Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 394 : GALOIS THEORY

Solution Set 5

5.1 Prove that $f(t) := 1 + t + t^2 + \cdots + t^{n-1}$ is irreducible over $\mathbb{Q}$ iff n is prime.

Let $f(t) := 1 + t + t^2 + \cdots + t^{n-1}$. Since this is a geometric series, we can write

$$f(t) = \frac{t^n - 1}{t - 1}.$$

If $n = ab$ is composite, we see that

$$\begin{aligned} f(t) = \frac{(t^a)^b - 1}{t-1} &= \frac{t^a - 1}{t-1} \cdot (1 + t^a + t^{2a} + \cdots + t^{a(b-1)}) \\ &= (1 + t + t^2 + \cdots + t^{a-1})(1 + t^a + t^{2a} + \cdots + t^{a(b-1)}). \end{aligned}$$

Else, if n is prime, we have

$$f(t+1) = t^{n-1} + \binom{n}{1} t^{n-2} + \binom{n}{2} t^{n-3} + \cdots + \binom{n}{n-2} t + \binom{n}{n-1}.$$

Applying Eisenstein at the prime n shows this is irreducible.

5.2 Let $\omega := e^{2\pi i/3}$. Show that $\mathbb{Q}(\omega) = \mathbb{Q}[\omega]$.

There are (at least!) two approaches to this:

1. High-brow approach. We clearly have $\mathbb{Q}[\omega] \subseteq \mathbb{Q}(\omega)$, so it suffices to prove the reverse inclusion. With Kronecker's theorem and some amount of work, one can show that $\mathbb{Q}[\omega] \simeq \mathbb{Q}[t]/(t^2 + t + 1)$. Once this is done, the rest is easy: by Kronecker's theorem we deduce that $\mathbb{Q}[\omega]$ must be a field. But by definition, $\mathbb{Q}(\omega)$ is the *smallest* field containing both $\mathbb{Q}$ and ω! QED.

2. Low-brow approach. We wish to show that $\mathbb{Q}[\omega]$ is a field. Since it's already a commutative ring, all that's left is to show existence of multiplicative inverses. Recall that $\omega^2 + \omega + 1 = 0$. It follows that any polynomial in ω can be expressed in the form $a + b\omega$. Thus it suffices to prove that $1 + c\omega$ has an inverse in $\mathbb{Q}[\omega]$. Note that

$$\frac{1}{1 + c\omega} = \frac{1 - c\omega + c^2\omega^2}{1 + c^3} = \frac{(1 - c^2) - (c + c^2)\omega}{1 + c^3} \in \mathbb{Q}[\omega].$$

[The easiest way to discover this is to expand the LHS by Taylor series. This isn't a proof, since convergence is an issue for some choices of c, but once one knows the answer, it's easy to prove it directly!]

5.3 Fun with quotients!

(a) Prove that $\mathbb{Q}[t]/\langle t^3-2\rangle \simeq \mathbb{Q}[\sqrt[3]{2}]$.

Step 1: prove that $\mathbb{Q}[t]/\langle t^3-2\rangle = \{[a+bt+ct^2] : a,b,c \in \mathbb{Q}\}$.

Step 2: prove that the map $[a+bt+ct^2] \mapsto a+b\sqrt[3]{2}+c\sqrt[3]{2}^2$ is an isomorphism.

(b) Prove that $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$. Do not use algebraic number theory! [*Hint: you may find the identity* $x^3+y^3=(x+y)(x^2-xy+y^2)$ *useful.*]

As in **5.2**, there are two approaches.

1. High-brow approach. We know by Kronecker and part (a) that $\mathbb{Q}[\sqrt[3]{2}]$ must be a field, and by inspection this field must contain both $\mathbb{Q}$ and $\sqrt[3]{2}$. Thus, $\mathbb{Q}[\sqrt[3]{2}] \supseteq \mathbb{Q}(\sqrt[3]{2})$. The reverse containment is clear.

2. Low-brow approach. It's easiest to proceed in stages:

Claim 1. Given $x \in \mathbb{Q}[\sqrt[3]{2}]$, there exists $y \in \mathbb{Q}[\sqrt[3]{2}]$ such that $xy \in \mathbb{Q}+(\sqrt[3]{2})^2\mathbb{Q}$.
Proof. Factor out the constant term of x to get $x/a = 1+b\sqrt[3]{2}+c(\sqrt[3]{2})^2$ for some $b,c \in \mathbb{Q}$. Add and subtract $(b\sqrt[3]{2})^2$. Then can multiply by $1-b\sqrt[3]{2}$ to deduce claim.

Claim 2. Given $\alpha \in \mathbb{Q}+(\sqrt[3]{2})^2\mathbb{Q}$ there exists $z \in \mathbb{Q}[\sqrt[3]{2}]$ such that $\alpha z \in \mathbb{Q}$.
Proof. Factor out constant term of α to write $\alpha/r = 1+s(\sqrt[3]{2})^2$ with $s \in \mathbb{Q}$. Set $\beta := s(\sqrt[3]{2})^2$. Then $\alpha/r \cdot (1-\beta+\beta^2) \in \mathbb{Q}$.

(c) Does there exist any $\alpha \in \mathbb{C}$ such that $\mathbb{Q}[t]/\langle t^3-2\rangle \simeq \mathbb{Q}(\alpha)$ but $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt[3]{2})$? Prove.

Yes: $\alpha = \omega\sqrt[3]{2}$.

(d) Are the two fields $\mathbb{Q}[t]/\langle t^2+3\rangle$ and $\mathbb{Q}[t]/\langle t^2+1\rangle$ isomorphic? Why or why not? Prove.

Nope. Both of these fields look like $\{[at+b] : a,b \in \mathbb{Q}\}$, but the natural guess at an isomorphism fails: if $\phi : \mathbb{Q}[t]/(t^2+3) \to \mathbb{Q}[t]/(t^2+1)$ is defined by $\phi([at+b]) := [at+b]$, then $\phi([9]) = \phi([t]^4) = [t]^4 = [1] = \phi([1])$, so it isn't injective.

But this doesn't answer the question: it's possible there exists some more complicated isomorphism between the two spaces! Before excluding this possibility, we make a quick shift to a more convenient viewpoint: one can prove that $\mathbb{Q}[t]/(t^2+3) \simeq \mathbb{Q}(i\sqrt{3})$ and $\mathbb{Q}[t]/(t^2+1) \simeq \mathbb{Q}(i)$. Thus is suffices to prove that $\mathbb{Q}(i\sqrt{3}) \not\simeq \mathbb{Q}(i)$. Well, suppose

$$\phi : \mathbb{Q}(i\sqrt{3}) \xrightarrow{\sim} \mathbb{Q}(i).$$

Note that $\phi(1) = 1$, whence $\phi(-1) = -1$ (it must equal ± 1, but ϕ must be injective). It follows that $\phi(n) = n$ for all $n \in \mathbb{Z}$, from which we deduce that $\phi(\alpha) = \alpha$ for all $\alpha \in \mathbb{Q}$. In other words, **any isomorphism between these two field extensions of $\mathbb{Q}$ must fix $\mathbb{Q}$**. But this immediately yields a problem: we must have $\phi(i\sqrt{3})^2 = -3$, whence $\phi(i\sqrt{3}) = \pm i\sqrt{3}$, neither of which live in $\mathbb{Q}(i)$.

(e) Are the two fields $\mathbb{R}[t]/\langle t^2+3\rangle$ and $\mathbb{R}[t]/\langle t^2+1\rangle$ isomorphic? Why or why not? Prove.

Yes, these two fields are isomorphic. Indeed, Kronecker's theorem implies

$$\begin{aligned}\mathbb{R}[t]/(t^2+3) \simeq \mathbb{R}[i\sqrt{3}] &= \{a+bi\sqrt{3} : a,b\in\mathbb{R}\}\\ &= \{a+bi : a,b\in\mathbb{R}\} = \mathbb{R}[i] \simeq \mathbb{R}[t]/(t^2+1).\end{aligned}$$

5.4 True facts about field extensions.

(a) Suppose K and L are fields, and that there exists a ring homomorphism $\varphi : K \to L$. Prove that L is a field extension of K.

It suffices to prove that φ is injective. Since φ preserves addition it must map $0 \mapsto 0$, and since it's a ring homomorphism, it must also send $1 \mapsto 1$ by definition. In particular, for any $x \neq y$ we have $\varphi(x-y)\varphi\big((x-y)^{-1}\big) = 1$. It follows that $\varphi(x-y) \neq 0$, or in other words, that $\varphi(x) \neq \varphi(y)$.

(b) Prove that $[L : K] = 1$ if and only if $L \simeq K$.

Given L/K, there exists some embedding $\varphi : K \hookrightarrow L$. We endow L with the structure of a vector space over K with scalar multiplication defined by $kx := \varphi(k)x$ for any $k \in K$ and $x \in L$.

The degree of L/K is 1 iff there exists a basis for L over K which consists of a single element. In other words, $[L : K] = 1$ iff there exists $x_0 \in L$ such that $L = \{kx_0 : k \in K\}$. But this implies the existence of $k_0 \in K^\times$ such that $k_0x_0 = 1$, whence

$$L = \{kx_0 : k \in K\} = \{jk_0x_0 : j \in K\} = \{j : j \in K\}.$$

In particular we deduce that φ is a surjection as well as an embedding, hence is an isomorphism between K and L.

(c) Suppose L/K is a field extension with char $K \neq 2$. Prove that $[L : K] = 2$ if and only if $\exists \alpha \in L$ such that $\alpha \notin K$, $L = K(\alpha)$, and $\alpha^2 \in K$.

The reverse direction is the easier of the two, so we dispense with it first. Given $\alpha \in L$ such that $\alpha \notin K$, $L = K(\alpha)$, and $\alpha^2 \in K$, we see that α is algebraic over K: it is a root of the polynomial $t^2 - \alpha^2 \in K[t]$. We immediately deduce that $K[\alpha] = K(\alpha)$. Moreover,

$$K[\alpha] \simeq K[t]/(t^2-\alpha^2),$$

whence every element of $K[\alpha]$ can be reduced to the form $x + \alpha y$ for some $x, y \in K$. Thus, $\{1, \alpha\}$ spans L/K, so $[L : K] \leq 2$. On the other hand, since $\alpha \notin K$ we see that $[L : K] \geq 2$. Thus, $[L : K] = 2$.

continued on next page...

Next we tackle the forward direction. Suppose L/K is a field extension of degree 2.

Lemma. There exists $\beta \in L$ such that $\{1, \beta\}$ is a basis for L/K.
Proof. By definition, we know there exists a basis $\{\alpha, \beta\}$ for L/K. If either of α or β is an element of K, we're done (after renormalization), so we may assume neither α nor β belong to K. I claim that in this case, $\{1, \beta\}$ is a basis. To see this, observe that we can express 1 in a unique way as a linear combination of α and β; note that the coefficients of both α and β must be nonzero, since neither lives in K. Thus we may express α as a linear combination of 1 and β. This immediately implies that $\{1, \beta\}$ spans L. To see that 1 and β are linearly independent, suppose $x + \beta y = 0$ for some $x, y \in K$. If y were nonzero, this would force $\beta \in K$, which we assumed isn't the case. Therefore, y must be 0; this in turn forces $x = 0$, and we're done! □

Thus armed, we proceed to the matter at hand. Pick a basis of L/K of the form $\{1, \beta\}$. This immediately implies that $\beta \notin K$ (else 1 and β would be linearly dependent over K), and also that $L = K(\beta)$. I claim that β is algebraic over K, and that its minimal polynomial $m_\beta \in K[t]$ has degree 2. Indeed, since any three elements of L must be linearly dependent, there must be some nontrivial linear combination of $1, \beta, \beta^2$ which produces 0, which implies that $\deg m_\beta \leq 2$. On the other hand, $\beta \notin K$, so $\deg m_\beta \geq 2$.

Therefore, we may write $m_\beta(t) = t^2 + Bt + C$ with $B, C \in K$ and $C \neq 0$. Now set $\alpha = \beta + B/2$. Then:

- $L = K(\beta) = K(\alpha)$, and
- $\alpha^2 = B^2/4 - C \in K$, but $\alpha \notin K$.

This concludes the proof.

(d) Suppose L/K is a field extension with the property that *every* $\alpha \in L$ is algebraic over K. Prove that any ring R lying between K and L (i.e. $K \subseteq R \subseteq L$) must be a field.

Note that since $R \subseteq L$, R must be a commutative ring. It therefore suffices to show that every nonzero $\alpha \in R$ has a multiplicative inverse in R. By hypothesis, α is algebraic over K. Let m_α be its minimal polynomial over K, say,

$$m_\alpha(t) := t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0 \in K[t].$$

Observe that $c_0 \neq 0$, else m_α would be reducible. Plugging in α and performing some algebraic manipulations produces

$$\alpha^{-1} = -c_0^{-1}(\alpha^{n-1} + c_{n-1}\alpha^{n-2} + \cdots + c_1),$$

which we know is in R since $c_0^{-1} \in K^\times \subseteq R$.

(e) Suppose $\alpha \in L/K$ is algebraic over K. Prove that $K(\alpha) = K[\alpha]$.

We proved in class that $K[\alpha] \simeq K[t]/\langle m_\alpha \rangle$. Moreover, since m_α is irreducible, the right hand side is a field. Thus $K[\alpha]$ is a field, which instantly implies $K[\alpha] = K(\alpha)$.

(f) Suppose $\alpha \in L/K$ is transcendental over K. Prove that $K(\alpha) \not\simeq K[\alpha]$.

If $K[\alpha] \simeq K(\alpha)$, then α is invertible in $K[\alpha]$, i.e. there exists some $p \in K[t]$ such that $\alpha p(\alpha) = 1$. But then α is a root of $tp(t) - 1 \in K[t]$, and therefore α is not transcendental.

5.5 Playing with algebraic numbers. (Please don't use tools you learned from algebraic number theory.)

(a) Prove that $\sqrt{2}+\sqrt{5}$ is algebraic.

In class (Lecture 11) we proved that for any α, β that are algebraic over K, the field extension $K(\alpha,\beta)/K$ is algebraic; in particular, $\alpha+\beta$, $\alpha\beta$, etc. are all algebraic over K. However, I asked you in class not to use this fact! Instead, we'll find the minimal polynomial.

Let $\alpha := \sqrt{2}+\sqrt{5}$. Then

$$\alpha^2 = 9 + 2\sqrt{10}$$

whence $(\alpha^2-9)^2 = 40$. After simplifying, we deduce that α is a root of $f(x) := x^4-18x^2+41$. I claim this is irreducible over $\mathbb{Q}$. Indeed, the rational root test shows that f has no roots in $\mathbb{Q}$, which only leaves the possibility that f is the product of two monic quadratics; moreover, by Gauss' lemma these must both be in $\mathbb{Z}[x]$. Some algebra shows this isn't possible, whence f is irreducible over $\mathbb{Q}$ and hence must be the minimal polynomial of α over $\mathbb{Q}$. (Alternatively, the quadratic formula shows that if β is a root of f, then $\alpha^2 = 9 \pm 2\sqrt{10} \notin \mathbb{Q}$.)

(b) Suppose α is algebraic over $\mathbb{Q}$. Prove that $i\alpha$ is also algebraic over $\mathbb{Q}$.

Again, we proved that the product of any two algebraic numbers must be algebraic, which settles the matter. Here's a more direct proof: suppose α has minimal polynomial $m \in \mathbb{Q}[x]$, and set

$$f(x) := m(-ix)\overline{m(-ix)}.$$

It's an exercise to prove that $f \in \mathbb{Q}[x]$, and we have

$$f(i\alpha) = m(\alpha)\overline{m(\alpha)} = 0,$$

which proves that $i\alpha$ is algebraic over $\mathbb{Q}$. (Note that f is not necessarily the *minimal* polynomial of α!)

(c) Suppose α is algebraic over $\mathbb{Q}$. Is $\sqrt{\alpha}$ algebraic over $\mathbb{Q}$? Justify your answer with a proof or a counterexample.

Let $m \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$, and set $f(x) := m(x^2)$. Clearly $f \in \mathbb{Q}[x]$, and

$$f(\sqrt{\alpha}) = m(\alpha) = 0,$$

so $\sqrt{\alpha}$ must be algebraic over $\mathbb{Q}$ as well.

(d) Given α algebraic over K, suppose m_α has odd degree. Prove that $K(\alpha^2) = K(\alpha)$.

It is clear that $K(\alpha^2) \subseteq K(\alpha)$. To show the reverse containment, it suffices to show α can be expressed as a rational expression over $K(\alpha^2)$. Let m_α denote the minimal polynomial of α over K, and write

$$m_\alpha(x) = A(x^2) + xB(x^2)$$

where $A, B \in K[x]$. Plugging α in and simplifying yields

$$\alpha = -A(\alpha^2)/B(\alpha^2) \in K(\alpha^2).$$

Actually, there's one more thing to check: that $B(\alpha^2) \neq 0$. To see this, note that $\deg m_\alpha = 1 + 2\deg B$. In particular, $\deg B(x^2) = 2\deg B < \deg m_\alpha$, whence $B(\alpha^2) \neq 0$.