019} + 32x^{53} + 8$ is divided by $x - 1$.

(c) Find polynomials $s(x)$ and $t(x)$ such that

$$(2x^3 + 2x^2 + 3x + 2)s(x) + (x^2 + 1)t(x) = 1.$$

[Bonus question: how did I know for sure that these polynomials were coprime?]

(d) Find a hcf for $x^4 + 4$ and $x^3 - 2x + 4$. Express it as $a(x)(x^4 + 4) + b(x)(x^3 - 2x + 4)$.

(e) Find polynomials $\lambda(x)$ and $\mu(x)$ such that $(1 + x)\lambda(x) + (x^3 - 2)\mu(x) = 1$.

Q 2. Write $\xi = \sqrt[3]{2}$. This question is about understanding the field operations in $\mathbb{Q}(\xi)$ explicitly.

(a) Find rational numbers a, b and c such that $a + b\xi + c\xi^2 = 1/(1 + \xi)$.
[*Hint*: use Part (e) of the previous question.]

(b) Fix rational numbers A, B. Find rational numbers a, b and c (depending on A, B) such that $a + b\xi + c\xi^2 = 1/(A + B\xi + \xi^2)$.

Q 3. Prove that if $f, g \in K[x]$ and at least one is non-zero, and if s, t are both hcf's of f and g, then $s = \lambda t$ for some $\lambda \in K^\times$.

Q 4. (a) We know that whether or not a polynomial is irreducible depends on which field it's considered as being over: for example $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{C}[x]$. But show that the notion of divisibility does not depend on such issues. More precisely show that if $K \subseteq L$ are fields, if $f, g \in K[x]$, and if $f \mid g$ in $L[x]$ then $f \mid g$ in $K[x]$.

(b) Is it true that if $f, g \in \mathbb{Z}[x]$ and $f \mid g$ in $\mathbb{Q}[x]$ then $f \mid g$ in $\mathbb{Z}[x]$? [*Hint*: No.] Is it true under the extra assumption that f is monic? [*Hint*: Yes.]

Q 5. (a) Prove that if $n \in \mathbb{Z}$ and $\sqrt{n} \notin \mathbb{Z}$ then $\sqrt{n} \notin \mathbb{Q}$.

(b) Prove that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. What is the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$?

(c) Use the Tower Law to prove that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Write down a basis for the $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Q 6. (a) Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

[*Hint*: the smallest subfield of the complex numbers containing $\mathbb{Q}$ and $\sqrt{2} + \sqrt{3}$ must contain loads of other things too: write some of them down.]

(b) Deduce that $x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$.

Q 7. Is $\sqrt{10} \in \mathbb{Q}(\sqrt{6}, \sqrt{15})$?

Q 8. Prove that: If $K \subseteq L \subseteq E$ are fields, and one of $[L : K]$ or $[E : L]$ is infinite, then $[E : K]$ is infinite.

Remark: for those unfamiliar with infinite-dimensional vector spaces, a vector space V over a field is infinite-dimensional iff it has no finite spanning set, iff for every $n \geq 1$ there exist n elements $v_1, v_2, \ldots, v_n$ which are linearly independent.

Q 9. (a) Prove that if $K \subseteq L$ is a finite extension of fields and V/L is a finite-dimensional vector space then $\dim_K(V) = [L : K] \dim_L(V)$.

(b) Prove that if $K \subseteq L \subseteq E$ and $[E : K] = [L : K]$ is finite, then $L = E$.

Q 10. Let K be a field with $\mathrm{char}(K) \neq 3$ and such that $f(x) = x^3 - 3x + 1 \in K[x]$ is irreducible. Let $L = K(\alpha)$ where α is a root of $f(x)$. Show that f splits completely over L.

[*Hint*: Factor f over $L[x]$ as $(x - \alpha)g(x)$. Now solve for $g(x) = 0$ in L observing that $12 - 3\alpha^2 = (-4 + \alpha + 2\alpha^2)^2$.]

Q 11 (†)**.** Let K be a field of characteristic 0 containing an element $\omega \in K$ with

$$\omega^2 + \omega + 1 = 0\,.$$

(For example you can take $K = \mathbb{Q}(\omega)$ where $\omega = \exp \frac{2\pi \mathrm{i}}{3}$.) In this question we carve a trick-free path to the formula for the solutions of the equation

$$y^3 + 3px + 2q = 0 \tag{†}$$

(where p, $q \in K$) that only involves taking radicals (i.e., $\sqrt[n]{\ }$ of something).

We assume that $K \subset L$ is the splitting field of the polynomial of Equation (†) and we denote by $\alpha_1, \alpha_2, \alpha_3 \in L$ the three roots. (You can already prove that such a field extension exists but I don't care that you do this here.)

We know that the Galois group G permutes the three roots.

(a) Write the action of the cyclic permutation $\sigma = (123)$ on the elements

$$u = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3, \quad v = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\,.$$

and conclude that $\sigma(u) = \omega u$ and $\sigma(v) = \omega^2 v$.[1]

(b) Find a formula expressing the three roots α_1, α_2, α_3 in terms of u and v.

[*Hint*: $\alpha_1 + \alpha_2 + \alpha_3 = 0$.]

(c) Consider the transposition $\tau = (23)$: show that $\tau(u) = v$ and $\tau(v) = u$, and hence argue that $u^3 + v^3$ and u^3v^3 are fixed by all of $\mathfrak{S}_3$ — and hence by all of G, irrespective of what G is. In other words, it follows from the Galois Correspondence that $u^3 + v^3$ and $u^3v^3 \in K$: show that this is indeed the case by finding explicit formulas for these quantities. Thus write down an explicit quadratic polynomial in $K[X]$ of which u^3, v^3 are the two roots. Solve the quadratic equation, and combine with (b) to derive the cubic formula.

[1] Whether or not there is an element of G that acts as σ on the three roots is not relevant at this point. Such an element may or may not exist.