

1. Exercise 6.2 #1(b) Show that  $u = 1 + \sqrt{1 + \sqrt[3]{2}}$  is algebraic over  $\mathbb{Q}$ .

**Solution:** Begin with algebraic trickery.

$$\begin{aligned} u &= 1 + \sqrt{1 + \sqrt[3]{2}} \\ u - 1 &= \sqrt{1 + \sqrt[3]{2}} \\ (u - 1)^2 &= 1 + \sqrt[3]{2} \\ u^2 - 2u &= \sqrt[3]{2} \\ (u^2 - 2u)^3 &= 2 \\ u^6 + 6u^5 + 12u^4 + 8u^3 &= 2 \\ u^6 + 6u^5 + 12u^4 + 8u^3 - 2 &= 0 \end{aligned}$$

So we have found a polynomial  $f(x) = x^6 + 6x^5 + 12x^4 + 8x^3 - 2$  so that  $f(u) = 0$ .

2. Exercise 6.2 #7 Find the minimal polynomial of  $u = \sqrt{3} - i$  over  $\mathbb{Q}$  and also over  $\mathbb{R}$ .

**Solution:** Use the same strategy as above:

$$\begin{aligned} u &= \sqrt{3} - i \\ u^2 &= 3 - 1 - 2\sqrt{3}i \\ u^2 - 2 &= -2\sqrt{3}i \\ u^4 - 4u^2 + 4 &= -12 \\ u^4 - 4u^2 + 16 &= 0. \end{aligned}$$

3. Exercise 6.2 #20 Let  $\mathbb{K}$  be a field extension of  $\mathbb{E}$  which is a field extension of  $\mathbb{F}$ , and let  $[\mathbb{E} : \mathbb{F}]$  be finite. Let  $u \in \mathbb{K}$  be algebraic over  $\mathbb{E}$ .

- (a) Show that  $[\mathbb{E}(u) : \mathbb{E}] \leq [\mathbb{F}(u) : \mathbb{F}]$ .

**Solution:** Let  $\mathbb{K} \supseteq \mathbb{E} \supseteq \mathbb{F}$ , and  $[\mathbb{E} : \mathbb{F}] = n$  be finite. Then let  $u$  be algebraic over  $\mathbb{K}$  with minimal polynomial  $m(x) \in \mathbb{F}[x]$ . Now we proceed by cases. If  $m$  is irreducible in  $\mathbb{E}$ , then it remains the minimal polynomial for  $u$  in  $\mathbb{E}$ , and the degrees of the two extensions are equal. Now, if  $m$  is reducible in  $\mathbb{E}$ , then there exists  $f, g \in \mathbb{E}[x]$ , both with degree less than  $m$ , and  $m = fg$ . We take the one which has  $u$  as a root and repeat the process until we reach an irreducible polynomial  $h \in \mathbb{E}(u)$  with  $u$  as a root. If this is not monic, we factor out the leading coefficient, and we will have a  $h' \in \mathbb{E}(u)$  with  $h'(u) = 0$  that is monic and irreducible. This has degree strictly less than  $m$ , and is minimal for  $u$ .

After all this we have  $[\mathbb{E}(u) : \mathbb{E}] = \deg h' \leq \deg m = [\mathbb{F}(u) : \mathbb{F}]$ .

- (b) Show that  $[\mathbb{E}(u) : \mathbb{F}(u)] \leq [\mathbb{E} : \mathbb{F}]$ . (Hint: Theorem 6.1.6.) Take the same minimal polynomials we found above; and rewrite both:

$$\begin{aligned} [\mathbb{E}(u) : \mathbb{F}(u)] &= [\mathbb{E}(u) : \mathbb{E}][\mathbb{E} : \mathbb{F}(u)] \\ &= [\mathbb{E}(u) : \mathbb{E}] \frac{[\mathbb{E} : \mathbb{F}]}{[\mathbb{F}(u) : \mathbb{F}]} \\ &= \deg h' \frac{n}{\deg m}. \end{aligned}$$

Then since  $\deg h' \leq \deg m$ ,  $\frac{\deg h'}{\deg m} \leq 1$ . So then  $[\mathbb{E}(u) : \mathbb{F}(u)] = \frac{n \deg h'}{\deg m} \leq n = [\mathbb{E} : \mathbb{F}]$ .

4. Exercise 6.3 #4(a) and 4(b). Find the splitting field  $\mathbb{E}$  of  $f(x) = x^3 + 1$  over  $\mathbb{F} = \mathbb{Z}_2$  and factor  $f(x)$  completely in  $\mathbb{F}[x]$ . Then, do the same thing but replace  $\mathbb{F} = \mathbb{Z}_2$  with  $\mathbb{F} = \mathbb{Z}_3$  (see the statement in the textbook).

**Solution:** For  $\mathbb{Z}_2$ , we check the elements.  $f(0) = 0^3 + 1 = 1$ , and  $f(1) = 1^3 + 1 \equiv 0$ , so 1 is a root of the polynomial. Rewrite  $f(x) = (x + 1)(x^2 + x + 1)$ . Then let  $f'(x) = x^2 + x + 1$ , and check that this is also irreducible in  $\mathbb{Z}_2$ :

$$f'(0) = 0^2 + 0 + 1 = 1 \neq 0, \quad f'(1) = 1^2 + 1 + 1 = 1 \neq 0.$$

So this polynomial has no roots in  $\mathbb{Z}_2$  and therefore is irreducible. Let  $\alpha$  be such that  $f'(\alpha) = 0$ . Then there exists (By Kronecker's Theorem) a field extension of  $F$  in which  $\alpha$  is a root, and  $\alpha^2 + \alpha \equiv 1 \pmod{2}$ . So we can factor  $f'(x) = (x + \alpha)(x + \alpha + 1)$ . And so  $f(x) = (x + 1)(x + \alpha)(x + \alpha + 1)$ , so  $x$  splits over  $\mathbb{Z}_2(\alpha)$ . And since  $f'$  is monic and irreducible, it is the minimal polynomial for  $\alpha$ . Having degree 2, we can say that  $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 2$ , and since  $|\mathbb{Z}_2| = 2$ , by the multiplication theorem  $|\mathbb{Z}_2(\alpha)| = 4$ . Then we can finally say by the characterization of finite fields that  $\mathbb{Z}_2(\alpha) \cong \mathbb{F}_4$ .

Now, in  $\mathbb{Z}_3$  we can see that  $f(2) = 9 \equiv 0 \pmod{3}$ , so  $2 \equiv -1$  is a root of  $f$ . Rewrite,  $f(x) = (x + 1)(x^2 + 2x + 1) = (x + 1)^3$ . So the splitting field for  $f$  over  $\mathbb{Z}_3$  is  $\mathbb{Z}_3$ .

5. Exercise 6.3 #9 Let  $f(x)$  and  $g(x)$  be polynomials in  $F[x]$ . Show that  $f(x)$  and  $g(x)$  are relatively prime (have no common nonconstant factors) in  $F[x]$  if and only if they have no common root in any extension  $E$  of  $F$ .

**Solution:**

$\implies$  : Let  $f, g \in F[x]$  be coprime, and suppose for the sake of contradiction that they have a common root  $a$  in some extension  $E$  of  $F$ . Then  $f(x) = f'(x)(x - a)$  and  $g(x) = g'(x)(x - a)$ . Then  $x - a$  is a common nonconstant factor, a contradiction! Therefore  $f, g$  must have no common factor in  $F[x]$ .

$\impliedby$  : Suppose that  $f, g$  share no root in any  $E \supseteq F$ . Then suppose for the sake of contradiction that there exists some  $h \in F[x]$ , and  $g = g'h, f = f'h$ . This polynomial must have a root in some extension of  $F$ , say  $u \in K$ . Then  $g(u) = g'(u)h(u) = 0 = f'(u)h(u) = f(u)$ . So  $u$  is a root of both  $f, g$ , a contradiction. Then by contradiction  $f, g$  must be coprime.

6. Exercise 6.3 #17 If  $E$  over  $F$  is an algebraic extension and every polynomial in  $F[x]$  splits over  $E$ , show that  $E$  is algebraically closed. (Hint: Theorem 6.2.6)

**Solution:** Let  $E \supseteq F$  be an algebraic extension, where every polynomial in  $F[x]$  splits over  $E$ . Then suppose for the sake of contradiction that  $E$  is not algebraically closed. So there exists some  $f(x) \in E[x]$ , where  $f$  has degree greater than one, and is irreducible. Write  $f(x) = a_0 + a_1x + \dots + a_nx^n$ , with each  $a_i \in E$ . Take the field extension  $F(a_0, \dots, a_n) = F(a_0)(\dots)(a_n)$ . Since  $E$  is an algebraic extension, each  $a_i$  has a finite degree monic polynomial, each adjoined element on  $F$  produces another finite degree extension (Theorem 6.2.6). Since this extension is finite, it must be algebraic.