

1. Set  $E = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$  and  $F = \mathbb{Q}(\sqrt{-3})$ . Clearly,  $E$  is a field extension of  $F$ .

(a) Find a basis for  $E$  viewed as a vector space over  $F$ .

Note that  $\deg(\sqrt{-3}, \mathbb{Q}) = 2$ , because  $\sqrt{-3}$  is a root of the quadratic polynomial  $x^2 + 3$ , which is irreducible over  $\mathbb{Q}$  (since  $\sqrt{-3} \notin \mathbb{Q}$ ). Therefore,  $[F : \mathbb{Q}] = 2$ . Similarly,  $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$ . This implies that  $[E : F] = [E : \mathbb{Q}] / [F : \mathbb{Q}] = 2$ , so the basis must have two elements.

To find the basis, it suffices to take any two elements of  $E$  that are linearly independent over  $F$  (that is, one of them is not a multiple of the other). For instance, take 1 and any  $\alpha \in E \setminus F$ ; two simplest bases are  $\{1, \sqrt{-1}\}$ , and  $\{1, \sqrt{3}\}$ .

(b) Find  $\alpha$  such that  $E = F(\alpha)$ .

We know that  $[E : F] = 2$ , so we need  $\alpha \in E$  that has degree 2 over  $F$ . Any  $\alpha \in E \setminus F$  works:  $E = F(\sqrt{3}) = F(\sqrt{-1})$ .

2. (a) Suppose  $a \in \overline{\mathbb{Z}_3}$  satisfies  $a^2 + 1 = 0$  (as usual,  $\overline{\mathbb{Z}_3}$  is an algebraic closure of  $\mathbb{Z}_3$ ). Find  $\deg(a, \mathbb{Z}_3)$ .

Since  $a$  is a root of a quadratic polynomial ( $x^2 + 1$ ), its degree is at most 2. Notice that  $x^2 + 1$  is irreducible over  $\mathbb{Z}_3$ , because it has no roots ( $0^2 + 1 = 1$ ,  $1^2 + 1 = 2^2 + 1 = 2$ ). Therefore,  $\deg(a, \mathbb{Z}_3) = 2$ .

(b) Find  $\deg(a, GF(3^3))$ , where  $GF(3^3) \subset \overline{\mathbb{Z}_3}$  is the finite field with  $3^3$  elements. Justify your answer.

By the same argument,  $\deg(a, GF(3^3)) \leq 2$ . Note that  $\deg(a, GF(3^3)) = 1$  if and only if  $a \in GF(3^3)$ . However,  $[GF(3^3) : \mathbb{Z}_3] = 3$ , so degrees of all elements of  $GF(3^3)$  (over  $\mathbb{Z}_3$ ) must divide 3. This implies  $a \notin GF(3^3)$  (as 2 does not divide 3), and so  $\deg(a, GF(3^3)) = 2$ .

3. Suppose  $F$  is a field, and suppose  $E_1 \supset F$ ,  $E_2 \supset F$  are two field extensions whose degrees  $[E_1 : F]$ ,  $[E_2 : F]$  are relatively prime. Prove that  $E_1 \cap E_2 = F$ .

Clearly  $E_1 \cap E_2 \supseteq F$ , so it suffices to check that if  $a \in E_1 \cap E_2$ , then  $a \in F$ . But then  $\deg(a, F)$  divides both  $[E_1 : F]$  and  $[E_2 : F]$ , and so  $\deg(a, F) = 1$ , because  $[E_1 : F]$  and  $[E_2 : F]$  are relatively prime. This means  $a \in F$ , as expected.

4. For a prime number  $p$ , define the polynomial  $Q(x)$  over the field  $\mathbb{Z}_p$  by

$$Q(x) = 1 + x^{p-1} + x^{2(p-1)} + x^{3(p-1)} + \cdots + x^{p(p-1)} \in \mathbb{Z}_p[x].$$

Show that any irreducible factor of  $Q(x)$  has degree 2. (Hint:  $Q(x) = \frac{x^{p^2} - x}{x^p - x}$ .)

Let  $P(x)$  be an irreducible factor of  $Q(x)$ . It has a root in  $\overline{\mathbb{Z}_p}$ ; let us denote it by  $a \in \overline{\mathbb{Z}_p}$ . Note that  $Q(a) = 0$ . Then  $P(x)$  is the minimal polynomial of  $a$  over  $\mathbb{Z}_p$ ; so we need to verify that  $\deg(a, \mathbb{Z}_p) = 2$  whenever  $a \in \overline{\mathbb{Z}_p}$ ,  $Q(a) = 0$ .

Let us now use the formula  $Q(x) = \frac{x^{p^2} - x}{x^p - x}$ . The roots of the numerator in  $\overline{\mathbb{Z}_p}$  are exactly the elements of  $GF(p^2)$ ; moreover, all roots are simple. The roots of the

denominator are elements of  $GF(p) = \mathbb{Z}_p$ , so  $Q(a) = 0$  if and only if  $a \in GF(p^2)$ ,  $a \notin \mathbb{Z}_p$ . We also know that  $[GF(p^2) : \mathbb{Z}_p] = 2$ ; this implies  $\deg(a, \mathbb{Z}_p) = 2$ .

5. Let  $\overline{F}$  be an algebraic closure of a field  $F$ . For a polynomial  $p(x) \in F[x]$ , denote by  $\alpha_1, \dots, \alpha_n \in \overline{F}$  its roots in  $\overline{F}$ ; here  $n = \deg(p)$ . Set  $E = F(\alpha_1, \dots, \alpha_n)$ . Prove that

$$[E : F] \leq n! = n \cdot (n-1) \cdots 2 \cdot 1.$$

(For partial credit, prove the weaker estimate  $[E : F] \leq n^n$ .)

Let us first prove the weaker estimate. Clearly,

$$\begin{aligned} [E : F] &= [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \cdot [F(\alpha_1, \dots, \alpha_{n-1}) : F(\alpha_1, \dots, \alpha_{n-2})] \cdots [F(\alpha_1) : F] \\ &= \deg(\alpha_n, F(\alpha_1, \dots, \alpha_{n-1})) \cdot \deg(\alpha_{n-1}, F(\alpha_1, \dots, \alpha_{n-2})) \cdots \deg(\alpha_1, F). \end{aligned}$$

Note that  $\alpha_i$  is a root of  $p \in F[x]$ , but we can also view  $p$  as a polynomial over  $F(\alpha_1, \dots, \alpha_{i-1})$ . It is then clear that  $\deg(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1})) \leq n$  (the equality is achieved if  $p(x)$  is irreducible). This implies the estimate.

To prove that  $[E : F] \leq n!$ , we notice that  $p(x)$  is reducible over  $F(\alpha_1, \dots, \alpha_{i-1})$  (even if it is irreducible over  $F$ ), because it has  $i-1$  roots, namely  $\alpha_1, \dots, \alpha_{i-1}$ , in this field. We can therefore write

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_{i-1})q(x),$$

where  $q(x)$  is a polynomial over  $F(\alpha_1, \dots, \alpha_{i-1})$  of degree  $n - (i-1)$ . Then  $\alpha_i$  is a root of  $q(x)$ , so  $\deg(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1})) \leq n - (i-1)$ . This gives the required estimate.