

1. Any field isomorphism must fix the base field, in this case  $\mathbb{Q}$ , so that  $\sqrt{2} \mapsto a + b\sqrt{3}$ ,  $b \neq 0$  is necessitated by injectivity. If  $\tau$  is such a map, then

$$2 = \tau(2) = \tau(\sqrt{2})\tau(\sqrt{2}) = (a + b\sqrt{3})^2 = 3b^2 + 2ab\sqrt{3} + a^2$$

since  $\sqrt{3}$  is linearly independent of 1 and  $b \neq 0$  we must have  $a = 0$ , hence  $2/3 = b^2$ . We may write  $b = s/t$ ,  $s, t \in \mathbb{Z}$  coprime, equivalently  $2t^2 = 3s^2$ , so  $2|s^2$  implies  $2|s$ , so that  $4|2t^2$ , implies  $2|t^2$  implies  $2|t$ , contradicting  $s, t$  being coprime.

Finite dimensional vector spaces are isomorphic when they have the same dimension,  $\sqrt{2}$  and 1 are linearly independent in a  $\mathbb{Q}$  vector space since  $\sqrt{2}$  is irrational (similarly  $\sqrt{3}$  and 1 are linearly independent). To see that  $(1, \sqrt{2})$  and  $(1, \sqrt{3})$  are bases respectively, we use algebraicity of  $\sqrt{2}$ ,  $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}/(x^2 - 2)$ , so by polynomial long division any element can be written as  $ax + b \mapsto a\sqrt{2} + b$ , for  $a, b \in \mathbb{Q}$ , hence this is a basis, and the argument is the same for  $\mathbb{Q}(\sqrt{3})$ .

2. To see that  $K/L$  is algebraic, it will suffice to show that  $t$  is algebraic over  $L$  (hence all elements, due to sums products and inverses preserving algebraicity). Consider the polynomial  $g(x)u - f(x)$  in  $L[x]$ , evaluating at  $t$  gives

$$g(t)u - f(t) = g(t)\frac{f(t)}{g(t)} - f(t) = f(t) - f(t) = 0$$

Hence  $t$  is algebraic over  $L$ , implying that  $K$  is algebraic over  $L$ . If  $L/F$  were algebraic, then by transitivity  $K/F$  would be algebraic but  $t \in K$  is transcendental over  $F$ , so by contrapositive  $L/F$  is algebraic. Now we prove that  $[K : L] = \max(\deg(f), \deg(g))$ , it will suffice to show  $\min(t, L) = g(x)u - f(x)$ , i.e. that this polynomial is irreducible. We can apply Gauss' lemma, so that it will suffice to show  $g(x)u - f(x) \in F[u][x]$  is irreducible. So write  $p(u, x)q(u, x) = g(x)u - f(x)$ , one of  $p, q$  has degree one in  $u$  so assume its  $q$  (hence  $\deg_u(p) = 0$ ), then  $q(u, x) = uh(x) + r(x)$ . It follows that  $uh(x)p(x) + r(x)p(x) = 1$ , hence  $p(x)|f(x), g(x)$ , implying  $p(x) = 1$ .

3. Let  $u, v \in K$ ,  $r, s \in F$ , then since multiplication is distributive and commutative in a field,

$$L_\alpha(ru + sv) = \alpha(ru + sv) = \alpha ru + \alpha sv = r\alpha u + s\alpha v = rL_\alpha(u) + sL_\alpha(v)$$

Since  $K$  is finite it is algebraic. Let  $m(a) := \min(\alpha, F) = c_n x^n + \dots + c_0$ , then  $1, a, \dots, a^{n-1}$  are a basis for  $K$  as a  $F$ -vectorspace. It follows that  $L_a : a^k \mapsto a^{k+1}$ ,  $0 \leq k \leq n-2$ , and  $a^{n-1} \xrightarrow{L_a} a^n = -c_{n-1}a^{n-1} - \dots - c_0$ . Writing  $L_a$  in our  $a^k$  basis,

$$L_a = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{bmatrix}$$

Now assume for induction that  $\det(L_{a_{k \times k}} - I_{k \times k} x) = x^k + x^{k-1}c_{n-1} + \dots + c_{n-k}$  (referring to the lower right  $k \times k$  submatrix). This is clear for  $k = 1$ , then

$$\begin{aligned} \det(L_{a_{k+1 \times k+1}} - I_{k+1 \times k+1} x) &= x \det(L_{a_{k \times k}} - I_{k \times k} x) + (-1)^{k+1} c_{n-k-1} \det(-I_{k+1 \times k+1}) \\ &= x^{k+1} + x^k c_{n-1} + \dots + x c_{n-k} + c_{n-k-1} \end{aligned}$$

The only elements having  $\det(Ix - L_\alpha) = \min(\alpha, F)$  are  $\alpha$  such that  $F(a) = F(\alpha)$  i.e.  $\deg(\min(\alpha, F)) = [F(a) : F]$ , the above proves  $\det(Ix - L_\alpha) = \min(\alpha, F)$  when  $F(\alpha) = F(a)$  (just write  $L_\alpha$  in  $\alpha^k$  basis). For the converse notice that  $\deg \det(Ix - L_\alpha) = [F(a) : F]$ , so the degree is too large to be the minimum polynomial of  $\alpha$  with minimum polynomial of smaller degree.

4. We have the tower of extensions  $F(a)/F(a^2)/F$ , since  $a$  satisfies  $x^2 - a^2$  in  $F(a^2)[x]$ , it is either in  $F(a^2)$ , or is algebraic of degree 2. Assume the latter, then by multiplicativity of degree,  $F(a)/F$  is even, hence by contrapositive  $a \in F(a^2)$ .

5. It will suffice to show  $R$  has no non-trivial proper ideals, first note  $R$  is a domain, since  $K$  does not have 0 divisors and  $R \subset K$ . Consider an ideal  $0 \neq I \subset R$ , if  $I \cap F \neq 0$ , then  $1 \in I = R$ , since any non-zero element of  $F$  is invertible, so that  $k \in I \cap F$  implies that  $1 \in kk^{-1} \in IF \subset IR = I$ . Otherwise if  $I \cap F = 0$ , then for some  $\alpha \in K \setminus F$ , we have  $\alpha \in I$ ,  $\alpha$  is algebraic, so has a minimum polynomial in  $F$ ,  $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ,  $a_0 \neq 0$ . It follows that  $-a_0^{-1}(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) = 1 \in I = R$ .

To show that  $a_0 \neq 0$ , assume it were, then take the smallest  $k$ , such that  $a_k \neq 0$ . It follows that  $\alpha^k(\alpha^{n-k} + a_{n-1}\alpha^{n-k-1} + \cdots + a_k) = 0$ , hence  $R$  is a domain implies that  $\alpha^k = 0$  or  $(\alpha^{n-k} + a_{n-1}\alpha^{n-k-1} + \cdots + a_k) = 0$ , contradicting  $\min(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$