David Beydler
MATH 540B
Due: 2/20/08

13.4 - 1, 2 13.5 - 2

13.4

1) [Determine the splitting field and its degree over $\mathbb{Q}$ for x^4-2.]

First of all, the roots of x^4-2 are: $\sqrt[4]{2}\, e^{i\left(\frac{2\pi k}{4}\right)}$, $k=0,1,2,3$.
So, we have $\sqrt[4]{2}$, $\sqrt[4]{2}\, i$, $-\sqrt[4]{2}$, $-\sqrt[4]{2}\, i$.

I claim that $\boxed{\mathbb{Q}(\sqrt[4]{2}, i)}$ is the splitting field over $\mathbb{Q}$ of x^4-2.
Let F be a splitting field over $\mathbb{Q}$ of x^4-2. Since $\sqrt[4]{2} \in F$ and $i = \frac{1}{2}(\sqrt[4]{2})^3(\sqrt[4]{2}\, i) \in F$, we get that $\mathbb{Q}(\sqrt[4]{2}, i) \subseteq F$. And since all the roots of x^4-2 are in $\mathbb{Q}(\sqrt[4]{2}, i)$, we get that $\mathbb{Q}(\sqrt[4]{2}, i) \supseteq F$.
So, $\mathbb{Q}(\sqrt[4]{2}, i) = F$, so $\mathbb{Q}(\sqrt[4]{2}, i)$ is a splitting field over $\mathbb{Q}$ of x^4-2.
By uniqueness $\mathbb{Q}(\sqrt[4]{2}, i)$ is <u>the</u> splitting field over $\mathbb{Q}$ of x^4-2.

Let's find the degree over $\mathbb{Q}$ of x^4-2 by constructing a tower of fields:

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt[4]{2}, i) & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[ur, dash, "m"] & & \mathbb{Q}(i) \arrow[ul, dash, "n"'] \\
 & \mathbb{Q} \arrow[ul, dash, "4"] \arrow[ur, dash, "2"'] &
\end{tikzcd}
$$

Since $m_{\sqrt[4]{2}, \mathbb{Q}} = x^4-2$, which is irreducible by Eisenstein with $p=2$.

Since $m_{i, \mathbb{Q}} = x^2+1$, which is irreducible by rational roots theorem (± 1 are not roots, but are the only candidates for roots).

We know that $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4m$
$= [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2n$,
so, $n = 2m$. Note that $m \leq 2$ since $x^2+1 \in \mathbb{Q}(\sqrt[4]{2})[x]$ has i as a root. But $m \neq 1$, since if $m=1$, we would have $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ which is not true because $i \notin \mathbb{Q}(\sqrt[4]{2})$. So, $m=2$. Thus the degree over $\mathbb{Q}$ of x^4-2 is $2 \cdot 4 = \boxed{8}$.

(13.4 cont) 2) [Determine the splitting field and its degree over $\mathbb{Q}$ for x^4+2.]

The roots of x^4+2 are: $\sqrt[4]{2}\, e^{i\left(\frac{\pi+2\pi k}{4}\right)}$, $k=0,1,2,3$.
So, we have: $\sqrt[4]{2}(e^{\frac{\pi}{4}i})$, $\sqrt[4]{2}(e^{\frac{3\pi}{4}i})$, $\sqrt[4]{2}(e^{\frac{5\pi}{4}i})$, $\sqrt[4]{2}(e^{\frac{7\pi}{4}i})$.
Expanding, we get $\sqrt[4]{2}\left(\pm\frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}i\right) = \pm\frac{1}{\sqrt[4]{2}} \pm \frac{1}{\sqrt[4]{2}}i$. Here they are listed out:

$$\frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i,\quad \frac{-1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i,\quad \frac{-1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}i,\quad \frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}i$$

I claim that $\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field over $\mathbb{Q}$ of x^4+2.
Let F be a splitting field over $\mathbb{Q}$ of x^4+2. Since
$\sqrt[4]{2} = \left[\left(\frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i + \frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}i\right)/2\right]^{-1} \in F$ and $i = \sqrt[4]{2}\left[\left(\frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i - \frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i\right)/2\right] \in F$,
we get that $\mathbb{Q}(\sqrt[4]{2}, i) \subseteq F$. And since all the roots of x^4+2 can be made from $\sqrt[4]{2}$ and i, we know that $\mathbb{Q}(\sqrt[4]{2}, i) \supseteq F$. So, $\mathbb{Q}(\sqrt[4]{2}, i) = F$, so $\mathbb{Q}(\sqrt[4]{2}, i)$ is a splitting field over $\mathbb{Q}$ of x^4+2.
By uniqueness, $\mathbb{Q}(\sqrt[4]{2}, i)$ is <u>the</u> splitting field over $\mathbb{Q}$ of x^4+2.

From #1, we get that $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$, so the degree over $\mathbb{Q}$ of x^4+2 is $\boxed{8}$.

DB3

$\boxed{13.5}$ 2) [Find all irreducible polynomials of degree 1, 2, and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16}-x$.]

Degree 1: $\boxed{x,\ x+1}$

Degree 2: Generally, these look like $f(x)=x^2+ax+b$. If $b=0$, then f factors: $x(x+a)$. So we must have that $b=1$. If $a=0$, then $f(x)=x^2+1=(x+1)(x+1)$. The only choice we have left is $f(x)=x^2+x+1$. This is irreducible since $f(0)=1$ and $f(1)=1$, so f has no roots in $\mathbb{F}_2$, so since f is of degree 2, it is irreducible.

$\boxed{x^2+x+1}$

Degree 4: In general, we have $g(x)=x^4+ax^3+bx^2+cx+d$. If $d=0$, then g factors: $x(x^3+ax^2+bx+c)$. So, $d=1$, and we have $g(x)=x^4+ax^3+bx^2+cx+1$. We can either have a linear or irreducible quadratic factor, so let's rule those cases out. If $g(1)=0$ then we have a linear factor. This happens if $g(1)=1+a+b+c+1=a+b+c=0$. There are 4 cases where this doesn't happen:

$a=1,\ b=0,\ c=0 \quad (x^4+x^3+1)$
$a=0,\ b=1,\ c=0 \quad (x^4+x^2+1)$
$a=0,\ b=0,\ c=1 \quad (x^4+x+1)$
$a=1,\ b=1,\ c=1 \quad (x^4+x^3+x^2+x+1)$

The only way g could break into irreducible quadratics would be $(x^2+x+1)(x^2+x+1)=x^4+x^2+1$.

So, we are left with the following irreducibles:

$\boxed{x^4+x^3+1,\ x^4+x+1,\ x^4+x^3+x^2+x+1}$

see next page

(13.5 cont) (2 cont)

The product of these irreducibles is computed as follows:

$$x(x+1)(x^2+x+1) = (x^2+x)(x^2+x+1)$$
$$= x^4+x^3+x^3+x^2+x^2+x$$
$$= x^4+x$$

$$(x^4+x)(x^4+x^2+1) = x^8+x^7+\cancel{x^4}+x^5+\cancel{x^4}+x$$
$$= x^8+x^7+x^5+x$$

$$(x^8+x^7+x^5+x)(x^4+x+1) = x^{12}+\cancel{x^9}+\cancel{x^8}+x^{11}+\cancel{x^8}+x^7+\cancel{x^9}+x^6+\cancel{x^5}+\cancel{x^5}+x^2+x$$
$$= x^{12}+x^{11}+x^7+x^6+x^2+x$$

$$(x^{12}+x^{11}+x^7+x^6+x^2+x)(x^4+x^3+x^2+x+1)$$
$$= x^{16}+x^{15}+x^{14}+x^{13}+x^{12}$$
$$+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}$$
$$+x^{11}+x^{10}+x^9+x^8+x^7$$
$$+x^{10}+x^9+x^8+x^7+x^6$$
$$+x^6+x^5+x^4+x^3+x^2$$
$$+x^5+x^4+x^3+x^2+x$$

I lined these up to show cancellation more easily.

$$= x^{16}+x$$
$$= \boxed{x^{16}-x}$$

(In $\mathbb{F}_2$, $x=-x$)