KMB, January 6, 2014

M3P11 Galois Theory, Solutions to problem Sheet 6

1.

(i) $a > 1$ so a has a prime divisor p; now use Eisenstein. Or use uniqueness of factorization to prove $\sqrt{a} \notin \mathbb{Q}$.

Next, if $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ then write $\sqrt{b} = x + y\sqrt{a}$; square, and use the fact that $\sqrt{a}$ is irrational to deduce that $2xy = 0$. Hence either $y = 0$ (contradiction, as $\sqrt{b} \notin \mathbb{Q}$) or $x = 0$ (contradiction, as we can write $ab = cd^2$ with c squarefree, and $a \neq b$ so $c \neq 1$, and again $\sqrt{c} \notin \mathbb{Q}$).

(ii) $F = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ and the preceding part, plus the tower law, shows that $[F : \mathbb{Q}] = 4$. Now F is a splitting field in characteristic zero, so it's finite, normal and separable, so Galois. By the fundamental theorem, $\mathrm{Gal}(F/\mathbb{Q})$ must be a finite group of order 4, so it's either C_4 or $C_2 \times C_2$. There are lots of ways of seeing that it is actually $C_2 \times C_2$. Here are two that spring to mind: firstly, C_4 only has one subgroup of order 2, whereas F has at least two subfields of degree 2 over $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, so by the correspondence in the fundamental theorem, C_4 is ruled out. And another way – if we set $K = \mathbb{Q}(\sqrt{a})$ then F/K is Galois and $[F : K] = 2$, so $\mathrm{Gal}(F/K)$ is cyclic of order 2 by the fundamental theorem, and the Galois group permutes the roots of $x^2 - b$. We deduce that there must be an element of $\mathrm{Gal}(F/K)$, and thus a field automorphism g_a of F, that sends $+\sqrt{b}$ to $-\sqrt{b}$ and fixes $\sqrt{a}$ (as it fixes K). Similarly there's an automorphism g_b of F that sends $+\sqrt{a}$ to $-\sqrt{a}$ and fixes $\sqrt{b}$. This gives us two elements of order 2 in $\mathrm{Gal}(F/\mathbb{Q})$, which must then be $C_2 \times C_2$. Of course their product, $g_a g_b$, sends $\sqrt{a}$ to $-\sqrt{a}$ and $\sqrt{b}$ to $-\sqrt{b}$, so it fixes $\sqrt{ab}$ and is the third non-trivial element of $\mathrm{Gal}(F/\mathbb{Q})$.

The subgroups of $C_2 \times C_2$ are: the subgroup of order 1 (corresponding to F), the group itself, of order 4 (corresponding to $\mathbb{Q}$) (both of these because the Galois correspondence is order-reversing, so i.e. sends the biggest things to the smallest things and vice-versa), and then there are three subgroups of order 2, corresponding to $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$. One way to see this for sure is, for example, that g_a fixes $\sqrt{a}$, so the subfield corresponding to $\langle g_a \rangle$ definitely contains $\sqrt{a}$, but has degree 2 over $\mathbb{Q}$ by the tower law and so must be $\mathbb{Q}(\sqrt{a})$. Arguing like this will show everything rigorously.

Finally, all of the subfields are normal over $\mathbb{Q}$, because all subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ are normal (as it's abelian).

(iii) Every element of $\mathrm{Gal}(F/\mathbb{Q})$ sends $\sqrt{a} + \sqrt{b}$ to something else! (for example g_a sends it to $\sqrt{a} - \sqrt{b}$). So the subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ corresponding to $\mathbb{Q}(\sqrt{a} + \sqrt{b})$ must be the identity, which corresponds to F, and so $F = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

(iv) If $\sqrt{r} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ then $\mathbb{Q}(\sqrt{r})$ must be one of the quadratic subfields of $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, and hence it must be either $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ or $\mathbb{Q}(\sqrt{pq})$ by part (ii). But by part (i) $\sqrt{r}$ is not in any of these fields! Done.

(v) $[F : \mathbb{Q}(\sqrt{p}, \sqrt{q})]$ must be 2 (as it isn't 1) and now use the tower law. The Galois group – we know firstly that any element of the Galois group will be determined by what it does to $\sqrt{p}$, $\sqrt{q}$ and $\sqrt{r}$, and of course $\sqrt{n}$ must be sent to $\pm\sqrt{n}$ for any $n \in \mathbb{Q}$, so there are at most eight possibilities for $\mathrm{Gal}(F/\mathbb{Q})$, corresponding to the $8 = 2^3$ choices we have for the signs. However we know the size of $\mathrm{Gal}(F/\mathbb{Q})$ is eight, so all eight possibilities must occur and the group must be $C_2 \times C_2 \times C_2$.

Let me stress here, for want of a better place, that you *cannot* just say "clearly $\sqrt{p}$, $\sqrt{q}$ and $\sqrt{r}$ are "independent" so we can move them around as we please" – one really has to come up with some sort of an argument to prove that there really is a field automorphism of F sending, for example, $\sqrt{p}$ to $-\sqrt{p}$, $\sqrt{q}$ to $+\sqrt{q}$ and $\sqrt{r}$ to $-\sqrt{r}$. You can build it explicitly from explicit elements you can write down in the Galois group using degree 4 subfields, or you can get it via the counting argument I just explained, but you *can't* just say "it's obvious" because Galois theory is offering you precisely the framework to make the arguments rigorous and I don't think it is obvious without this framework.

(vi) Meh. Think of the Galois group as a 3-dimensional vector space over the field with two elements. There are seven 1-dimensional subspaces (each cyclic of order 2 and generated by the seven non-trivial elements), and there are also seven 2-dimensional subspaces, by arguing for example on the dual vector space – or by arguing that any subgroup of order 4 of $C_2 \times C_2 \times C_2$ is the kernel of a group homomorphism to C_2 and such a homomorphism is determined by where the three generators go; there are eight choices, one of which gives the trivial homomorphism and the other seven of which give order 4 subgroups.

Hence other than F and $\mathbb{Q}$ there are 14 fields; seven have degree 2 and seven have degree 4. The degree 2 ones are $\mathbb{Q}(\sqrt{p^a q^b r^c})$ as a, b, c each run through 0 and 1, but not all zero. The degree 4 ones are $\mathbb{Q}(\sqrt{p^a q^b r^c}, \sqrt{p^d q^e r^f})$ as $(a, b, c), (d, e, f)$ run through bases of the seven 2-dimensional subspaces of the Galois group considered as a vector space of dimension 3 over the field with 2 elements.

(vi) We know all seven non-trivial elements of the Galois group, and none of them fix $\sqrt{p} + \sqrt{q} + \sqrt{r}$ (because if you think of it as a real number, they all send it to something strictly smaller), so the subgroup corresponding to $\mathbb{Q}(\sqrt{p} + \sqrt{q} + \sqrt{r})$ is trivial and we're home.

(vii) Induction and the argument in (v) gives the degree; considering possibilities of signs gives that the Galois group is what you think it is, acting how you think it acts, and the last part again follows by observing that $\mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n})$ corresponding to the trivial subgroup.

2. (i) This is just the same as $x^3 - 2$. If the roots are α, β, γ then the Galois group permutes them, it has order 3 so it must be S_3, the subgroups of order 2 generated by the transpositions fix $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\gamma)$ of degree $6/2 = 3$, and the subgroup A_3 of order 3 corresponds to a normal extension of degree $5/3 = 2$ which must be $\mathbb{Q}(\omega)$ with $1 \neq \omega$ and $\omega^3 = 1$. the normal ones are F, $\mathbb{Q}$ and $\mathbb{Q}(\omega)$.

(ii) Let the roots of $x^4 - 11$ be α (positive and real), and $i\alpha$, $-\alpha$, $-i\alpha$. Now $x^4 - 11$ is irreducible by Eienstein and $\mathbb{Q}(\alpha)$ is contained within the reals so it has degree 4 over $\mathbb{Q}$ and $i \notin \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha, i)$ must have degree 8 over $\mathbb{Q}$ by the tower law, and is clearly a splitting field for $x^4 - 11$. The Galois group is then a subgroup of S_4 (permutations of the roots) of order 8 and as it happens there is only one of these up to isomorphism, by Sylow's theorems for example, if you know Sylow's theorems, so if you're happy with this group theory then the Galois group must be D_8 because D_8 is *a* subgroup of S_4 of order 8. If you're not happy to use Sylow's theorems then you'll have to do it by hand. Again we're lucky in that $\mathbb{Q}(\alpha, i)$ is degree 8 over $\mathbb{Q}$ so the Galois group has order 8, but there are only four possibilities for where an automorphism can send α (the four roots of its min poly) and there are only two possibilies for i (namely $\pm i$) so each must occur. Note that this argument wouldn't have worked if we had used the alternative presentation $\mathbb{Q}(\alpha, \beta)$ of the splitting field; there would have been four possibilities for β and we would have had to think more.

Having established that α maps to something in $\{\alpha, i\alpha, -\alpha, -i\alpha\}$ and i maps to $\pm i$ we need to figure out what this group of order 8 actually *is*. If $i \mapsto i$ and if $\alpha \mapsto i^n \alpha$ then $i^d \alpha \mapsto i^{n+d} \alpha$ and we see that if we regard the four roots of $x^4 - 11$ as the corners of a square then this map corresponds to rotating the square. Similarly fixing α and sending i to $-i$ corresponds to reflecting the square along the long diagonal from $+\alpha$ to $-\alpha$. So now we see that we have two elements which generate the dihedral group D_8 (a rotation and a reflection) and so this must be the full Galois group.

3.

$$\begin{aligned}
\mathbb{Q} &\subseteq \mathbb{Q}\left(8^{1/5}\right) \\
&\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5} + 6}\right) \\
&\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5} + 6}, 5^{1/3}\right) \\
&\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5} + 6}, 5^{1/3}, \sqrt[11]{5^{1/3} + \sqrt{8^{1/5} + 6}}\right) \\
&\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5} + 6}, 5^{1/3}, \sqrt[11]{5^{1/3} + \sqrt{8^{1/5} + 6}}, 9^{1/7}\right)
\end{aligned}$$

4. Q7 of the previous sheet showed $\mathrm{Gal}(F/\mathbb{Q})$ was cyclic of order $p - 1$, which is even, so there is a unique subgroup of order $(p-1)/2$ (the squares, if you're thinking about things number-theoretically) corresponding to a unique quadratic subextension in F.

If $p=3$ then $F=\mathbb{Q}((-1+\sqrt{-3})/2)=\mathbb{Q}(\sqrt{-3})$ so $n=-3$.

If $p=5$ then $F=\mathbb{Q}(\zeta_5)$ with $\zeta_5=e^{2\pi i/5}$. Now F contains $\zeta_5+\zeta_5^{-1}=2\cos(72^o)$ and there are various cute ways of showing that this is $(\sqrt{5}-1)/2$ (drawing some cunning lines in a pentagon, or observing that $\cos(5\theta)$ is a polynomial in $\cos(\theta)$ and then setting $\theta=72^o$, or several other tricks). Anyway, we deduce $\sqrt{5}\in F$ and $n=5$.

In general the quadratic subfield is $\mathbb{Q}(\sqrt{p})$ if $p=4n+1$ and $\mathbb{Q}(\sqrt{-p})$ if $p=4n-1$; this is a little tricky to prove without any help, although you'll find some slick proofs in books; Legendre symbols (qudaratic residues etc) can help here.

5. I don't know how to prove this directly. A proof using separable degrees goes like this: α separable over E implies $[F:E]_s=[F:E]$ by 6.4, and hence F/E is separable by 6.6.

6.

(i) If $L=E(\alpha_1,\ldots,\alpha_n)$ then for $E\subseteq K\subseteq F$ we have that K contains L iff K contains all the α_i. So if $E\subseteq K\subseteq F$ then E contains N iff E contains M and the α_i iff E contains M and L; hence N is the smallest subfield of F containing M and L.

(ii) If L is the splitting field of $p(x)\in E[x]$ and M is the splitting field of $q(x)\in E[x]$ (these polynomials exist by normality) then I claim N is the splitting field of $p(x)q(x)$; indeed if the α_i are the roots of p and β_j are the roots of q then by the first part N is the field generated by the α_i and the β_j. Now N is finite and normal; moreover each of the α_i and the β_j are separable over E (as each is contained in either L or M) and hence each time we adjoin one we get a separable extension; finally a separable extension of a separable extension is separable (by comparing degrees and separable degrees).

(iii) If $g\in\mathrm{Gal}(N/E)$ then $g(L)=L$ by 6.7 and hence the restriction of g to L is in $\mathrm{Gal}(L/E)$. Similar for M/E. So we get a map $\mathrm{Gal}(N/E)\to\mathrm{Gal}(L/E)\times\mathrm{Gal}(M/E)$. This is easily checked to be a group homomorphism. It's injective because anything in the kernel fixes L and M pointwise, so fixes LM pointwise; but $LM=N$.

It's not always surjective though – for example if $L=M$ then it hardly ever is. More generally if $L\cap M\neq E$ then there will be problems. However if $L\cap M=E$ then my guess is that the map is a bijection; however it's nearly midnight and so I think I'll leave this as an exercise for the interested reader!