

Math 210B

Fields II

Brett Hemenway

March 3, 2006

10. To check our answers, we can use this short piece of MAGMA code, we just keep adding roots until the polynomial splits.

```
function RecursiveSplit( f, n )
L := Factorization( f );
i := 1;
while( i le #L and Degree( L[i][1] ) eq 1) do
i := i + 1;
end while;
if( i gt #L ) then
return( n ); //f splits
else
f1 := L[i][1]; //pick off the first non-linear factor of f
end if;
k := quo<Parent(f)|f1>; //Adjoin a root of the irreducible factor f1
K<t1> := PolynomialRing( k );
g := 0;
for i:=0 to Degree(f) do
g := g + Coefficient(f,i)*t1^i; //Rewrite f as a polynomial in K<t1>
end for;
return( RecursiveSplit( g, Degree(f1)*n ) );
end function;

function SplittingDegree( f )
return RecursiveSplit( f, 1 );
end function;
```

If $f \in \mathbb{Q}[t]$ and K is the splitting field of f over \mathbb{Q} , to determine $[K : \mathbb{Q}]$, we first factor f over \mathbb{C} .

(a) $f = t^4 + 1$ then

$$\begin{aligned} f &= (t^2 + i)(t^2 - i) = \left(t - \frac{1-i}{\sqrt{2}}\right) \left(t + \frac{1-i}{\sqrt{2}}\right) \left(t - \frac{i+1}{\sqrt{2}}\right) \left(t + \frac{i+1}{\sqrt{2}}\right) \\ &= \left(t - e^{\frac{\pi i}{4}}\right) \left(t - e^{\frac{-\pi i}{4}}\right) \left(t - e^{\frac{3\pi i}{4}}\right) \left(t - e^{\frac{-3\pi i}{4}}\right) \end{aligned}$$

Thus $K = F\left(e^{\frac{\pi i}{4}}\right)$. Since f is irreducible, we see that $m_{\mathbb{Q}}\left(e^{\frac{\pi i}{4}}\right) = f$, so $[K : \mathbb{Q}] = 4$.

```
>Q<t> := PolynomialRing( Rationals() );
>SplittingDegree( t^4 + 1);
4
```

(b) $f = t^6 + 1$ then

$$\begin{aligned} f &= (t^2 + 1)(t^4 - t^2 + 1) \\ &= \left(t - e^{\frac{\pi i}{6}}\right) \left(t - e^{\frac{-\pi i}{6}}\right) \left(t - e^{\frac{3\pi i}{6}}\right) \left(t - e^{\frac{-3\pi i}{6}}\right) \left(t - e^{\frac{5\pi i}{6}}\right) \left(t - e^{\frac{-5\pi i}{6}}\right) \end{aligned}$$

Thus $K = F\left(e^{\frac{\pi i}{6}}\right)$. From the factorization of f , we see that $m_{\mathbb{Q}}\left(e^{\frac{\pi i}{6}}\right) = (t^4 - t^2 + 1)$, so $[K : \mathbb{Q}] = 4$.

```
>Q<t> := PolynomialRing( Rationals() );
>SplittingDegree( t^6 + 1);
4
```

(c) $f = t^4 - 2$ then

$$f = (t^2 - \sqrt{2})(t^2 + \sqrt{2}) = (t - \sqrt[4]{2})(t + \sqrt[4]{2})(t - i\sqrt[4]{2})(t + i\sqrt[4]{2})$$

Thus $K = \mathbb{Q}(\sqrt[4]{2}, i)$, since $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$, we have $[K : \mathbb{Q}] = 8$.

```
>Q<t> := PolynomialRing( Rationals() );
>SplittingDegree( t^4 - 2);
8
```

(d) $f = t^6 - 2$ then

$$\begin{aligned} f &= (t^3 - \sqrt{2})(t^3 + \sqrt{2}) \\ &= (t - \sqrt[6]{2})(t - \omega\sqrt[6]{2})(t - \omega^2\sqrt[6]{2})(t + \sqrt[6]{2})(t + \omega\sqrt[6]{2})(t + \omega^2\sqrt[6]{2}) \end{aligned}$$

Where ω is a cube root of unity, i.e. $\omega = e^{\frac{2\pi i}{3}}$. Thus f splits over $\mathbb{Q}(\sqrt[6]{2}, \omega)$. We know that f is irreducible by Eisenstein, so $m_{\mathbb{Q}}(\sqrt[6]{2}) = f$, which gives $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$. We have $m_{\mathbb{Q}(\sqrt[6]{2})}(\omega) = (t^3 - 1)/(t - 1) = t^2 + t + 1$. Thus $[\mathbb{Q}(\sqrt[6]{2}, \omega) : \mathbb{Q}(\sqrt[6]{2})] = 2 = \phi(3)$. Putting this together, we have $[K : \mathbb{Q}] = 12$.

```
>Q<t> := PolynomialRing( Rationals() );
>SplittingDegree( t^6 - 2);
12
```

- (e) $f = t^6 + t^3 + 1$, we notice that f is the minimal polynomial for the ninth roots of unity, i.e.

$$f = \prod_{\gcd(i,9)=1} (t - e^{\frac{2\pi i}{9}})$$

Thus f splits over $\mathbb{Q}(e^{\frac{2\pi i}{9}})$ and since f is irreducible, we have $m_{\mathbb{Q}}(e^{\frac{2\pi i}{9}}) = f$, so $[K : \mathbb{Q}] = 6$.

```
>Q<t> := PolynomialRing( Rationals() );
>SplittingDegree( t^6 + t^3 + 1);
6
```

11. (a) $f = t^4 - 5t^2 + 6$ thus

$$\begin{aligned} f &= (t^2 - 3)(t^2 - 2) \\ &= (t - \sqrt{3})(t + \sqrt{3})(t - \sqrt{2})(t + \sqrt{2}) \end{aligned}$$

Thus the splitting field of f is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have that

$$\begin{aligned} [K : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= 2 \cdot 2 \\ &= 4 \end{aligned}$$

- (b) $f = t^6 - 1$ then

$$\begin{aligned} f &= (t^3 - 1)(t^3 + 1) \\ &= (t - 1)(t^2 + t + 1)(t + 1)(t^2 - t + 1) \\ &= (t - 1) \left(t - e^{\frac{2\pi i}{3}} \right) \left(t - e^{\frac{4\pi i}{3}} \right) (t + 1) \left(t - e^{\frac{\pi i}{3}} \right) \left(t - e^{\frac{5\pi i}{3}} \right) \end{aligned}$$

Thus we can see that f splits over $\mathbb{Q}\left(e^{\frac{\pi i}{3}}\right)$. From the factorization above, we have that $m_{\mathbb{Q}}\left(e^{\frac{\pi i}{3}}\right) = t^2 - t + 1$. Thus $[K : \mathbb{Q}] = 2 = \phi(6)$.

(c) $f = t^6 - 8$ then

$$\begin{aligned} f &= (t^2 - 2)(t^4 + 2t^2 + 4) \\ &= (t - \sqrt{2})(t + \sqrt{2})(t^2 - \sqrt{2}t + 2)(t^2 + \sqrt{2} + 2) \\ &= (t - \sqrt{2})(t + \sqrt{2})\left(t - \sqrt{2}e^{\frac{\pi i}{3}}\right)\left(t - \sqrt{2}e^{\frac{-\pi i}{3}}\right)\left(t - \sqrt{2}e^{\frac{4\pi i}{3}}\right)\left(t - \sqrt{2}e^{\frac{-4\pi i}{3}}\right) \end{aligned}$$

We have that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and $m_{\mathbb{Q}(\sqrt{2})}\left(e^{\frac{\pi i}{3}}\right) = t^2 - \sqrt{2}t + 1$, which is irreducible, so $[\mathbb{Q}\left(\sqrt{2}, e^{\frac{\pi i}{3}}\right) : \mathbb{Q}(\sqrt{2})] = 2$. Since, this field is the splitting field of f , we have that $K = \mathbb{Q}\left(\sqrt{2}, e^{\frac{\pi i}{3}}\right)$ and $[K : \mathbb{Q}] = 4$.

12. Let $F = \mathbb{Z}/p\mathbb{Z}$

(a) If $p = 2$, then $f(t) = t^2 + t + 1$ is irreducible, just notice that $f(1) = f(0) = 1$.

If p is odd then there are p monic irreducible polynomials of degree 1. Thus there are $(p^2 + 1)/2$ distinct products of degree 1 polynomials. There are p^2 monic polynomials of degree 2. Since every reducible degree 2 polynomial can be factored into a product of degree 1 polynomials, we see that there must be $(p^2 - 1)/2$ monic irreducible degree 2 polynomials.

(b) Let f be an irreducible degree 2 polynomial in $F[t]$. Then the ideal (f) is prime, and since $F[t]$ is a UFD, (f) is maximal. Thus $F[t]/(f)$ is a field. Every element in $F[t]/(f)$ can be written as $at + b$ for $a, b \in F$, so we see that $|F[t]/(f)| = p^2$.

(c) If f_1, f_2 degree 2 irreducible polynomials in $F[t]$, if u_i is a root of f_i , then clearly f_i splits in $F(u_i) = F[t]/(f_i)$ because it has one root in that field. By part (b) these fields both have p^2 elements. So by problem 16, they are both the splitting fields of $t^{p^2} - t$, so by the uniqueness of splitting fields, we have that $F(u_1) \simeq F(u_2)$. Note that this works for irreducible polynomials of any degree, not just 2.

13. Let K/F and $f \in F[t]$.

- (a) Let $\phi : K \rightarrow K$ an F -automorphism. Then if $\alpha \in K$, $f[t] = f_n t^n + \dots + f_0$, then we have

$$\phi(f(\alpha)) = \phi(f_n \alpha^n + \dots + f_0) = f_n \phi(\alpha)^n + \dots + f_0 = f(\phi(\alpha))$$

Thus ϕ takes roots of f to roots of f .

- (b) If $F \subset \mathbb{R}$, and $\alpha = a + ib \in \mathbb{C}$ is a root of f , then $a - ib$ is a root of f because complex conjugation is an \mathbb{R} -automorphism of \mathbb{C} , and hence an F -automorphism of \mathbb{C} .
- (c) Let $F = \mathbb{Q}$, and $m \in \mathbb{Z}$, m not a square. Then the map $a + b\sqrt{m} \mapsto a - b\sqrt{m}$, is an F -automorphism, of $\mathbb{Q}(\sqrt{m})$, so by part (a), if $a + b\sqrt{m}$ is a root of f , then so is $a - b\sqrt{m}$.
14. Let $\phi : \mathbb{R} \rightarrow \mathbb{R}$ be a field automorphism. Then $\phi(1) = 1$, so $\phi(n) = \phi(1) + \dots + \phi(1) = n$. So ϕ fixes \mathbb{Z} . Now

$$1 = \phi(1) = \phi\left(n \frac{1}{n}\right) = n\phi\left(\frac{1}{n}\right)$$

Thus $\phi\left(\frac{1}{n}\right) = \frac{1}{n}$, so ϕ fixes \mathbb{Q} . If $a \in \mathbb{R}$, and $a > 0$, then $\sqrt{a} \in \mathbb{R}$, so

$$\phi(a) = \phi\left(\sqrt{a^2}\right) = \phi(\sqrt{a})^2 \geq 0$$

Thus ϕ preserves order, because

$$b \geq a \Rightarrow b - a \geq 0 \Rightarrow \phi(b - a) \geq 0 \Rightarrow \phi(b) - \phi(a) \geq 0 \Rightarrow \phi(b) \geq \phi(a)$$

Now, suppose $\phi(a) \neq a$. Then, without loss of generality we can assume $\phi(a) > a$. So let $q \in \mathbb{Q}$ with $a < q < \phi(a)$. Then we would have $\phi(a) \leq \phi(q) = q < \phi(a)$ a contradiction. So ϕ must be the identity automorphism.

15. Let p_1, \dots, p_n be distinct prime numbers. Let $f = (t^2 - p_1) \cdots (t^2 - p_n) \in \mathbb{Q}[t]$. We can see that each factor $t^2 - p_i$ is irreducible over a field F iff $t^2 - p_i$ has no roots in F . So we build up a tower of extensions. We can see that $t^2 - p_1$ is irreducible over $\mathbb{Q}[t]$, and so $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$. Let $K_1 = \mathbb{Q}(\sqrt{p_1})$. Then $\sqrt{p_2} \notin \mathbb{Q}(\sqrt{p_1})$, so $[K_1(\sqrt{p_2}) : K_1] = 2$, because $m_{\mathbb{Q}}(\sqrt{p_2}) = m_{K_1}(\sqrt{p_2}) = t^2 - p_2$. It is clear that we can continue in this way, with $K_i = K_{i-1}(\sqrt{p_i})$, and $[K_i : K_{i-1}] = 2$. Thus

$$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = [K_n : K_{n-1}] \cdots [K_1 : \mathbb{Q}] = 2 \cdots 2 = 2^n$$

16. Let $F = \mathbb{Z}/p\mathbb{Z}$, and $f = t^{p^e} - t$. Suppose K is a finite field with p^e elements, then by Lagrange's theorem $x^{p^e} = x$ for all $x \in K$ (see problem 3d). So the polynomial f has p^e distinct roots in K . Thus f splits in K . Clearly F injects into K , so we can view F as a subset of K . There is no subfield of K over which f splits, because every element in K is a root of f , so K is a splitting field of f . Since we have shown the uniqueness of splitting fields, this shows the uniqueness of fields of degree p^e .
17. Let F be a field of characteristic $p > 0$. Let $f = t^4 + 1$. Notice that

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\hookrightarrow F \\ a &\mapsto \underbrace{1_F + \dots + 1_F}_{a \text{ times}} \end{aligned}$$

So if f factors over $\mathbb{Z}/p\mathbb{Z}$, then f factors over F . So we will factor f over $\mathbb{Z}/p\mathbb{Z}$. If $p = 2$, then $f = (t + 1)^4$. Now suppose $p > 2$. We consider three cases

- (i) If $\sqrt{-1} \in F$, then

$$t^4 + 1 = (t^2 - \sqrt{-1})(t^2 + \sqrt{-1})$$

- (ii) If $\sqrt{-2} \in F$, then

$$t^4 + 1 = (t^2 + \sqrt{-2}t + 1)(t^2 - \sqrt{-2}t + 1)$$

- (iii) If $\sqrt{2} \in F$, then

$$t^4 + 1 = (t^2 + \sqrt{2}t - 1)(t^2 - \sqrt{2}t - 1)$$

If we can show that at least one of $\sqrt{-1}, \sqrt{-2}, \sqrt{2}$ lies in $\mathbb{Z}/p\mathbb{Z}$, we will have that f is reducible. Recall that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group. Suppose $(\mathbb{Z}/p\mathbb{Z})^\times = \{\alpha, \alpha^2, \dots, \alpha^{p-1} = 1\}$. From this we can see that $\beta \in \mathbb{Z}/p\mathbb{Z}$ is a square iff $\beta = \alpha^{2n}$ for some n . Now notice that $(-1) \cdot (-2) = 2$. So if $\alpha^{n_1} = -1$, $\alpha^{n_2} = -2$, and $\alpha^{n_3} = 2$, we have $\alpha^{n_1} \alpha^{n_2} = \alpha^{n_3}$ which means that $n_1 + n_2 \equiv n_3 \pmod{p-1}$. Since $p-1$ is even (we have considered the case $p = 2$ already), $n_1 + n_2 \equiv n_3 \pmod{2}$. Thus at least one of the n_i must be even, so at least one of $-1, -2, 2$ is a square. Thus f splits into quadratic factors in $\mathbb{Z}/p\mathbb{Z}$, so f splits into quadratic factors over F . So if $f = g_1 g_2$, where g_1, g_2 are degree 2 polynomials, then either g_i splits or g_i is irreducible. If g_i splits,

then it splits over F_{p^2} , by problem 12c. Since all the splitting fields of degree two polynomials over $\mathbb{Z}/p\mathbb{Z}$ are isomorphic, we have that g_2 splits over F_{p^2} as well. Thus if F contains the finite field having p^2 elements, then f splits. Sometimes f splits over $\mathbb{Z}/p\mathbb{Z}$, as we saw when $p = 2$. We will now analyze this case further. If f splits further, then f must have a root. Again, we return to the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. We know that $\alpha^{p-1} = 1$, so $\alpha^{\frac{p-1}{2}} = -1$. Thus if $\beta^4 = -1$, we have $\beta = \alpha^n$ for some n , so $4n \equiv \frac{p-1}{2} \pmod{p-1}$, thus $8n \equiv 0 \pmod{p-1}$. Thus $p \equiv 1 \pmod{8}$. Conversely, if $p \equiv 1 \pmod{8}$, then $\alpha^{\frac{p-1}{8}}$, is a root of f . Thus f has a root in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod{8}$. Suppose f has a root, β . Then

$$f = t^4 + 1 = (t - \beta)(t - \beta^3)(t - \beta^5)(t - \beta^7)$$

If you don't want to multiply out the right hand side to check this equation, you can notice that $f = \Phi_8$, or

```
> simplify( (t-beta)*(t-beta^3)*(t-beta^5)*(t-beta^7), {beta^4=-1} );
      4
      t + 1
```

To summarize: if $p = 2$ or $p \equiv 1 \pmod{8}$, then f splits over F . If $p > 2$ and $p \not\equiv 1 \pmod{8}$, then f splits if F contains \mathbb{F}_{p^2} .

18. Let $f = t^6 - 3 \in F[t]$.

(a) $F = \mathbb{Q}$. Then f is irreducible by Eisenstein.

$$\begin{aligned} f &= (t^3 - \sqrt{3})(t^3 + \sqrt{3}) \\ &= (t - \sqrt[6]{3})(t - \omega\sqrt[6]{3})(t - \omega^2\sqrt[6]{3})(t + \sqrt[6]{3})(t + \omega\sqrt[6]{3})(t + \omega^2\sqrt[6]{3}) \end{aligned}$$

Where ω is a cube root of unity, i.e. $\omega = e^{\frac{2\pi i}{3}}$. Thus f splits over $\mathbb{Q}(\sqrt[6]{3}, \omega)$. We know that f is irreducible by Eisenstein, so $m_{\mathbb{Q}(\sqrt[6]{3})} = f$, which gives $[\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}] = 6$. We have $m_{\mathbb{Q}(\sqrt[6]{3})}(\omega) = (t^3 - 1)/(t - 1) = t^2 + t + 1$. Thus $[\mathbb{Q}(\sqrt[6]{3}, \omega) : \mathbb{Q}(\sqrt[6]{3})] = 2 = \phi(3)$. Putting this together, we have $[K : \mathbb{Q}] = 12$. We can check:

```
> F<t> := PolynomialRing( Rationals() );
> SplittingDegree( t^6 - 3 );
12
```

(b) $F = \mathbb{Z}/5\mathbb{Z}$. Then f is reducible

$$f = (t^2 + 3)(t^2 + 2t + 3)(t^2 + 3t + 3)$$

As we saw in problem 12c, and 17. The splitting fields of any two degree two polynomials over $\mathbb{Z}/p\mathbb{Z}$ are the same, so the splitting field of f is just the splitting field of t^2+3 , which is $K = F[t]/(t^2+3)$, so $[K : F] = 2$. We can verify this explicitly:

Magma V2.12-19 Fri Feb 10 2006 19:37:03 on fats

Type ? for help. Type <Ctrl>-D to quit.

```
> F := PolynomialRing( FiniteField(5) );
```

```
> K<u> := quo<F|t^2+3>;
```

```
> K<u> := quo<F|F.1^2+3>;
```

```
> L<t> := PolynomialRing( K );
```

```
> Factorization( t^2 + 2*t + 3);
```

```
[
<t + 2*u + 1, 1>,
<t + 3*u + 1, 1>
```

```
]
```

```
> Factorization( t^2 + 3*t + 3);
```

```
[
<t + 2*u + 4, 1>,
<t + 3*u + 4, 1>
```

```
]
```

Or:

```
> F<t> := PolynomialRing( FiniteField(5) );
```

```
> SplittingDegree( t^6 - 3 );
```

```
2
```

(c) $F = \mathbb{Z}/7\mathbb{Z}$. Then f is irreducible

```
> F<t> := PolynomialRing( FiniteField( 7 ) );
```

```
> IsIrreducible( t^6 - 3 );
```

```
true
```

Then if u is a root of f , we have $[F(u) : F] = 6$. Then by problem 12c, we have that f splits in $F(u)$, so $K = F(u)$, and $[K : F] = 6$.

Now we repeat this with the polynomial $f = t^6 + 3$.

(d) $F = \mathbb{Q}$. Then f is irreducible by Eisenstein.

$$f = (t - \sqrt[6]{-3})(t + \sqrt[6]{-3}) \left(t - \frac{(\sqrt[6]{-3})^4}{2} - \frac{1}{2}\sqrt[6]{-3} \right) \left(t - \frac{(\sqrt[6]{-3})^4}{2} + \frac{1}{2}\sqrt[6]{-3} \right) \setminus \\ \left(t + \frac{(\sqrt[6]{-3})^4}{2} - \frac{1}{2}\sqrt[6]{-3} \right) \left(t + \frac{(\sqrt[6]{-3})^4}{2} + \frac{1}{2}\sqrt[6]{-3} \right)$$

So f splits over $F(\sqrt[6]{-3})$, but $m_{\mathbb{Q}}(\sqrt[6]{-3}) = f$, so $[K : F] = 6$.

```
> F<t> := PolynomialRing( Rationals() );
> SplittingDegree( t^6 + 3 );
6
```

(e) $F = \mathbb{Z}/5\mathbb{Z}$. Then

$$f = (t^2 + 4t + 2)(t^2 + t + 2)(t^2 + 2)$$

So by problem 12c, if we split one of the degree two factors, we split all of them, thus

$$K = F[t]/(t^2 + 4t + 2) \simeq F[t]/(t^2 + t + 2) \simeq F[t]/(t^2 + 2)$$

splits f , and so $[K : F] = 2$.

```
> F<t> := PolynomialRing( FiniteField( 5 ) );
> SplittingDegree( t^6 + 3 );
2
```

(f) $F = \mathbb{Z}/7\mathbb{Z}$, then

$$f = (t^3 + 2)(t^3 + 5)$$

Thus by problem 12c, we have that

$$K = F[t]/(t^3 + 2) \simeq F[t]/(t^3 + 5)$$

splits f , so $[K : F] = 3$.