SOLUTIONS TO WORKSHEET #2

Problem 1. — *Let L/K be a finite field extension of degree two. Prove that:*

(i) *if* $\mathrm{char}(K) \neq 2$*, then* $L = K(x)$ *for some* $x \in L$ *such that* $x^2 \in K$*; whereas*

(ii) *if* $\mathrm{char}(K) = 2$*, then either* $L = K(x)$ *with* $x^2 \in K$*, or* $L = K(x)$ *with* $x^2 + x \in K$*.*

Solution. That L/K is of degree 2 means that L is a 2-dimensional K-vector space. So choose any basis $L = K \cdot 1 \oplus K \cdot y$, where $y \in L \setminus K$ is an arbitrary element. The element $y^2 \in L$ can therefore be expressed as a K-linear combination of the basis 1 and y; equivalently, there is an equation

$$y^2 + ay + b = 0 \in L$$

for some $a, b \in K$. If $\mathrm{char}(K) \neq 2$, we may complete the square and obtain an equation

$$y^2 + ay + b \pm \frac{1}{4}a^2 = (y + \frac{1}{2}a)^2 + b - \frac{1}{4}a^2 = x^2 + (b - \frac{1}{4}a) = 0$$

where $x := y + \frac{1}{2}a$. Since y is not in the K-span of 1, neither will x, meaning $x \in L \setminus K$ and that $\{1, x\}$ is a K-basis of L. Therefore $L = K(x)$ and $x^2 = \frac{1}{4}a - b \in K$.

In the case that $\mathrm{char}(K) = 2$, then we cannot complete the square—we had to divide by 4, but $4 = 0$ in K! However, if $a \neq 0$, then we may divide the relation by a^2 to see that

$$\left(\frac{y}{a}\right)^2 + \frac{y}{a} + \frac{b}{a^2} = x^2 + x + \frac{b}{a^2} = 0$$

where $x := y/a$. So, if $a \neq 0$, then $L = K(x)$ where $x^2 + x = b/a^2 \in K$. If $a = 0$, then taking $x := y$, the original relation already gives $L = K(x)$ with $x^2 \in K$. This now covers all cases. ■

Problem 2. — *Let L/K be a finite field extension whose degree is a prime number. Prove that there are no intermediate fields between K and L.*

Solution. Suppose that there is a chain of field extensions $L \subseteq F \subseteq K$. Since degrees of field extensions are but vector space dimensions, there is the relation

$$[L : K] = [L : F] \cdot [F : K]$$

If $[K : L]$ were prime, then either $[K : F] = 1$ or $[F : L] = 1$, meaning that $F = K$ or $F = L$. In other words, there are no intermediate fields between a field extension of prime degree. ■

Problem 3. — *Let $K(\alpha)/K$ be a finite field extension of odd degree.*

(i) *Prove that $K(\alpha) = K(\alpha^2)$.*

(ii) *Give an example to show that the previous statement can be false if $[K(\alpha) : K]$ is even.*

Solution. Suppose $d := [K(\alpha) : K]$ is odd. View $K(\alpha^2)$ as an intermediate field extension between K and $K(\alpha)$, and consider the degree relation

$$d = [K(\alpha) : K(\alpha^2)] \cdot [K(\alpha^2) : K].$$

On the other hand, since every $x \in K(\alpha)$ may be written as

$$x = \sum_{i=0}^{d-1} c_i \alpha^i = \Big(\sum_{i=0}^{(d-1)/2} c_{2i} \alpha^{2i}\Big) + \Big(\sum_{i=0}^{(d-3)/2} c_{2i+1} \alpha^{2i}\Big)\alpha$$

Date: September 25, 2025.

for some $c_0, \dots, c_{d-1} \in K$. Each parenthetical terms on the right are all members of $K(\alpha^2)$, indicating that $[K(\alpha) : K(\alpha^2)] \leq 2$. But $d = [K(\alpha) : K]$ is odd, so the degree relation forces $[K(\alpha) : K(\alpha^2)] = 1$: that is, $K(\alpha) = K(\alpha^2)$.

Of course, when $d := [K(\alpha) : K]$ is even, it may be the case that $K(\alpha)$ and $K(\alpha^2)$ differ: this was essentially addressed in Problem 1! To see an explicit example, take the real numbers $K := \mathbf{R}$ and adjoin the imaginary root to obtain $K(\alpha) := \mathbf{R}(\sqrt{-1}) = \mathbf{C}$. Then $K(\alpha^2) = \mathbf{R}(-1) = \mathbf{R}$. ■

Problem 4. — *Let L/K be an algebraic field extension, denote the group of K-automorphisms of L by* $\mathrm{Aut}(L/K)$ *and assume that for every $\alpha \in L \setminus K$ we can find $\varphi \in \mathrm{Aut}(L/K)$ such that $\varphi(\alpha) \neq \alpha$. Pick $\beta \in L$ and let $f \in K[x]$ be the corresponding minimal polynomial. Prove that the group* $\mathrm{Aut}(L/K)$ *acts transitively on the set of roots of f.*

Solution. Write the minimal polynomial $f(x)$ of β as

$$f(x) = x^m + c_1 x^{m-1} + \cdots + c_{m-1}x + c_m = (x - r_1)(x - r_2)\cdots(x - r_m)$$

for coefficients $c_1, \dots, c_m \in K$ and roots $r_1, \dots, r_m \in L$. Expanding the product and comparing coefficients of x^k gives *Vieta's formulae*:

$$c_k = s_k(r_1, r_2, \dots, r_m) = \sum\nolimits_{1 \leq i_1 < i_2 < \cdots < i_k \leq m} r_{i_1} r_{i_2} \cdots r_{i_k}$$

where $s_k(r_1, r_2, \dots, r_m)$ is the k-th symmetric polynomial in the roots $r_1, r_2 \dots, r_m$. For example,

$$c_1 = r_1 + r_2 + \cdots + r_m, \;\; c_2 = \sum\nolimits_{1 \leq i < j \leq m} r_i r_j, \;\; \text{and} \;\; c_m = r_1 r_2 \cdots r_m.$$

The symmetric polynomials are named as such because they are invariant under the symmetric group: concretely, for any permutation $\sigma : \{1, \dots, m\} \to \{1, \dots, m\}$,

$$s_k(r_{\sigma(1)}, r_{\sigma(2)}, \dots, r_{\sigma(m)}) = s_k(r_1, r_2, \dots, r_m).$$

Suppose now that, perhaps after relabelling the roots, the orbit of r_1 under $\mathrm{Aut}(L/K)$ is the set $\{r_1, r_2, \dots, r_n\}$ for some $1 \leq n \leq m$. Form the polynomial

$$g(x) := (x - r_1)(x - r_2)\cdots(x - r_n) = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n.$$

As before, the k-th coefficient $b_k = s_k(r_1, r_2, \dots, r_n)$ is given by the k-th symmetric polynomial on $r_1, r_2, \dots, r_n$. But since $\{r_1, r_2, \dots, r_n\}$ is the full orbit of r_1 under $\mathrm{Aut}(L/K)$, any $\varphi \in \mathrm{Aut}(L/K)$ simply permutes the set, and so

$$\begin{aligned} \varphi(b_k) = \varphi(s_k(r_1, r_2, \dots, r_m)) &= s_k(\varphi(r_1), \varphi(r_2), \dots, \varphi(r_m)) \\ &= s_k(r_{\sigma(1)}, r_{\sigma(2)}, \dots, r_{\sigma(m)}) = s_k(r_1, r_2, \dots, r_m) = b_k \end{aligned}$$

where $\sigma : \{1, \dots, m\} \to \{1, \dots, m\}$ is some permutation, the first line uses the fact that φ is a homomorphism of fields, and the final line uses the invariance of the symmetric polynomials under the symmetric group. Since this is true for all $\varphi \in \mathrm{Aut}(L/K)$, the hypothesis implies that, in fact, $b_k \in K$ for each $k = 1, \dots, n$; in other words, $g(x) \in K[x]$.

The polynomial $g(x)$ divides $f(x)$ since the roots of the former are a subset of those of the latter. Applying the polynomial division algorithm gives another polynomial $h(x) \in K[x]$ such that

$$f(x) = g(x)h(x).$$

Now $f(x)$ is the minimal polynomial of $\beta \in L$, so $f(\beta) = 0$. The relation implies that either $g(\beta) = 0$ or $h(\beta) = 0$. But minimality implies that $f(x)$ divides either $g(x)$ or else $h(x)$. This is only possible if $f(x) = g(x)$, so that $n = m$ above, meaning that $\mathrm{Aut}(L/K)$ acts transitively on $\{r_1, \dots, r_m\}$. ■

Problem 5. — *Let* $\mathbf{F}_2 = \{0,1\}$ *be the field with* 2 *elements and let* $\mathbf{F}_4 := \mathbf{F}_2(\alpha)$ *be the field extension generated by a root* α *of* $1 + x + x^2 \in \mathbf{F}_2[x]$. *Prove that* $\varphi : \mathbf{F}_4 \to \mathbf{F}_4$ *given by* $a + b\alpha \mapsto a + b + b\alpha$ *is an element of* $\mathrm{Aut}(\mathbf{F}_4/\mathbf{F}_2)$, *where* $a, b \in \mathbf{F}_2$.

Solution. It is clear from the definition that $\varphi : \mathbf{F}_4 \to \mathbf{F}_4$ acts trivially on $\mathbf{F}_2$; in particular, it preserves the additive and multiplicative units. Moreover, since $\mathbf{F}_4 = \{0, 1, \alpha, 1+\alpha\}$ and

$$\varphi(\alpha) = 1 + \alpha \text{ and } \varphi(1+\alpha) = 2 + \alpha = \alpha,$$

using the relation $2 = 0$ in $\mathbf{F}_2$, the function φ is even a bijection. It remains to verify that φ is a homomorphism of fields, namely, that it preserves addition and multiplication. Let $a_1, a_2, b_1, b_2 \in \mathbf{F}_2$. For addition, directly compute:

$$\begin{aligned}\varphi((a_1 + b_1\alpha) + (a_2 + b_2\alpha)) &= \varphi((a_1 + a_2) + (b_1 + b_2)\alpha) \\ &= (a_1 + a_2 + b_1 + b_2) + (b_1 + b_2)\alpha \\ &= (a_1 + b_1 + b_1\alpha) + (a_2 + b_2 + b_2\alpha) \\ &= \varphi(a_1 + b_1\alpha) + \varphi(a_2 + b_2\alpha).\end{aligned}$$

For multiplication, use the relation $\alpha^2 = \alpha + 1$ to obtain, on the one hand

$$\begin{aligned}\varphi((a_1 + b_1\alpha)(a_2 + b_2\alpha)) &= \varphi(a_1a_2 + (a_1b_2 + a_2b_1)\alpha + b_1b_2\alpha^2) \\ &= \varphi(a_1a_2 + b_1b_2 + (a_1b_2 + a_2b_1 + b_1b_2)\alpha) \\ &= a_1a_2 + b_1b_2 + a_1b_2 + a_2b_1 + b_1b_2 + (a_1b_2 + a_2b_1 + b_1b_2)\alpha \\ &= a_1a_2 + a_1b_2 + a_2b_1 + (a_1b_2 + a_2b_1 + b_1b_2)\alpha\end{aligned}$$

where $2b_1b_2 = 0$ since $\mathbf{F}_2$ has characteristic 2. On the other hand,

$$\begin{aligned}\varphi(a_1 + b_1\alpha)\varphi(a_2 + b_2\alpha) &= (a_1 + b_1 + b_1\alpha)(a_2 + b_2 + b_2\alpha) \\ &= a_1a_2 + a_1b_2 + a_2b_1 + b_1b_2 + (a_1b_2 + a_2b_1 + 2b_1b_2)\alpha + b_1b_2\alpha^2 \\ &= a_1a_2 + a_1b_2 + a_2b_1 + 2b_1b_2 + (a_1b_2 + a_2b_1 + b_1b_2)\alpha \\ &= a_1a_2 + a_1b_2 + a_2b_1 + (a_1b_2 + a_2b_1 + b_1b_2)\alpha.\end{aligned}$$

Comparing the final lines of both computations shows that

$$\varphi((a_1 + b_1\alpha)(a_2 + b_2\alpha)) = \varphi(a_1 + b_1\alpha)\varphi(a_2 + b_2\alpha). \qquad \blacksquare$$

Problem 6. — *Prove that the set* $\mathbf{A}$ *of complex numbers that are algebraic over* $\mathbf{Q}$ *form a subfield of* $\mathbf{C}$ *that is algebraically closed. This gives an example of an algebraic field extension which is not finite.*

Solution. Defined in this way, $\mathbf{A}$ is but a subset of $\mathbf{C}$, so the task is to show it is a field. Of course, any element of $\mathbf{Q}$ is algebraic over $\mathbf{Q}$, so $\mathbf{Q} \subset \mathbf{A}$, showing that $\mathbf{A}$ contains 0 and 1. It remains to show that it is closed under addition, multiplication, and taking inverses. But for this, let $\alpha, \beta \in \mathbf{A}$ be any elements. By definition, they are algebraic over $\mathbf{Q}$, so that together they generate a finite field extension $\mathbf{Q}(\alpha, \beta)$ over $\mathbf{Q}$. Every element in a finite field extension is algebraic over the base. Since each of $\alpha + \beta$, $\alpha\beta$, α^{-1}, and β^{-1} lie in $\mathbf{Q}(\alpha, \beta)$, they are algebraic over $\mathbf{Q}$ and therefore lie in $\mathbf{A}$. Thus $\mathbf{A}$ is closed under all the field operations, and thus is itself a field.

To see that $\mathbf{A}$ is algebraically closed, let $f(x) \in \mathbf{A}[x]$ be a polynomial. Since $f(x)$ has only finitely many coefficients, it may be viewed as an element of $K[x] \subset \mathbf{A}[x]$ where K is the finite field extension of $\mathbf{Q}$ obtained by adjoining the coefficients of $f(x)$. Adjoining the finitely many roots of $f(x)$ to K then produces a finite field extension L/K. But then L is a finite field extension of $\mathbf{Q}$, meaning that the roots of $f(x)$ are algebraic over $\mathbf{Q}$, and so lie in $\mathbf{A}$. Thus all the roots of $f(x)$ lie in $\mathbf{A}$, meaning it is algebraically closed. $\blacksquare$

Problem 7. — *Let L/K be a field extension such that one can pick $x \neq y \in L$ transcendental over K. Prove that x is algebraic over $K(y)$ if and only if y is algebraic over $K(x)$.*

Solution. An argument showing that if x is algebraic over $K(y)$ then y is algebraic over $K(x)$ will give the argument for the converse by swapping the symbols x and y. So suppose x is algebraic over $K(y)$. This means that there is a polynomial

$$f(t) := t^m + c_1(y) \cdot t^{m-1} + \cdots + c_{m-1}(y) \cdot t + c_m(y) \in K(y)[t]$$

such that $f(x) = 0$. The rational functions $c_i(y)$ are quotients of polynomials in y, so put them all over a common denominator $a_0(y) \in K[y]$ and write them as $c_i(y) = a_i(y)/a_0(y)$ for polynomials $a_i(y) \in K[y]$. Set $n := \max\{\deg_y a_i(y) : 0 \leq i \leq m\}$ and write

$$a_i(y) := \sum_{j=0}^{n} a_{i,j} y^{n-j} \text{ for } a_{i,j} \in K.$$

Then $a_0(y) \cdot f(t)$ may be reorganized in the following way:

$$\begin{aligned} a_0(y) \cdot f(t) &= a_0(y) \cdot t^m + a_1(y) \cdot t^{m-1} + \cdots + a_{m-1}(y) \cdot t + a_m(y) \\ &= \sum_{i=0}^{m} \Big(\sum_{j=0}^{n} a_{i,j} y^{n-j} \Big) t^{m-i} = \sum_{j=0}^{n} \Big(\sum_{i=0}^{m} a_{i,j} t^{m-i} \Big) y^{n-j} \end{aligned}$$

Setting $b_j(t) := \sum_{i=0}^{m} a_{i,j} t^{m-i}$ then gives the relation

$$a_0(y) \cdot f(t) = b_0(t) \cdot y^n + b_1(t) \cdot y^{n-1} + \cdots + b_{n-1}(t) \cdot y + b_n(t)$$

where $b_0(t) \neq 0$ by the choice of n. Consider now the polynomial

$$g(s) := s^n + \frac{b_1(x)}{b_0(x)} \cdot s^{n-1} + \cdots + \frac{b_{n-1}(x)}{b_0(x)} \cdot s + \frac{b_n(x)}{b_0(x)} \in K(x)[s].$$

Note that $b_0(x) \neq 0$ since x is transcendental over K. Now the relation established means that

$$a_0(y) \cdot f(x) = b_0(x) \cdot g(y).$$

But $f(x) = 0$, so $g(y) = 0$, meaning that y is algebraic over $K(x)$. ∎