1. [August 2007 Prelim, Part 4, Question 1] Let $f \in \mathbb{Q}[x]$, monic, irreducible of the degree d. Suppose that the Galois group of f is Abelian of order 360. What are the possible values of d?

   Proof. [Note that the Galois group of f is simply the Galois group of the splitting field of f.] Let K be the splitting field of f [over $\mathbb{Q}$]. Let $\alpha \in K$ be a root of f and let $F \stackrel{\text{def}}{=} \mathbb{Q}[\alpha]$. Then, $F \subseteq K$ and f is the minimal polynomial of α over $\mathbb{Q}$ [as it is monic, irreducible and $f(\alpha) = 0$]. Thus $[F : \mathbb{Q}] = d$.

   But since $K/\mathbb{Q}$ is Abelian, so is $F/\mathbb{Q}$ [as seen in class]. In particular, $F/\mathbb{Q}$ is normal, and since f is irreducible with a root in F, we must have that f splits in F. Thus, $K = F = \mathbb{Q}[\alpha]$, and $d = \deg(f) = [\mathbb{Q}[\alpha] : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})| = 360$. [I.e., $d = 360$ is the only possibility.] $\square$

2. [A question that was asked in class by Thomas] Consider the field extensions:

$$
\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & F = K_1 \cap K_2 &
\end{tikzcd}
$$

   If K_1/F is Galois, then so is K_1K_2/K_2, with isomorphic Galois groups. This implies [by the *Fundamental Theorem of Galois Theory*] that there is a 1-to-1 and onto correspondence between intermediate fields of K_1/F and K_1K_2/K_2. Is it the case that this holds even if K_1/F is not Galois?

   Answer. **Separable Extensions:** Yes.

Let L_1 be the normal closure of K_1/F. [Hence, L_1/F is Galois.] So, we have:

$$\begin{tikzcd}[column sep=small]
& L_1K_2 \arrow[dl, dash] \arrow[dr, dash] & & \\
L_1 \arrow[dr, dash] & & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
& K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
& & F = K_1 \cap K_2 &
\end{tikzcd}$$

Since Galois extensions are distinguished, we have that L_1K_2/K_2 is Galois. By *Natural Irrationalities*, we have that $\mathrm{Gal}(L_1K_2/K_2) \cong \mathrm{Gal}(L_1/F)$, via the map $\Phi : \sigma \mapsto \sigma|_{L_1}$.

Then, clearly, if $\sigma \in \mathrm{Gal}(L_1K_2/K_1K_2)$, we have that $(\sigma|_{L_1})\,|_{K_1} = \mathrm{id}_{K_1}$, and hence $\Phi(\sigma) = \sigma|_{L_1} \in \mathrm{Gal}(L_1/K_1)$.

Conversely, if $\sigma \in \mathrm{Gal}(L_1/K_1)$, then there is $\tilde{\sigma} \in \mathrm{Gal}(L_1K_2/K_2)$ such that $\Phi(\tilde{\sigma}) = \sigma$. But, then $\tilde{\sigma}$ fixes both K_1 [as $\tilde{\sigma}|_{K_1} = (\tilde{\sigma}_{L_1})|_{K_1} = \sigma|_{K_1} = \mathrm{id}_{K_1}$, as $\sigma \in \mathrm{Gal}(L_1/K_1)$] and K_2 [as $\tilde{\sigma} \in \mathrm{Gal}(L_1K_2/K_2)$], and hence $\tilde{\sigma} \in \mathrm{Gal}(L_1K_2/K_1K_2)$.

Therefore, Φ induces an isomorphism between $\mathrm{Gal}(L_1K_2/K_1K_2)$ and $\mathrm{Gal}(L_1/K_1)$. So, the intermediate extensions between K_1/F correspond to subgroups of $\mathrm{Gal}(L_1/F)$ containing $\mathrm{Gal}(L_1/K_1)$, while the intermediate extensions between L_1K_2/K_2 correspond to subgroups of $\mathrm{Gal}(L_1K_2/K_2)$ containing $\mathrm{Gal}(L_1K_2/K_1K_2)$, and Φ gives us a bijection between these.

[More explicitly: if $F \subseteq E \subseteq K_1$, then let $H = \mathrm{Gal}(L_1/E)$ and E corresponds to $(L_1K_2)^{\Phi^{-1}(H)}$, an intermediate extension of L_1K_2/K_2.]

Inseparable Extensions: No. [Thanks to S. Mulay!]

Consider $F = \mathbb{F}_p(x^p + y^p, x^py^p)$, $K_1 = \mathbb{F}_p(x+y, xy)$, $K_2 = \mathbb{F}_p(x^p, y)$, where x and y are algebraically independent transcendental elements [i.e., variables].

We have that $K_1 \cap K_2 = F$: we have that the map σ which switches x and y is an automorphism of $\mathbb{F}_p(x, y)$ that fixes K_1 [and F]. [In fact $\mathbb{F}_p(x+y, xy) = \mathbb{F}_p(x, y)^{\langle\sigma\rangle}$] So, if $f \in K_1$ it must be symmetric in x and y. But, if also $f \in K_2$, this means that all powers of x and of y must be multiples of p, i.e., $f \in \mathbb{F}_p(x^p, y^p)$. So, $f \in \mathbb{F}_p(x^p, y^p) \cap \mathbb{F}_p(x+y, xy) = \mathbb{F}_p(x^p + y^p, x^py^p)$ [by the symmetry in x and y].

Clearly, $K_1K_2 = \mathbb{F}_p(x,y)$. So, we have:

$$\begin{tikzcd}[column sep=small]
& K_1K_2 = \mathbb{F}_p(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 = \mathbb{F}_p(x+y, xy) \arrow[dr, dash] & & K_2 = \mathbb{F}_p(x^p, y) \arrow[dl, dash] \\
& K_1 \cap K_2 = F = \mathbb{F}_p(x^p + y^p, x^p y^p) &
\end{tikzcd}$$

So, since $[K_1K_2 : K_2] = p$, there are no proper intermediate extensions between K_1K_2 and K_2. On the other hand, there are infinitely many intermediate extensions between K_1 and $F = K_1 \cap K_2$, as K_1/F has no primitive element: if $f \in K_1$, then $f^p \in F$, but $[K_1 : F] = p^2$. [Note that $u \stackrel{\text{def}}{=} x + y$ and $v \stackrel{\text{def}}{=} xy$ are algebraically independent over $\mathbb{F}_p$!]

[**Note:** K_1/F is purely transcendental, so my comment in class that it worked for purely transcendental was mistaken.]

Transcendental [i.e., non-algebraic] Extensions: No.

Let $K_1 = \mathbb{Q}(x)$, $K_2 = \mathbb{Q}(x+y, xy)$. As above, if $f \in K_2$, then it is symmetric in x and y. If also $f \in K_1$, as it has no y's, it has no x's. So, $K_1 \cap K_2 = \mathbb{Q}$. Also, $K_1K_2 = \mathbb{Q}(x,y)$. So, we have:

$$\begin{tikzcd}[column sep=small]
& K_1K_2 = \mathbb{Q}(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 = \mathbb{Q}(x) \arrow[dr, dash] & & K_2 = \mathbb{Q}(x+y, xy) \arrow[dl, dash] \\
& K_1 \cap K_2 = \mathbb{Q} &
\end{tikzcd}$$

Now, $K_1/\mathbb{Q}$ has infinitely many intermediate extensions [e.g., $\mathbb{Q}(x^n)$ for $n \in \{2, 3, 4, \ldots\}$], but $[K_1K_2 : K_2] = 2$ [as $K_1K_2 = K_2(x) \supsetneq K_2$ and x is a root of $T^2 - (x+y)T + (xy) \in K_2[T]$], so there are no proper intermediate extensions between K_1K_2 and K_2. $\square$