GALOIS THEORY
Solutions to Worksheet 6

A 1. (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 hence it is normal.

(iii) $\mathbb{Q}(7^{1/3})$ contains one, but not all, roots of the irreducible polynomial x^3-7[1] (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 hence it is normal.

(v) $\mathbb{Q}(\sqrt{1+\sqrt{7}})$ is not normal over $\mathbb{Q}$. Here is 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 the polynomial $X^4-2X^2-6\in\mathbb{Q}[X]$. 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 is irreducible over $\mathbb{Q}$ (one can use the Eisenstein criterion, or argue in an adhoc manner, or use the theory of biquadratic extensions soon to be discussed), so **this polynomial has some but not all roots in** $\mathbb{Q}(\sqrt{1+\sqrt{7}})$ which — by Remark 17 (ii) following Lemma 16 of the GALOIS THEORY notes — is hence not normal over $\mathbb{Q}$.[2]

(vi) $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is normal over $\mathbb{Q}$, despite the formal similarity with part (v). 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 $X^4-4X^2+2\in\mathbb{Q}[X]$. 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.

A 2. (a) First note that if $\alpha=2^{1/3}$ then L is the splitting field of X^3-2 over $\mathbb{Q}$; indeed the splitting field is by definition $\mathbb{Q}(\alpha,\omega\alpha,\omega^2\alpha)$ (as these are the roots), and this field must be $\mathbb{Q}(\alpha,\omega)$ because each of the generators of one field can be easily checked to be in the other.

[1] In other words we are using the following property of normal extensions: If $K\subset L$ is normal, and $f\in K[X]$ an irreducible polynomial, then either f has no roots in L, or f splits completely in L.

[2] The very important statement made in Remark 17 (ii) is repeated in Theorem 41 (I) of Sec. 8 of the GALOIS THEORY notes.

We immediately deduce that $K \subset L$ and $F \subset L$ are normal because both are the splitting field of $X^3 - 2$, seen as a polynomial in either $K[X]$ or $F[X]$. (We can also deduce normality of $F \subset L$ from normality of $K \subset L$.) However $K \subset F$ is not normal, because $X^3 - 2$ is irreducible over K and has one, but not all, roots in F.

(b) Let's first compute some degrees. We know the min poly of $\sqrt{2}$ over $\mathbb{Q}$ has degree 2, so $[F : K] = 2$. Also the min poly of $2^{1/4}$ over $\mathbb{Q}$ must be $X^4 - 2$ (because this poly is irreducible by Eisenstein), and hence $[L : K] = 4$. By the tower law we deduce $[L : F] = 2$ (and hence that $X^2 - \sqrt{2}$ must be the min poly of $2^{1/4}$ over F, but we don't need this). We could argue that $K \subset F$ and $F \subset L$ are normal because they both have degree 2, but we can also see it directly: F is the splitting field of $X^2 - 2$ over K and L is the splitting field of $X^2 - \sqrt{2}$ over F, so they're both normal. However, $X^4 - 2$ is irreducible over K and has one root in L (in fact two roots in L) but not all its roots (as two are not real, whereas $L \subseteq \mathbb{R}$ so $K \subset L$ is not normal).

(c) If H is normal in G then for all $g \in G$ $g^{-1}Hg = H$, so trivially for all $g \in K$ $g^{-1}Hg = H$, that is, H is normal in K.

Examples: $H = \{1\} \subseteq K = \langle (1\,2) \rangle \subseteq S_3$ for the first, and $H = \langle \sigma \rangle \subseteq K = \langle \sigma, \rho^2 \rangle \subseteq G = D_8$ for the second, with $D_8 = \langle \rho, \sigma \rangle$ the dihedral group generated by a rotation ρ of order 4 and a reflection σ of order 2.

A 3. Let's start by adjoining one root of $X^4 - p$, say, α, the positive real 4^{th} root of p. We get a field $K = \mathbb{Q}(\alpha)$. By Eisenstein, $X^4 - p$ is irreducible over $\mathbb{Q}$, so $[K : \mathbb{Q}] = 4$. Is K a splitting field? No, because it's a subfield of the reals, and $X^4 - p$ has some non-real roots (namely $\pm \mathtt{i}\alpha$). However, K does contain two roots of $X^4 - p$, namely $\pm\alpha$, so $X^4 - p$ must factor as $(X + \alpha)(X - \alpha)q(X)$, with $q(X) \in K[X]$ of degree 2 and irreducible (as no roots in K). If $\beta = \mathtt{i}\alpha$ is a root of $q(X)$ and $F = K(\beta)$ then $[F : K] = 2$ so by the tower law $[F : \mathbb{Q}] = 8$. We can alternatively write $F = K(\mathtt{i})$ as $\beta = \mathtt{i}\alpha$, so $F = \mathbb{Q}(\mathtt{i}, \alpha)$.

F is a splitting field over $\mathbb{Q}$ so it's finite, normal and separable (separability isn't an issue as we're in characteristic 0). So we know that the Galois group G of $\mathbb{Q} \subset F$ has size 8. We also know that if $\tau : F \to F$ is an isomorphism then $\tau(\alpha)$ had better be a 4^{th} root of $\tau(p) = p$, so it's $\pm\alpha$ or $\pm\mathtt{i}\alpha$; there are at most 4 choices for $\tau(\alpha)$. Similarly $\tau(\mathtt{i}) = \pm\mathtt{i}$ so there are at most 2 choices for $\tau(\mathtt{i})$. This gives at most 8 choices for τ; however we know that G has size 8, so all eight choices must work. It is not hard now to convince yourself that G is isomorphic to D_8 (think of a square with corners labelled $\alpha, \mathtt{i}\alpha, -\alpha, -\mathtt{i}\alpha$).

A 4. (a) The statement is obvious if b is a square in K so let us assume that it is not. Suppose that there are $x, y \in K$ such that

$$a = (x + y\sqrt{b})^2 = (x^2 + by^2) + 2xy\sqrt{b}$$

Since $1, \sqrt{b}$ are linearly independent over K, we must have that **either**

(i) $y = 0$, in which case $a = x^2$ is a square in K, **or**

(ii) $x = 0$, in which case $a = y^2 b$ and then $ab = (yb)^2$ is a square in K.

(b) Consider $K = \mathbb{F}_2(t)$, $a = 1 + t$, $b = t$. Now $a = (1 + \sqrt{t})^2$ is a square in $K(\sqrt{b})$, but neither a nor b is a square in K.

(c) Suppose say that $a+\beta$ is a square in L. This means that there are $x, y \in K$ such that

$$a+\beta = (x+y\beta)^2 = (x^2+y^2b) + 2xy\beta$$

but then $a-\beta = (x-y\beta)^2$ is also a square in L, and

$$c = a^2-b = (a+\beta)(a-\beta) = [(x+y\beta)(x-y\beta)]^2 = [x^2-y^2b]^2$$

is a square in L.

(d) The roots are $\pm\sqrt{a\pm\sqrt{b}}$; so choose β, α, $\alpha' \in L$ such that $\beta^2 = b$, $\alpha^2 = a+\beta$, ${\alpha'}^2 = a-\beta$. We work with the diagram

$$\begin{tikzcd}
 & L & \\
K(\alpha) \arrow[ur] & & K(\alpha') \arrow[ul] \\
 & K(\beta) \arrow[ul] \arrow[ur] & \\
 & K \arrow[u] &
\end{tikzcd}$$

First, $[K(\beta):K] = 2$ since we are assuming that b is not a square in K.

Write $K_1 = K(\beta)$. I **claim** that $[K(\alpha):K_1] = 2$. Indeed, by Part (b), if $a+\beta$ were a square in K_1, then also $a-\beta$ would be a square in K_1 and then $c = (a+\beta)(a-\beta) = a^2-b$ is a square in K, contradicting one of our assumptions.

Similarly, also $[K(\alpha'):K_1] = 2$.

The conclusion of Part (d) follows from the tower law and the **new claim**: $K_1(\alpha) \neq K_1(\alpha')$. Indeed suppose for a contradiction that $\alpha' \in K_1(\alpha)$: this is saying that $a-\beta$ is a square in $K_1(\sqrt{a+\beta})$. From Part (a) with $u = a-\beta$ and $v = a+\beta$ in K_1, we conclude that **either**:

(i) $a-\beta$ is a square in K_1, contradicting the claim proved that $[K_1(\alpha'):K_1] = 2$, **or**:

(ii) $c = (a-\beta)(a+\beta) = a^2-b$ is a square in K_1.

Since the first alternative led to a contradiction, it must be that c is a square in K_1. We apply Part (a) again with $u = c$, $v = b$ in K. We have c a square in $K(\sqrt{b})$, that is, either c or cb is a square in K, contradicting our assumptions. This final contradiction shows that $K_1(\alpha) \neq K_1(\alpha')$ and finishes Part (c).