GALOIS THEORY
Solutions to Worksheet 2

A 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 $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$. 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) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$. 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 a result proved in class ($[K(\lambda) : K]$ is the degree of the minimal polynomial of λ over K).

A 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) $p(X) = X^4 - 10X^2 + 1$ 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 $[\mathbb{Q}(\alpha) : \mathbb{Q}] =$ deg(minimal poly. of a) imply that the degree of the min poly of α is 4, so $p(X)$ must be a constant multiple of this min poly, so it must be the min poly, so it must be irreducible.

A 3. Answer is yes! It's $\frac{1}{3}\sqrt{6}\sqrt{15}$.

A 4. (a) This is a variant of the Tower Law argument: Let $e_1, \ldots, e_n$ be a basis for L/K and $f_1, \ldots, f_m$ be a basis for V/L. Then $e_i \in L$ and $f_j \in V$, and V is an L-vector space, so $g_{ij} = e_i f_j$ makes sense. Of course the claim is that the g_{ij} form a basis for V considered as a K-vector space, and the same proof as in the tower law works: the g_{ij} span because if $v \in V$ then write v as an L-linear combination of the f_j and then write each coefficient as a K-linear combination of the e_i, and multiply out. For linear independence, if a linear combination

$\sum_{i,j} \mu_{ij} g_{ij} = 0$ then write this as $\sum_j (\sum_i \mu_{ij} e_i) f_j = \sum_j \lambda_j f_j$ and by linear independence of the f_j over L we know the λ_j must be zero, and this means the μ_{ij} are all zero by linear independence of the e_i over K.

(b) So?

A 5. (a) If $a \in R$, then a is the root of a polynomial

$$1 + b_1 X + b_2 X^2 + \cdots + b_n X^n \in K[X]$$

and from this we deduce that

$$\frac{1}{a} = -b_1 - b_2 a - \cdots - b_n a^{n-1} \in R$$

(b) It is obvious that the intersection of any number of subfields of a field is a field. So $K(S)$ is the intersection of all subfields of L that contain K and S (one of these fields is L itself hence the intersection is nonempty). If $S \subset K$ then $K(S) = K$ and we are done. Otherwise pick $t \in S \setminus K$. It follows from the tower law that $[L : K(t)] < [L : K]$, hence we may assume inductively that there is a finite subset $T^\star \subset S$ such that

$$K(S) = K(t)(S) = K(t)(T^\star)$$

but then clearly $K(t)(T^\star) = K(\{t\} \cup T^\star)$.[1] If, say, $T = \{t_1, \ldots, t_n\}$, then $K[T] = K[t_1, \ldots, t_n] = R$ is a ring, $K \subset R \subset L$, hence by Part (a) $k[T]$ is actually a field. If F is any field, $K \subset F \subset L$, such that $T \subset F$, then clearly $K[T] \subset F$, therefore $K[T]$ is the smallest field that contains K and T, in other words, $K[T] = K(T)$.

(c) Clearly $F_1 F_2 = K(F_1, F_2)$ in the notation of Part (b). By Part (b) then there are elements $a_1, \ldots, a_m \in F_1$ and $b_1, \ldots, b_n \in F_2$ such that

$$F_1 F_2 = K[a_1, \ldots, a_m, b_1, \ldots, b_m]$$

It is clear that every polynomial expression in the a_i and b_j can be written as a finite sum as required.

[1] You may prove, it you want, that for all subsets S_1, $S_2 \subset L$, $K(S_1)(S_2) = K(S_1 \cup S_2)$.