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

Alessio Corti

26th January 2020

Q 1. In this question, if $\alpha \in \mathbb{R}_{>0}$ and $n \in \mathbb{Z}_{\geq 1}$ then by $\alpha^{1/n}$ or $\sqrt[n]{\alpha}$ I mean the unique positive real number β with $\beta^n = \alpha$. (This removes ambiguities about a general complex number having n complex roots in this question).

(i) Set $\gamma = (1+\sqrt{3})^{1/3}$. Prove that γ is *algebraic*[1]. What is its degree over $\mathbb{Q}$? What is its degree over $\mathbb{Q}(\sqrt{3})$?

(ii) Set $\delta = (10+6\sqrt{3})^{1/3}$. Prove that δ is algebraic. What is its degree over $\mathbb{Q}$? What is its degree over $\mathbb{Q}(\sqrt{2})$?

Q 2. In this question we'll find an explicit complex number z such that $\overline{z} \notin \mathbb{Q}(z)$ (by $\overline{z}$ I mean the complex conjugate of z.)

(a) Set $\omega = e^{2\pi i/3}$, so $\omega^3 = 1$, and say $\alpha = 2^{1/3} \in \mathbb{R}$ the real cube root of 2. Set $z = \omega\alpha$. What is $[\mathbb{Q}(z) : \mathbb{Q}]$? [*Hint: minimal polynomial*].

(b) What is $[\mathbb{Q}(\omega) : \mathbb{Q}]$?

(c) Let's assume temporarily that $\overline{z} \in \mathbb{Q}(z)$. Show that this implies $\omega \in \mathbb{Q}(z)$. Why does this contradict the tower law? Deduce $\overline{z} \notin \mathbb{Q}(z)$.

(d) Let's write $z = x + iy$. Prove that none of x, i or y are in $\mathbb{Q}(z)$.

Q 3. The purpose of this question is to make the proof of the Gauss' Lemma more digestible.

(a) Prove that if R is a commutative ring with 1, and $x \in R$ then $0x = 0$.

(b) Prove that if K is a field and $a, b \in K$ are both non-zero, then $ab \neq 0$.

(c) If K is a field and $f = \sum_{i=0}^{d} a_i x^i \in K[x]$ is a non-zero polynomial, then (by choosing d sensibly) we may assume $a_d \neq 0$; we call $a_d x^d$ the *leading term* of f, and d the *degree* of f, and we write $d = \deg(f)$. Prove that if $f, g \in K[x]$ are non-zero, then fg is also non-zero, and $\deg(fg) = \deg(f) + \deg(g)$.

(d) Prove that if $f, g, h \in K[x]$ and $h \neq 0$ and $fh = gh$, then $f = g$ (the cancellation property for polynomial rings).

[Some of you will know that $f, g \neq 0 \implies fg \neq 0$ is the assertion that $K[x]$ is an *integral domain*. **Note** that we used in class the fact that $\mathbb{F}_p[X]$ is an integral domain in the proof of the Gauss Lemma.]

[1] By definition a complex number $z \in \mathbb{C}$ is algebraic if it is the root of a polynomial with coefficients in $\mathbb{Q}$.

Q 4. Factor the following polynomials in $\mathbb{Q}[x]$ into irreducible ones, giving proofs that your factors really are irreducible.

(i) $x^3 - 8$;

(ii) $x^{1000} - 6$;

(iii) $x^4 + 4$;

(iv) $2x^3 + 5x^2 + 5x + 3$;

(v) $x^5 + 6x^2 - 9x + 12$;

(vi) $x^{73} - 1$;

(vii) $x^{73} + 1$;

(viii) $x^{12} - 1$.

Q 5. Prove that if $\alpha = 2^{1/10}$ then $\mathbb{Q}(\alpha)$ has a basis $\{1, \alpha, \alpha^2, \ldots, \alpha^9\}$.

Q 6. Let A denote the set of complex numbers that are algebraic (over $\mathbb{Q}$).

(i) Prove that A is a field.

(ii) Prove that $[A : \mathbb{Q}] = \infty$. [*Hint: you can use Eisenstein to construct irreducible polynomials of large degree.*]

(iii) Prove that A is a countable set.

(iv) Prove that $[\mathbb{C} : A] = \infty$.

Q 7. The Eisenstein criterion is not a brilliant way to decide if a polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible. A much better strategy is to choose a prime p and show that the reduction of f modulo p is irreducible in $\mathbb{F}_p[x]$.

Make a list of all irreducible polynomials of degree ≤ 3 in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, and $\mathbb{F}_5[x]$. (This is most definitely NOT a stupid thing to do.)

Q 8 (†). (a) Suppose that $a, b \in K$ are such that a is a square in $K(\sqrt{b})$.[2] Prove that either a or ab is a square in K.

(b) Let $a, b \in K$ and suppose that b is NOT a square in K; let $L = K(\beta)$ with $\beta^2 = b$. Prove that: If one of $a + \beta$, $a - \beta$ is a square in L, then so is the other, and deduce that $c = a^2 - b$ is a square in K.

(c) Let $a, b \in K$ and set $c = a^2 - b$; suppose that none of b, c, or bc is a square in K. If L is a splitting field of the polynomial:

$$(x^2 - a)^2 - b \in K[x],$$

prove that $[L : K] = 8$.

[*Hint: use Part (a) and Part (b) repeatedly.*]

Q 9 (†). Suppose that $\mathrm{char}(K) \neq 2$, and let $K \subset L$ be a field extension of degree 4. Prove that the following two conditions are equivalent:

[2]In general if K is a field we say that $a \in K$ *is a square* iff the polynomial $X^2 - a \in K[X]$ splits into two linear factors, or, equivalently, there exists $\alpha \in K$ such that $\alpha^2 = a$.

(i) There exists a (nontrivial) intermediate field $K \subset E \subset L$;

(ii) $L = K(\alpha)$ for some $\alpha \in L$ having minimal polynomial over K of the form:

$$f = x^4 + ax^2 + b \in K[x] \,.$$

Q 10. Say F is the splitting field of $x^3 - 11$ over $\mathbb{Q}$. Figure out the Galois group $\mathrm{Gal}(F/\mathbb{Q})$. List all the subfields of F, all the subgroups of the Galois group, and draw a picture of the Galois correspondence.

Q 11. Say $E = \mathbb{Q}$ and let F be the splitting field of $x^4 - p$, where p is a prime number. What is $[F : E]$? What is $\mathrm{Gal}(F/E)$? [*Hint: you can just go ahead and do the question, but you may find Question 8 helpful.*]