

MATH 731, FALL 2008
HOMEWORK SET 9 sample solutions

- A. Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} (and verify it is the minimal polynomial). Show that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

Answer & Proof. Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 = 5 + 2\sqrt{6}$, so $(\alpha^2 - 5)^2 = 24$. This means α is a root of $f = x^4 - 10x^2 + 1$. We believe this is the minimal polynomial, but all we know immediately is that it's a multiple of the minimal polynomial. We give four proofs of this fact, but only the first one is complete.

Proof 1 that f is the minimal polynomial. If we show f is irreducible, it's the minimal polynomial. It would be nice to apply Eisenstein's criterion — perhaps to $f(x \pm a)$ — but that doesn't seem to work. The rational root test tells us ± 1 are the only possible roots and they are not roots, so if f factors, it factors as $f = gh$ with g, h of degree 2.

By Gauss's Lemma, if there is such a factorization in $\mathbb{Q}[x]$, there must be one in $\mathbb{Z}[x]$. Hence we may assume $g = x^2 + ax + b$, $h = x^2 + cx + d$, $c, d \in \mathbb{Z}$. Thus $x^4 - 10x^2 + 1 = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd$. This immediately tells us $c = -a$, and equating the other coefficients, we see $b+d-a^2 = -10$, $a(d-b) = 0$, $bd = 1$. The last equality tells us $b = d = \pm 1$, and the first equality then becomes $\pm 2 - a^2 = -10$, which has no integer solutions. Thus it is impossible for such g, h to exist.

Proof 2 that f is the minimal polynomial. Again, we show f is irreducible. One can show that if $\alpha, \beta, \gamma, \delta$ are the 4 numbers $\pm\sqrt{2} \pm \sqrt{3}$, then $\alpha, \beta, \gamma, \delta$ are roots of f . Thus $f = (x - \alpha)(x - \beta)(x - \gamma)(x - \delta)$. You can check(!) that none of these numbers are rational, so f has no linear or cubic factors in $\mathbb{Q}[x]$.

Thus if f is reducible, it has two quadratic factors. That means some pair of $\alpha, \beta, \gamma, \delta$ has rational sum and rational product. You can check(!) that this is not the case. For example, the sum is either $\pm 2\sqrt{2}$ or $\pm 2\sqrt{3}$ or 0, and if it is 0, the product is $-(\sqrt{2} \pm \sqrt{3})^2$, which is not rational. Thus f is irreducible.

Proof 3 that f is the minimal polynomial. As we noted above, the rational root test shows that f has no linear, and hence no cubic, factors. Thus if f is not the minimal polynomial, the minimal polynomial must have the form $g = x^2 + ax + b$. Now $g(\alpha) = 2\sqrt{6} + a\sqrt{2} + a\sqrt{3} + (b+5)$. This can never equal zero, since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over \mathbb{Q} . (But is this linear independence obvious?)

Proof 4 that f is the minimal polynomial. $\alpha = \sqrt{2} + \sqrt{3}$ lies in $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Note that $[E : \mathbb{Q}] = 4$, since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$. (Why not?) Thus the splitting field for the minimal polynomial of α must be a subfield of E . If it is E , then $x^4 - 10x^2 + 1$ is the minimal polynomial of α .

If the splitting field is smaller than E , then it has dimension 2 over \mathbb{Q} . Since the automorphism group of E is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, there are only three quadratic extensions of \mathbb{Q} inside E , namely $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{6}]$. To finish the proof, show that $\sqrt{2} + \sqrt{3}$ is not in any of those fields.

Once we know f is the minimal polynomial, we know $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$. Since $\alpha = \sqrt{2} + \sqrt{3}$, we clearly have $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. But

$$\left[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q} \right] = \left[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}] \right] \left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q} \right] \leq 2 \cdot 2 = 4.$$

Thus the dimensions are both 4 and $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

- B. Let $F_n/F_{n-1}/F_{n-2}/\cdots/F_1/F_0$ be a tower of fields. Prove that F_n/F_0 is an algebraic extension if and only if F_i/F_{i-1} is an algebraic extension for each $i = 1, \dots, n$.

Proof. Suppose F_n/F_0 is algebraic and $\alpha \in F_i$. Then $\alpha \in F_n$, so it is a root of some nonconstant polynomial $f \in F_0[x]$. Certainly $f \in F_{i-1}[x]$, so α is algebraic over F_{i-1} .

Suppose conversely that each F_i/F_{i-1} is algebraic. We will prove that F_n/F_0 is algebraic by induction on n . This is true by hypothesis when $n = 1$.

Suppose now that we are given a tower as above and F_{n-1}/F_0 is algebraic. We will use Propositions 2.4 and 2.10 repeatedly. Let $\alpha \in F_n$ have minimal polynomial $p \in F_{n-1}[x]$. By hypothesis, the coefficients a_0, \dots, a_m of p are algebraic over F_0 , so $K = F[a_0, \dots, a_m] = F(a_0, \dots, a_m)$ is a finite dimensional extension of F_0 .

Since $f \in K[x]$, we see that α is algebraic over K . Thus $K(\alpha) = K[\alpha]$ is finite dimensional over K . It follows that $K(\alpha)$ is finite dimensional over F_0 . Since $F_0[\alpha] \subseteq K[\alpha]$, $F_0[\alpha]$ is finite dimensional over F_0 . Thus α is algebraic over F_0 .

- C. Let E/F be an algebraic extension of fields and let $\phi : E \rightarrow E$ be an F -homomorphism.

(1) Suppose $\alpha \in E$ and the minimal polynomial $p \in F[x]$ of α has degree n . We know $\phi^i(\alpha)$ is a root of p for all $i \in \mathbb{N}$. Show that $\phi^k(\alpha) = \alpha$ for some positive integer $k \leq n$.

Proof. Since ϕ fixes elements of F pointwise, we have $p(\phi(\alpha)) = \phi(p(\alpha)) = 0$, so $\phi(\alpha)$ is a root of p . By induction, it follows that $\phi^i(\alpha)$ is a root of p for every $i \in \mathbb{N}$. However, p has at most n roots, so there must exist i, j with $0 \leq i < j \leq n$ with $\phi^i(\alpha) = \phi^j(\alpha)$. If we set $k = j - i$, then since ϕ is one-to-one (as are all field homomorphisms), we have $\phi^k(\alpha) = \alpha$.

(2) Conclude that ϕ is onto.

Proof. Let $\alpha \in E$. By (1), there is a positive integer k with $\alpha = \phi^k(\alpha) = \phi(\phi^{k-1}(\alpha))$. Thus $\alpha \in \text{im } \phi$.