KMB, November 15, 2013

M3P11 Galois Theory, Problem Sheet 4, solutions

1. In the language of rings, the argument goes like this: the kernel is an ideal, and if it is non-zero then it contains an invertible element (as every non-zero element of a field is invertible) and hence contains 1; but 1 maps to 1 and hence cannot be in the kernel.

Without this language, the argument goes something like this. Say $\phi : K \to L$ is a homomorphism of fields. By definition $\phi(1) = 1$. Say $\phi(t) = 0$ for some $t \neq 0$. Then $1\phi(1) = \phi(t)\phi(1/t) = 0.\phi(1/t)$. But in any field we have $0.x = 0$ for all x, as $0 + 0 = 0$ so $0.x + 0.x = (0 + 0).x = 0.x$ and cancelling $0.x$ in the additive group of K we deduce $0.x = 0$. This is a contradiction.

2. We need to check that any non-constant polynomial $p(x) \in F[x]$ has a root in F. Because K is algebraically closed, $p(x)$ certainly has a root in K. This root is algebraic over F, and hence algebraic over E; hence it is in F by definition. Finally F is obviously algebraic over E, by definition.

Note also that F is normal over E, because any polynomial in $E[x]$ has all its roots in F.

3.

(i) $\mathbb{Q}(\sqrt{6})$ is the splitting field of the polynomial $x^2 - 6$ and is hence normal over $\mathbb{Q}$.

(ii) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2 - 2)(x^2 - 3)$ and is hence normal.

(iii) $\mathbb{Q}(7^{1/3})$ contains one, but not all, roots of the irreducible polynomial $x^3 - 7$ (because the other roots are not even real), so it is not normal over $\mathbb{Q}$.

(iv) $\mathbb{Q}(7^{1/3}, e^{2\pi i/3})$ is the splitting field of $x^3 - 7$ and is hence normal.

(v) [Easier version] $\mathbb{Q}(\sqrt{1 + \sqrt{7}})$ is not normal over $\mathbb{Q}$. Here's why. If $\alpha = \sqrt{1 + \sqrt{7}}$ then $\alpha^2 - 1 = \sqrt{7}$, so $(\alpha^2 - 1)^2 = 7$ and α is hence a root of $x^4 - 2x^2 - 6 = 0$. We can spot the four complex roots of this polynomial; they are $\pm\sqrt{1 \pm \sqrt{7}}$ (just substitute in to see that all of these are roots). Two of these numbers are real and two pure imaginary; in particular not all of them are in $\mathbb{Q}(\sqrt{1 + \sqrt{7}})$, which is a subfield of the reals. However, $x^4 - 2x^2 - 6 = 0$ is irreducible over $\mathbb{Q}$ by Eisenstein, so this polynomial has some but not all roots in $\mathbb{Q}(\sqrt{1 + \sqrt{7}})$ which is hence not normal over $\mathbb{Q}$.

[Original version; harder because you can't use Eisenstein]. $\mathbb{Q}(\sqrt{1 + \sqrt{2}})$ is not normal over $\mathbb{Q}$. Here is why. If $\alpha = \sqrt{1 + \sqrt{2}}$ then $\alpha^2 - 1 = \sqrt{2}$, so $(\alpha^2 - 1)^2 = 2$ and α is hence a root of $x^4 - 2x^2 - 1 = 0$. We can spot the four complex roots of this polynomial; they are $\pm\sqrt{1 \pm \sqrt{2}}$ (just substitute in to see that all of these are roots). Two of these numbers are real and two pure imaginary, and all four are hence distinct. I now claim that the polynomial $x^4 - 2x^2 - 1$ is irreducible over $\mathbb{Q}$. For certainly it has no rational roots (for example if α is rational then $\alpha^2 - 1$ would also be rational, but this is $\sqrt{2}$) so the only other possibility is that it factors into two irreducible quadratics. However quadratic polynomials with rational coefficients and non-real roots have complex conjugate roots, and hence one of the irreducible factors must have roots $\pm\sqrt{1 - \sqrt{2}}$, meaning that it must be a rational multiple of $x^2 - (1 - \sqrt{2})$; but this polynomial does not have rational coefficients.

We conclude that $x^4 - 2x^2 - 1$ is an irreducible polynomial over $\mathbb{Q}$ with one, but not all, of its roots in $\mathbb{Q}(\alpha)$, and hence $\mathbb{Q}(\alpha)$ is not normal over $\mathbb{Q}$.

(vi) $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is normal over $\mathbb{Q}$, despite the last extension not being normal. The difference is that if $\alpha = \sqrt{2 + \sqrt{2}}$ then (as in the previous question) we see $(\alpha^2 - 2)^2 = 2$ and hence α is a root of $x^4 - 4x^2 + 2 = 0$. This polynomial is irreducible by Eisenstein, but in this case $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is actually its splitting field. For two of its roots are $\pm\alpha$ and the other two are $\pm\sqrt{2 - \sqrt{2}}$ and if $\beta = \sqrt{2 - \sqrt{2}}$ then we see $\alpha\beta = \sqrt{2} = \alpha^2 - 2$, and hence $\beta = (\alpha^2 - 2)/\alpha \in \mathbb{Q}(\alpha)$! So the extension is a splitting field and hence normal.

4. If $\lambda \in F \backslash E$ then $1, \lambda$ is a basis for F over E and hence $\lambda^2 = a\lambda + b$ for some $a, b \in E$. The roots of $x^2 - ax - b = 0$ are hence λ and $a - \lambda$, and neither of these are in E, so $x^2 - ax - b$ is irreducible over E and its splitting field is F, which is hence normal over E.

5. Say $\alpha_1, \ldots, \alpha_n$ is an E-basis for F. Let $p_i(x)$ denote the min poly of α_i over E and let $p(x) = \prod_i p_i(x)$. Let K be a splitting field for $p(x)$ over F. The α_i are all roots of $p(x)$; let β_j

denote the others. Then $K = F(\alpha_i, \beta_j) = E(\alpha_i, \beta_j)$ is a splitting field for $p(x)$ over E too, and is hence normal over E. We claim that it is the normal closure of F. For if $F \subseteq M \subseteq K$ is normal, then each $p_i(x)$ is irreducible over E and has a root in F and hence in M, so splits completely in M; hence p splits completely in M and all the α_i and β_j are in M; thus $M = K$.

In the initial version of this example sheet I asked whether you could generalise this to the general algebraic case. The result is true, but you need to know about splitting fields of infinite sets of polynomials in order to approach this part in a sensible way.

6. (i) If $p(x)$ is irreducible over E and has a root in $M \cap N$, then it has a root in M and a root in N, and hence splits completely in both M and N. So all the roots of $p(x)$ in F are in both M and N, and hence in $M \cap N$. Hence $M \cap N$ is normal.

(ii) If M is the splitting field of $f(x)$ and N is the splitting field of $g(x)$ then MN is the splitting field of $f(x)g(x)$. Hence MN is normal.

7. Say $\alpha \in F$. Let $p(x)$ denote its min poly over E. Then $p(x)$ is irreducible over E and has a root in F, so it has all its roots in F. Similarly $i(\alpha)$ is a root of $i(p(x))$ (the polynomial obtained from $p(x)$ by hitting all the coefficients with i); but $p(x) \in E[x]$ so $i(p(x)) = p(x)$. Moreover $i(F)$ is normal over E (because it is isomorphic to F) and hence p splits completely in $i(F)$ too. In particular this means that $i(F)$ must contain the root α of $p(x)$. Hence $i(F)$ contains F. Now by a dimension count we have $i(F) = F$.