

**Frank Moore**  
**Algebra 901 Notes**  
**Professor: Tom Marley**

**Theorem:** Let  $E/F$  and  $F/L$  be field extensions. Then  $E/L$  is algebraic if and only if  $E/F$  and  $F/L$  are algebraic.

*Proof:* For the forward direction, let  $\alpha \in E$ . Then  $\alpha$  satisfies a polynomial over  $L$ , and hence over  $F$ . Similarly for  $\alpha \in F$ . Consider the reverse direction now. So, let  $\alpha \in E$ . Then there exists a monic polynomial  $f(x) \in F[x]$  such that  $f(\alpha) = 0$ . Write  $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$  where the  $c_i \in F$ . Let  $K = L(c_{n-1}, \dots, c_0)$ . Then  $K$  is a finite algebraic extension of  $L$ . Also,  $f(x) \in K[x]$ . Since  $f(\alpha) = 0$ , we see that  $\alpha$  is algebraic over  $K$ . Therefore  $[K(\alpha) : K] < \infty$ . Therefore, we have that  $[K(\alpha) : L] = [K(\alpha) : K][K : L] < \infty$ . As  $K(\alpha)/L$  is finite, it is algebraic, hence  $\alpha$  is algebraic over  $L$ . Therefore,  $E/L$  is algebraic.

**Definition:** Let  $F$  be a field and  $f \in F[x] \setminus F$ . A field  $L \supset F$  is called a splitting field for  $f(x)$  over  $F$  if  $f(x)$  factors into linear polynomials over  $L[x]$ , but not in any proper subfield of  $L$  containing  $F$ . We say that  $f(x)$  “splits completely” in  $L[x]$ .

**Remarks:**

1. If  $f(x) \in F[x]$  splits completely in a field  $E$  containing  $F$ , then a splitting field for  $f(x)$  is  $F$  adjoin the roots of  $f(x)$  in  $E$ . For example, if  $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$  in  $E[x]$  then a splitting field for  $F$  is  $F(\alpha_1, \dots, \alpha_n)$ .
2. If  $\deg f = n$  and  $L$  is a splitting field for  $f$  then  $[L : F] \leq n!$ .

*Proof:* Let  $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ , so that  $L = F(\alpha_1, \dots, \alpha_n)$ . We proceed by induction on  $n$ . If  $n = 1$  then  $F$  is already the splitting field for  $f$ . If  $n > 1$ , let  $\alpha \in L$  be a root of  $f(x)$ . Then, in  $L[x]$ ,  $f(x) = (x - \alpha)g(x)$ . We first prove a claim:

**Claim:** Let  $E/F$  be a field extension, and let  $g, h \in F[x]$ . If  $g \mid h$  in  $E[x]$  then  $g \mid h$  in  $F[x]$ .

*Proof:* Set  $h = gq$  where  $q \in E[x]$ . Then use the division algorithm in  $F[x]$  to get  $h = gq_1 + r$  where  $q_1, r \in F[x]$  and  $\deg r < \deg g$ . But this same equation holds in  $E[x]$ , so by the uniqueness of the division algorithm, we have that  $q = q_1$  and hence  $q \in F[x]$ .

So, by the claim we have that  $f(x) = (x - \alpha)g(x)$  in  $F(\alpha)[x]$ . Now  $\deg g = n - 1$ . Now we know that  $[F(\alpha) : F] \leq n$  as  $\alpha$  is a root of  $f(x)$  and  $\deg f = n$ . Also,  $L$  is the splitting field of  $g(x)$  over  $F(\alpha)[x]$ . By induction, we have that  $[L : F(\alpha)] \leq n - 1!$ , so that  $[L : F] \leq n!$ .

**Examples:**

1. Find the splitting field for  $x^2 - 5$  over  $\mathbb{Q}$ . This is clearly  $\mathbb{Q}(\sqrt{5})$ .
2. Find the splitting field for  $x^2 - 5$  over  $\mathbb{Q}(\sqrt[3]{5})$ . Set  $L = \mathbb{Q}(\sqrt[3]{5})(\sqrt{5}) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{5})$ , and set  $F = \mathbb{Q}(\sqrt[3]{5})$ . We wish to find out  $[L : F] = [F(\sqrt{5}) : F] = \text{degree of minimal polynomial} = \deg \text{Irr}(\sqrt{5}, \mathbb{Q}(\sqrt[3]{5}))$ . Certainly if  $f(x) = x^2 - 5 \in F[x]$  and  $f(\sqrt{5}) = 0$ . Therefore we have that  $\text{Irr}(\sqrt{5}, \mathbb{Q}(\sqrt[3]{5})) \mid f(x)$ . So,  $\text{Irr}(\sqrt{5}, \mathbb{Q}(\sqrt[3]{5}))$  is either  $x^2 - 5$  or  $x - \sqrt{5}$ . So the question now becomes is  $\sqrt{5} \in \mathbb{Q}(\sqrt[3]{5})$ ? Note that  $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$  as  $x^2 - 5$  is irreducible over  $\mathbb{Q}$  by Eisenstein and similarly, we

have that  $[\mathbb{Q}(\sqrt[3]{5} : \mathbb{Q}) = 3$ . Therefore, if  $\sqrt{5} \in \mathbb{Q}(\sqrt[3]{5})$ , we would have that  $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[3]{5}, \mathbb{Q})$  and thus  $2 \mid 3$ , a contradiction. Therefore, we have that  $[L : \mathbb{Q}(\sqrt[3]{5})] = 2$ .

3. Let  $f(x) = x^2 - 1 \in \mathbb{Q}[x]$ . The roots of  $f(x)$  are called the  $n$ th roots of unity :  $e^{2\pi ik/n}$  for  $0 \leq k \leq n-1$ . The splitting field for  $f(x)$  over  $\mathbb{Q}$  is  $L = \mathbb{Q}(\{e^{2\pi ik/n} \mid 0 \leq k \leq n-1\}) = \mathbb{Q}(e^{2\pi i/n})$ . Note also that  $U_n = \{e^{2\pi ik/n} \mid k \in \{0, 1, \dots, n-1\}\}$  is a cyclic multiplicative group of order  $n$ . Any cyclic generator of  $U_n$  is called a primitive  $n$ th root of unity. I.e.  $e^{2\pi ik/n}$  is primitive if and only if  $(k, n) = 1$ . So  $L = \mathbb{Q}(\omega)$  where  $\omega$  is a primitive  $n$ th root of unity. What is  $[\mathbb{Q}(\omega) : \mathbb{Q}]$ ? We will see later that this is precisely  $\phi(n)$ .

**Proposition:** Let  $p$  be a prime and  $\omega$  be a primitive  $p$ th root of unity over  $\mathbb{Q}$ . Then the irreducible polynomial of  $\omega$  is as follows:

$$\text{Irr}(\omega, \mathbb{Q}) = x^{p-1} + x^{p-2} + \dots + x + 1$$

and therefore, we have that  $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ .

*Proof:*  $\omega$  is a root of  $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1)$  (let the second factor be  $f(x)$ ). Hence  $\omega$  is a root of  $f(x)$ . It is enough to show that  $f(x)$  is irreducible over  $\mathbb{Q}$ . First we mention an important remark:

**Remark:** Let  $f(x)$  be a polynomial in  $F[x]$  where  $F$  is a field and let  $a \in F$ . Then  $f(x)$  is irreducible over  $F$  if and only if  $f(x + a)$  is irreducible over  $F$ .

So, consider  $x^p - 1 = (x - 1)f(x)$ . Then  $(x + 1)^p - 1 = xf(x + 1)$ . Expanding gives

$$x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{i}x^i + \dots + \binom{p}{p-1}x = xf(x + 1)$$

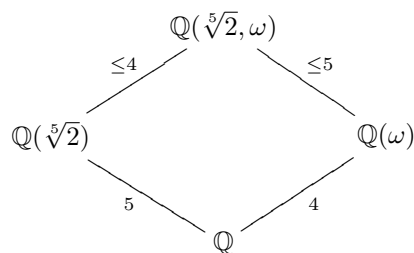
Cancelling  $x$  gives

$$x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{i}x^{i-1} + \dots + \binom{p}{p-1} = f(x + 1)$$

Now by Eisenstein (take  $p = p$ ) we have that  $f(x + 1)$  is irreducible over  $\mathbb{Q}$ . Hence by the remark  $f(x)$  is irreducible over  $\mathbb{Q}$ .

**Example:** Find the splitting field and its degree of  $x^5 - 2$  over  $\mathbb{Q}$ .

*Solution:* The roots of  $x^5 - 2$  are  $\omega^i \sqrt[5]{2}$  for  $i = 0, 1, 2, 3, 4$  and where  $\omega$  is a primitive 5th root of unity. Let  $L$  be the splitting field of  $x^5 - 2$  over  $\mathbb{Q}$ . Then  $L = \mathbb{Q}(\sqrt[5]{2}, \omega \sqrt[5]{2}, \dots, \omega^4 \sqrt[5]{2}) = \mathbb{Q}(\sqrt[5]{2}, \omega)$ . We have the following tower of fields:



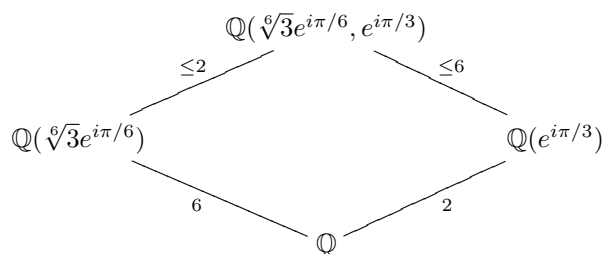
Where the numbers on the extensions denote either the degree or a bound on the degree. We know the bottom two degrees are what they are by a previous proposition or by Eisenstein. The others are bounded by that because we have a polynomial that is satisfied by the element we are adjoining. (I am not certain why the extensions also have to be at least that amount, perhaps the same trick from above applies as  $4 \nmid 5$  and  $5 \nmid 4$ .) So the degree of  $[\mathbb{Q}(\sqrt[5]{2}, \omega) : \mathbb{Q}] = 20$ .

**Example:** Find the splitting field and its degree of  $x^6 + 3$  over  $\mathbb{Q}$ .

*Solution:* Let  $z = re^{i\theta}$  be a root of  $x^6 + 3$ . Then  $r^6 e^{6i\theta} = -3 = 3e^{i\pi}$ . So  $r = \sqrt[6]{3}$  and  $6\theta = \pi + 2\pi k$  or  $\theta = \frac{\pi}{6} + \frac{\pi}{3}k$ . Therefore, we have that

$$\begin{aligned} z &= \sqrt[6]{3} e^{i(\frac{\pi}{6} + \frac{\pi}{3}k)} \\ &= \sqrt[6]{3} e^{i\frac{\pi}{6}} \cdot (e^{i\frac{\pi}{3}})^k \end{aligned}$$

Hence,  $L = \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6}, e^{i\pi/3})$ . Thus, we have the following tower of fields:



Where we know that  $[\mathbb{Q}(\sqrt[6]{3}e^{i\pi/6}) : \mathbb{Q}] = 6$  since  $x^6 + 3$  is irreducible by Eisenstein. Also, note that  $e^{i\pi/3} = e^{i\pi} = -1$ , so that it is a root of  $x^3 + 1 = (x+1)(x^2 - x + 1)$ . Therefore,  $e^{i\pi/3}$  is a root of  $x^2 - x + 1$  which is irreducible over  $\mathbb{Q}$ . Hence the question becomes is  $e^{i\pi/3}$  in  $\mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$ . First, note that

$$e^{i\pi/3} = \cos(\pi/3) + i \sin(\pi/3) = \frac{1}{2} + i \frac{\sqrt{3}}{2}$$

but,  $(\sqrt[6]{3}e^{i\pi/6})^3 = \sqrt{3}e^{i\pi/2} = i\sqrt{3} \in \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$ . Therefore we see that  $e^{i\pi/3} \in \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$ , hence  $L = \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$ , so that  $[L : \mathbb{Q}] = 6$ .

**Theorem:** Let  $F$  be a field and  $f(x) \in F[x]$  be a non-constant polynomial. Then there exists a splitting field for  $f(x)$  over  $F$ .

*Proof:* Induction on  $n$ , the degree of  $f$ . Let  $g(x)$  be an irreducible factor of  $f(x)$ . So