KMB, 21/10/13

M3P11 Galois Theory, Problem Sheet 2 Solutions

1. (a) If $\sqrt{n} = p/q$ in lowest terms (with $p, q \in \mathbb{Z}$ and $q \neq 0$) then we deduce that $nq^2 = p^2$. In particular q^2 divides p^2 – but q^2 and p^2 are coprime, so $q^2 = 1$, so $p/q \in \mathbb{Z}$.

(b) We know $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ (if you like you can deduce this from 2.4 and the fact that $x^2 - 2$ is irreducible, although we did prove it directly). We now prove $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ by contradiction.

If $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ then squaring both sides and tidying up, we deduce $2ab\sqrt{2} \in \mathbb{Q}$. But $\sqrt{2} \notin \mathbb{Q}$ by part (a), so $2ab = 0$, so either $a = 0$ or $b = 0$. If $b = 0$ then $\sqrt{3} \in \mathbb{Q}$, contradicting part (a). If $a = 0$ then $\sqrt{3} = b\sqrt{2}$ and multiplying both sides by $\sqrt{2}$ we deduce $\sqrt{6} \in \mathbb{Q}$, also contradicting part (a). Either way we're there, so $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

The min poly of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ must then be $x^2 - 3$. Why? It's monic, and has coefficients in the right field, so the only issue is whether it's irreducible. And it is, because if it factored then it would have to factor into two linear factors, and one of them would be (up to a constant) $x - \sqrt{3}$, but we've just shown that this polynomial does not have coefficients in $\mathbb{Q}(\sqrt{2})$.

(c) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.2 = 4$. We know both extensions on the right have degree 2; for one it's clear and for the other it comes from part (b) and Lemma 2.4.

2. (a) If $\alpha = \sqrt{2} + \sqrt{3}$ then $\alpha^2 = 5 + 2\sqrt{6}$ and hence $\sqrt{6} = (\alpha^2 - 5)/2 \in \mathbb{Q}(\alpha)$. Hence $\beta := \sqrt{6}\alpha = \sqrt{12} + \sqrt{18} = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\alpha)$. So $\sqrt{2} = \beta - 2\alpha \in \mathbb{Q}(\alpha)$ and now $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$.

We deduce that $\mathbb{Q}(\alpha)$ contains $\sqrt{2}$ and $\sqrt{3}$, so it contains $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. The converse inclusion is obvious, so the two fields are equal.

(b) $p(x) = x^4 - 10x + 1$ can be checked to be a polynomial in $\mathbb{Q}[x]$ such that $p(\alpha) = 0$. Hence it is a multiple of the minimal polynomial of α. But part (a) and Lemma 2.4 imply that the degree of the min poly of α is 4, so $p(\alpha)$ must be a constant multiple of this min poly, so it must be the min poly, so it must be irreducible!

3. Evil trick question: answer is yes! It's $\frac{1}{3}\sqrt{6}\sqrt{15}$.

4. (i) γ clearly satisfies $(\gamma^3 - 1)^2 = 3$, so it's a root of the polynomial $(x^3 - 1)^2 - 3$ which is $x^6 - 2x^3 - 2$. This polynomial is irreducible by Eisenstein, so it must be the min poly of γ, and the degree of γ over $\mathbb{Q}$ is 6.

Note that $\sqrt{3} = \gamma^3 - 1 \in \mathbb{Q}(\gamma)$ so if $F = \mathbb{Q}(\gamma)$ and $K = \mathbb{Q}(\sqrt{3})$ we must have $\mathbb{Q} \subseteq K \subseteq F$ and the tower law gives $2[F : K] = [K : \mathbb{Q}][F : K] = [F : \mathbb{Q}] = 6$ by Lemma 2.4, and we deduce $[F : K] = 3$. Because F contains $\sqrt{3}$ it must contain K and it's not hard to deduce that $F = K(\gamma)$. By Lemma 2.4 again, the degree of γ over K must then be 3.

Note that if one could show that $x^3 - (1 + \sqrt{3})$ were irreducible in $K[x]$ then this would be another way to do the question, but I did not explain any techniques for doing this. In fact Eisenstein's criterion works fine over number fields, so this would be another way of doing it, but I don't want to assume any of next term's algebraic number theory course in this course.

(ii) Even more evil trick question. Turns out $\delta = 1 + \sqrt{3}$ (cube it out to check) so the degree is 2 over $\mathbb{Q}$ and also over $\mathbb{Q}(\sqrt{2})$, the latter because we saw in 1(b) that $\delta \notin \mathbb{Q}(\sqrt{2})$ (it would imply $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$).

5. Any subfield of $\mathbb{C}$ must contain 0 and 1, and be closed under $+$ and $-$ (so must contain $\mathbb{Z}$) and also $\times$ and division (so must contain $\mathbb{Q}$).

6. If $[K : E]$ is infinite then F has an infinite-dimensional E-subspace and hence must be infinite-dimensional over E (for any $n \geq 1$ we can choose n E-linearly independent elements of K and these give n E-linearly independent elements of F).

If $[F : K]$ is infinite, then $[F : E]$ must also be infinite, because for any n we can choose n elements of F that are K-linearly independent, and these are easily checked to also be E-linearly independent.

7.

(i) By Proposition 2.2 we know that if $E \subseteq F$ then $z \in F$ is algebraic over E iff $[F : E]$ is finite. Now say a, b are complex numbers, algebraic over $\mathbb{Q}$. Then $[\mathbb{Q}(a) : \mathbb{Q}]$ is finite. Moreover b is algebraic over $\mathbb{Q}(a)$, because it is a root of a non-zero polynomial with coefficients in $\mathbb{Q} \subseteq \mathbb{Q}(a)$. Hence b is algebraic over $\mathbb{Q}(a)$, so $[\mathbb{Q}(a)(b) : \mathbb{Q}(a)]$ is finite. But $\mathbb{Q}(a)(b) = \mathbb{Q}(a, b)$ (think about it) so both $[\mathbb{Q}(a, b) : \mathbb{Q}(a)]$ and $[\mathbb{Q}(a) : \mathbb{Q}]$ are finite. By the tower law $[\mathbb{Q}(a, b) : \mathbb{Q}]$ is finite. Hence $\mathbb{Q}(a + b)$, $\mathbb{Q}(a - b)$, $\mathbb{Q}(ab)$ and, if $a \neq 0$, $\mathbb{Q}(1/a)$ are all sub-$\mathbb{Q}$-vector spaces of the finite-dimensional vector space $\mathbb{Q}(a, b)$, and hence are also finite-dimensional. Hence $a \pm b$, ab and $1/a$ are algebraic. So A is a field.

(ii) Say $[A : \mathbb{Q}] = n < \infty$. Let $p(x) = x^{n+1} - 2$ and let $\alpha \in \mathbb{C}$ be a root. Then α is algebraic and its min poly must be $p(x)$ as $p(x)$ is monic and irreducible. So $n = [A : \mathbb{Q}] = [A : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = (n + 1)[A : \mathbb{Q}(\alpha)] \geq n + 1 > n$, a contradiction.

(iii) For each n there are only countably many elements of $\mathbb{Q}[x]$ with degree at most n, and a countable union of countable sets is countable, so there are only countably many polynomials. Each algebraic number is a root of a non-zero polynomial in $\mathbb{Q}[x]$ and such a polynomial has only finitely many roots, and a countable union of finite sets is countable, so A is countable.

(iv) If $[\mathbb{C} : A]$ were finite then $\mathbb{C}$ would be isomorphic to A^n for some $n \in \mathbb{Z}_{\geq 1}$ and hence $\mathbb{C}$ would be countable, a contradiction.