GRV II test 3 answers

1. Let $f(x)$ be irreducible in $\mathbb{Q}[x]$ and $g(x)$ be irreducible in $K[x]$ where $[K : \mathbb{Q}] = d$. Suppose that $g|f$.

   (a) Show that $\deg(f)$ divides $d \cdot \deg(g)$.

   Let α be a root of g. Then $[K(\alpha) : K] = \deg(g)$ because g is irreducible over K. Hence $[K(\alpha) : \mathbb{Q}] = d \cdot \deg(g)$. Now α is also a root of f since g divides f. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f)$ because f is irreducible over $\mathbb{Q}$. But $\mathbb{Q}(\alpha) \subseteq K(\alpha)$ and thus $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides $[K(\alpha) : \mathbb{Q}]$.

   (b) Take-home: If K is Galois over $\mathbb{Q}$ then show that all irreducible factors of f in $K[x]$ have the same degree.

   Let G be the Galois group. Let $P = \prod_{\sigma \in G} \sigma(g) \in K[x]$. If $\sigma \in G$ then $\sigma(g)$ is irreducible in $K[x]$ because σ is an automorphism of K. So all irreducible factors of P in $K[x]$ are conjugated to g, so they all have degree $\deg(g)$. But P is G-invariant so its coefficients lie in $K^G = \mathbb{Q}$. Hence $P \in \mathbb{Q}[x]$. The gcd of f and P is either 1 or f because f is irreducible in $\mathbb{Q}[x]$. But it is not 1 since g divides f and P. So this gcd is f, so $f|P$. So irreducible factors of f in $K[x]$ are also irreducible factors of P, and thus have degree $\deg(g)$.
   Footnote: although we don't need this, $P = f^e$ where e is the number of σ's for which $\sigma(g) = g$.

2. Let $k = \mathbb{Q}(\zeta_n)$ and let $a \in k$ and $K = k(a^{1/n})$.

   (a) Show that K/k is a Galois extension.

   Let $f = x^n - a \in k[x]$. Its splitting field over k contains $a^{1/n}$ and thus contains K. Conversely, f splits over K because K contains all roots $\zeta_n^i a^{1/n}$ of f. So K is a the splitting field over k, and is thus Galois over k (in char $= 0$ we don't have to check if f is separable).

   (b) Take-home: Show that $\mathrm{Gal}(K/k)$ is a subgroup of C_n.

   If $a = 0$ then this Galois group is $\{1\}$ which is a subgroup of any group. So assume $a \neq 0$. Let $G = \mathrm{Gal}(K/k)$. We define a group homomorphism $\phi : G \to \mathbb{Z}/(n)$ as follows. If $\sigma \in G$, then it sends $a^{1/n}$ (a root of f) to some root of f. Any root of f can be written as $\zeta_n^i a^{1/n}$ for some $i \in \mathbb{Z}$. Denote $[i]$ as the image of i in $\mathbb{Z}/(n)$. Then we define $\phi(\sigma)$ as $[i]$. This ϕ is injective because $[i]$ is uniquely determined by $\sigma(a^{1/n}) = \zeta_n^i a^{1/n}$. So ϕ maps G injectively to a subgroup of $\mathbb{Z}/(n) \cong C_n$.
   Note: ϕ need not be surjective, for example, if $a = 4$ and $n = 4$ then $[K : k] < n$.

3. Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$.
   Hint for (a)+(b): you can count them without computing them.

(a) How many subfields $E \subset K$ have $[E : \mathbb{Q}] = 4$?

Five.
Recall from class and previous handouts that the Galois group of $x^4 - 2$ is the dihedral group $D_{2\cdot 4}$. The fields E have $[K : E] = 8/4 = 2$ so have to count the number of subgroups of order two, each of which contains e plus one element of order 2. So we just have to count the number of elements of order 2 in $D_{2\cdot 4}$. These are: all 4 reflections, as well as the 180-degree rotation.

Note: in Exercise 3, counting subgroups is much easier than counting subfields, hence the hint.

(b) How many of those subfields are Galois over $\mathbb{Q}$?

One. The only way a subgroup of order two $\{e, \sigma\}$ can be normal is when σ is in the center. Of the five elements of order 2, only one is in the center (namely: the 180-degree rotation).

4. Suppose that $K \subset \mathbb{C}$ is finite extension of $\mathbb{Q}$ with degree $[K : \mathbb{Q}] = n$.

(a) If $\sqrt[d]{2} \in K$ then show that $d|n$.

If $\sqrt[d]{2} \in K$ then $\mathbb{Q}(\sqrt[d]{2}) \subseteq K$ but then $[K : \mathbb{Q}] = n$ must be divisible by $[\mathbb{Q}(\sqrt[d]{2}) : \mathbb{Q}] = d$.

(b) In the rest of this exercise, assume that $K/\mathbb{Q}$ is Galois with group G.

If $\sqrt[d]{2} \in K$ then show that $\phi(d)|n$ where ϕ is the Euler ϕ function.

If K is Galois over $\mathbb{Q}$ and $\sqrt[d]{2} \in K$ then K must also contain all roots of its minpoly $x^d - 2$ over $\mathbb{Q}$. Then $\zeta_d \sqrt[d]{2} \in K$, hence $\zeta_d \in K$, and hence $\mathbb{Q}(\zeta_d) \subseteq\in K$. Then $[K : \mathbb{Q}] = n$ must be divisible by $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \phi(d)$.

(c) If G is abelian then show that $\sqrt[3]{2} \notin K$.

If G is abelian, then any subgroup is normal, and thus any subfield is Galois over $\mathbb{Q}$. But $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$.

(d) If G is cyclic then show that $\zeta_8 \notin K$.

If G is cyclic, then any quotient group of G is cyclic as well, and thus $\mathrm{Gal}(E/\mathbb{Q})$ is cyclic for any subfield E of K. Hence $\mathbb{Q}(\zeta_8)$ (whose Galois group is not cyclic) can not be a subfield of K.

(e) Take-home: show that $[K : K \bigcap \mathbb{R}] \leq 2$.

Complex conjugation is an element $\tau \in G$ and has order ≤ 2
(order 1 if $K \subseteq \mathbb{R}$, and order 2 otherwise).
Now $[K : K \bigcap \mathbb{R}] = [K : K^{<\tau>}] = | < \tau > | \leq 2$.

Note: if K is not Galois then complex conjugation need not be in $\mathrm{Aut}(K)$ (the complex conjugate of K could be $\neq K$) in which case $[K : K \bigcap \mathbb{R}]$ could be larger than 2, for instance, if $K = \mathbb{Q}(\sqrt[4]{-2})$ then $[K : K \bigcap \mathbb{R}] = [K : \mathbb{Q}] = 4$.