1) Recall that a field F is an integral domain where each non-zero element is a unit. If we denote 1_F as the multiplicative identity of F, then we denote the additive group order of 1_F as $\operatorname{ch} F$.

Example 0.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are fields with infinite characteristic.*

Example 0.2. *Given prime p, $\mathbb{Z}_p$ is a field with characteristic p. We denote it F_p.*

We can naturally view F as a ring, and thus obtain a ring morphism $\varphi : \mathbb{Z} \to F$ with $n \mapsto n(1_F)$.

Proposition 0.3. *If $\operatorname{ch} F < \infty$, then $\ker \varphi = (\operatorname{ch} F)\mathbb{Z}$.*

Proof. If $n \in \ker \varphi$ then $n(1_F) = 0$. Since $\operatorname{ch} F$ is defined as the additive group order of 1_F, it must divide n so $n \in (\operatorname{ch} F)\mathbb{Z}$. The other inclusion is obvious. ■

Corollary 0.3.1. *If $\operatorname{ch} F < \infty$, then $\operatorname{ch} F$ is prime.*

Proof. Note that φ is surjective, so $\mathbb{Z}/(\operatorname{ch} F)\mathbb{Z} \cong \varphi(\mathbb{Z})$, where $\varphi(\mathbb{Z})$ is a subfield of F. This means $\mathbb{Z}/(\operatorname{ch} F)\mathbb{Z}$ is a field, and so $(\operatorname{ch} F)\mathbb{Z}$ must be a prime ideal of $\mathbb{Z}$. This means $\operatorname{ch} F$ is prime. ■

Corollary 0.3.2. *If F is a finite field then $F = p^n$ for some prime p and $n \in \mathbb{N}$.*

Proof. Clearly $\operatorname{ch} F < \infty$, and F is a vector space over $\mathbb{Z}/(\operatorname{ch} F)\mathbb{Z}$ (a field since $\operatorname{ch} F$ is prime). Since F is finite, it must also be finite-dimensional, so if its dimension is n then $|F| = (\operatorname{ch} F)^n$. ■

2) If K is a field containing F, then K/F is a field extension. Note that K is a vector space over F, so we define the degree of K, F, denoted $[K : F]$, as the dimension of K as a vector space over F.

Example 0.4. $\mathbb{R}$ *is a field which (under embedding) is a subfield of* $\mathbb{C}$*, so* $\mathbb{C}/\mathbb{R}$ *is a field extension. Note that* $\mathbb{C}$ *is a 2-dimensional real vector space, so the degree* $[\mathbb{C} : \mathbb{R}]$ *is 2.*

Example 0.5. $\mathbb{Q}$ *is a field which (under embedding) is a subfield of* $\mathbb{Q}(\sqrt{2})$*, so* $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *is a field extension. Note that* $\mathbb{Q}(\sqrt{2})$ *is a 2-dimensional* $\mathbb{Q}$ *vector space (it is spanned by* $(1,0)$ *and* $(0,1)$*), so the degree* $[\mathbb{Q}(\sqrt{2}), \mathbb{Q}]$ *is 2.*

Example 0.6. *Given prime p, F_p is a field, and F_{p^n} is a field containing F_p. It is a n-dimensional vector space over F_p, thus the degree $[F_{p^n} : F_p]$ is n.*

Given two field extensions K/F and H/K, what is the degree of H/F? There is a simple formula.

Proposition 0.7. $[H : F] = [H : K][K : F]$.

Proof. If we let $[H : K] = n$, then by definition we can choose elements $h_1, ..., h_n$ that are K-linear independent and whose K-span equals H. Letting $[K : F] = m$, we can also choose $k_1, ..., k_m$ that are F-linear independent and whose F-span equals K. So if we consider the list $h_1k_1, ..., h_nk_m$, we claim that this is a F-linear independent list whose F-span equals H. For convenience denote $f_{i,j} = h_ik_j$.

- Suppose $\sum_{i,j} a_{i,j} f_{i,j} = 0$ for some scalars $a_{i,j} \in F$. Then $\sum_{i=1}^{n}(\sum_{j=1}^{m} a_{i,j}k_j)h_i = 0$. Since $a_{i,j}k_j \in K$, by K-linear independence we have $\sum_{j=1}^{m} a_{i,j}k_j = 0$ for each $1 \le i \le n$. For a fixed $1 \le i \le n$, using F-linear independence we have $a_{i,j}$ for all $1 \le j \le m$. So we have shown F-linear independence.

- Given $h \in H$, by the K-span property choose $a_1, ..., a_n \in K$ such that $\sum_{i=1}^{n} a_i h_i = h$. For a fixed $1 \leq i \leq n$, by the F-span property, choose $b_{i,1}, ..., b_{i,m} \in F$ such that $a_i = \sum_{j=1}^{m} b_{i,j} k_j$. Then $h = \sum_{i=1}^{n} (\sum_{j=1}^{m} b_{i,j} k_j) h_i$, and this summation can be simplied.

As required. ■

3) Note that not every polynomial $p \in F[x]$ has roots in F. However, we've seen that we could "create" fields to force the existence of polynomials, like $\mathbb{R}$ for $\mathbb{Q}$, and $\mathbb{C}$ for $\mathbb{R}$. So the question is, given a $p \in F[x]$, does there exist a field K containing an embedded copy of F where p has a root in K?

Proposition 0.8. *There exists such a field K.*

Proof. We can assume that p is irreducible in $F[x]$, because else it would have a zero in F (and the proposition would be trivial!). By irreducibility, (p) is a maximal ideal (Note $F[x]$ is a UFD), so $K = F[x]/(p)$ is a field. We can embed F into K via $f \to \overline{f}$. If we let $\theta \in F[x]$ be quotient of the identity polynomial in K, then clearly $p(\theta) = 0$. ■

Having such a K as defined in the proof, we investigate its field extension degree (Note that K is naturally a field over F).

Proposition 0.9. *If $n = \deg p$, then $1, \theta, ..., \theta^{n-1}$ forms a F-basis for $F[x]/(p)$.*

Proof. Linear independence is clear. Span is also clear, because for any polynomial $q \in F[x]$ we can use long division to obtain $q = sp + r$ where $\deg r < n$. ■

Corollary 0.9.1. $[F[x]/(p) : F] = \deg p$.

To make this construction more concrete, here are some examples.

Example 0.10. $\mathbb{R}$ *and* $x^2 + 1 \in \mathbb{R}[x]$.

We define $K = \mathbb{R}[x]/(x^2+1)$ and embed $\mathbb{R}$ into it with $r \mapsto \overline{r}$. Letting $\theta \in K$ be defined as the quotient of the identity polynomial, we have $\theta^2 + 1 = 0$, and we have $K = \{a + b\theta : a, b \in \mathbb{R}\}$. Addition is obvious, and multiplication is:

$$\begin{aligned}(a + b\theta)(c + d\theta) &= ac + (ad + bc)\theta + bd\theta^2 \\ &= (ac - bd) + (ad + bc)\theta\end{aligned}$$

This clearly shows us that K is isomorphic to $\mathbb{C}$.

Example 0.11. $\mathbb{Q}$ *and* $x^3 + 2 \in \mathbb{Q}[x]$.

We define $K = \mathbb{Q}[x]/(x^3 + 2)$ and embed $\mathbb{Q}$ into it. Letting $\theta \in K$ be defined as the quotient of the identity polynomial, we have $\theta^3 + 2 = 0$, and $K = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{R}\}$. By cumbersome multiplication we see that it is isomorphic to $\mathbb{Q}(\sqrt[3]{2})$.

The above has shown the *existence* of a field extension where we can solve polynomials, but is there some kind of uniqueness?

Given a field extension K/F and a $a \in K$, we let $F(a)$ be the smallest subfield of K containing F and a, and call it the field generated by a. Here is the uniqueness statement we are looking for:

Proposition 0.12. *Given $p \in F[x]$ and a root $a \in K$ where K/F is a field extension, we have $F[x]/(p) \cong F(a)$.*

Proof. We can define the field morphism $\varphi : F[x]/(p) \to F(a)$ by defining $\varphi(f) = f$ for $f \in F$, $\varphi(\theta) = a$, and then extending φ to a field morphism. We have injectivity, because $\ker \varphi$ is an ideal of $F[x]/(p)$, and thus is either trivial or $F[x]/(p)$, with the latter being clearly impossible. We have surjectivity, because the image of F is a field containing F and a (we use the minimal property of $F(a)$). ■

Corollary 0.12.1. *$F[x]/(p)$ is the smallest field containing F for which p has a zero in.*

Proof. If K is a field containing F for which p has a zero $a \in K$, then K contains $F(a)$ which is isomorphic to $F[x]/(p)$. ■

Corollary 0.12.2. *$F(a)$ is the F-span of $1, a, ..., a^{n-1}$.*

Proof. In the ring isomorphism mentioned, 1 maps to 1 and θ maps to a. ■

4) Given a field extension K/F, $a \in K$ is algebraic in F if it is a zero of a polynomial in $F[x]$, and transcendental in F otherwise. If every $a \in K$ is algebraic in F, then the field extension K/F is transcendental.

Proposition 0.13. *For every $a \in K$ algebraic in F, there exists a unique monic $p \in F[x]$ of minimal degree for which a is a zero.*

Proof. Choosing a monic $p \in F[x]$ of minimal degree for which $p(a) = 0$, we show that p is irreducible. If $p = qr$, then $p(a) = 0$ implies either $q(a) = 0$ or $r(a) = 0$. If $q(a) = 0$ for example, then we can multiply q, r by non-zero elements to ensure that q is monic, and then by minimal property we have $p = q$, showing irreducibility.

To show uniqueness, suppose we have a monic $q \in F[x]$ of minimal degree for which a is zero. We then have $\deg p = \deg q$. Using long division we have $q = pr + s$ for some $s \in F[x]$ with $\deg s < \deg p$. Since $p(a) = r(a) = 0$, we have $s(a) = 0$. We then must have $s = 0$. (since otherwise we can scalar multiply s to make it monic, contradicting minimal property). Since p, q are both monic, we have $r = 1$ so $p = q$. ■

The above polynomial in $F[x]$ is denoted $m_{a,F}$, and the degree of $m_{a,F}$ is called the degree of a. Noting that there were lots of conditions on $m_{a,F}$ that we imposed, here is a simplification:

Corollary 0.13.1. *If $a \in K$ is a zero of $p \in F[x]$, then $p = m_{a,F}$ iff p is monic and irreducible.*

Proof. If $p = m_{a,F}$ then we know p is monic and irreducible. If p is monic and irreducible, then we want to show that $p = m_{a,F}$. Since $m_{a,F}$ has minimal degree, we have $\deg p \geq \deg m_{a,F}$. By long division we have $p = m_{a,F}q + s$ for some $s \in F[x]$ with $\deg s < \deg m_{a,F}$. Since $s(a) = 0$, similar to the above proof we must have $s = 0$, so $p = m_{a,F}q$. Since p is irreducible, q must be a unit in F. But $p, m_{a,F}$ are both monic so $p = 1$ thus $p = m_{a,F}$. ■

Corollary 0.13.2. *If $a \in K$ and $p \in F[x]$, then $p(a) = 0$ iff $m_{a,F}$ divides p.*

Proof. Decompose p into irreducibles (we can assume monic). One must have a as a zero. ■

Noting that $m_{A,F}$ is irreducible, this aligns with our discussion of extending fields to solving irreducible polynomials, so we naturally obtain the following results:

Corollary 0.13.3. *$F(a) \cong F[x]/(m_{a,F})$.*

Recall that $F(a_1, a_2, ...)$ is the field generated by $a_1, a_2, ... \in K$. The above Corollaries give us a convenient way of calculating a simple extension, but how about an extension from multiple elements? The following proposition tells us that this is no different from repeated simple extensions.

Proposition 0.14. *$F(a, b) = (F(a))(b) = (F(b))(a)$.*

Proof. It suffices to show $F(a, b) = (F(a))(b)$. Note that $(F(a))(b)$ contains F, a, b, so $F(a, b) \supset (F(a))(b)$. Next note that $F(a, b)$ is a subfield of K containing $F(a), b$, so $F(a, b) \subset (F(a))(b)$. ■

Clearly, we can generalize this argument to extensions over any amount of elements. We can now classify when an element is Algebraic, and in general when a field extension is Algebraic:

Proposition 0.15. *$a \in K$ is Algebraic over F iff the simple extension $F(a)/F$ has finite degree.*

Proof. If a is Algebraic over F, then $F(a) \cong F[x]/(m_{a,F})$ implies that $F(a)$ is the F-span of $1, a, ..., a^{n-1}$ where $n = \deg m_{a,F}$, and so $[F(a) : F] = n$. Conversely, if $[F(a) : F]$ is finite (say equals n) then $F(a)$ is a finite dimensional vector space over F. Therefore, the $n + 1$ elements $1, a, ..., a^n \in F(a)$ must be F-linear dependent, and thus we can choose $\lambda_0, ..., \lambda_n \in F$ such that

$$\lambda_0 + \lambda_1 a + \cdots + \lambda_n a^n = 0$$

Which shows that a is Algebraic over F. ■

Corollary 0.15.1. *If $[K : F]$ is finite, then K/F is Algebraic over F.*

Proof. Given any $a \in K$, $[K : F] < \infty$ means that $F(a)$, as a F-vector subspace of K, must also be a finite-dimensional F-vector space, where $[F(a) : F]$ divides $[K : F]$. So by the proposition, a is Algebraic over F. ■

The above result gives us some insight about Algebraic numbers. Here is a characterization of finite extensions.

Proposition 0.16. *$[K : F]$ is finite iff K is finitely generated by Algebraic elements over F.*

Proof. If $K = F(a_1, ..., a_n)$ where $a_1, ..., a_n$ are Algebraic over F, then $[K : F]$ must be finite because $F(a_1, ..., a_n)$ can be decomposed into simple extensions (By Proposition 0.14) and we can iterate the tower law to multiple a finite number of finite degrees (Degrees are finite because of Algebraic-ness). $[K : F]$ being finite implies that K/F is Algebraic.

If $[K : F]$ is finite, then K/F is Algebraic over F. Letting $[K : F] = n$, we choose a basis $a_1, ..., a_n$ of K as a F-vector space. It follows that $K = F(a_1, ..., a_n)$, and each $a_1, ..., a_n$ are Algebraic over F as we previously deduced. ■

Corollary 0.16.1. *If $a, b \in K$ are algebraic over F, then so are $a + b$, $a - b$, ab, ab^{-1}.*

Proof. We have $a \in F(a)$ and $b \in F(b)$, so $a, b \in F(a, b)$, where $[F(a, b) : F]$ is finite by the tower law (note that $a, b \in K$ are algebraic over F). If we let c be the result of an operation on a, b (like $a + b$ or ab), then we still have $c \in F(a, b)$. Then c is Algebraic over F because $[F(a, b) : F]$ is finite (Use a linear dependence argument, similar to a proof above). ■

5) In this section, we will apply the aforementioned theory to prove some impossibility theorems regarding Constructibility (Which Ancient Mathematicians considered with rulers and compasses). We will first consider a quadratic extension:

Proposition 0.17. *If K/F is a field extension where $\operatorname{ch} F \neq 2$, then $[K : F] = 2$ iff $K = F(a)$ for some $a \in K - F$ with $a^2 \in F$ (we then denote $a = \sqrt{D}$ and write $K = F(\sqrt{D})$).*

Proof. If $[K : F] = 2$ then choose a $c \in K - F$. Since $[K : F]$ is finite, K/F is Algebraic over F so we can consider the minimal polynomial $m_{c,F}$. Since $c \notin F$, the degree $m_{c,F}$ cannot be 1 and must be 2. Therefore $F \leq F(c) \leq K$ where $[F(c) : F] = 2$, and so $K = F(c)$. Writing $m_{c,F}(x) = x^2 + \lambda_1 x + \lambda_2$, by elementary algebra $m_{c,F}(c) = 0$ implies

$$(2c + \lambda_1)^2 = \lambda_1^2 - 4\lambda_2$$

So letting $a = 2c + \lambda_1$, we have $a^2 = \lambda_1^2 - 4\lambda_2 \in F$, but $a \in K - F$ because $a \in F$ would imply $2c = a - \lambda_1 \in F$, a contradiction. We clearly have $F(a) = F(c)$, because any subfield of K containing F, c must contain a because $a = 2c + \lambda_1$, and vice versa. Therefore $K = F(a) = F(c)$, and we denote $D = \lambda_1^2 - 4\lambda_2$ "The discriminant of $m_{c,F}$" and $a = \sqrt{D}$, so that $K = F(\sqrt{D})$.

Conversely, if $K = F(a)$ for some $a \in K - F$ with $a^2 \in F$, then a is a zero of the polynomial $x^2 - a^2 \in F[x]$. Since $a \notin F$ the degree of $m_{a,F}$ cannot be 1, so $m_{a,F}(x) = x^2 - a^2$. It follows that $[K : F] = [F(a) : F] = \deg m_{a,F} = 2$. ■

In the above, we call a 2-degree field extension a "Quadratic extension". Now for constructable numbers:

Definition 0.18. *$a \in \mathbb{R}$ is said to be constructable if there exists $r_1, ..., r_n \in \mathbb{R}$ such that $a = r_n$ and for each $1 \leq k \leq n$, r_k is obtained by Addition/Subtraction/Multiplication/Division/Square-Root in $\mathbb{Q}(r_1, ..., r_{k-1})$.*

We then have the immediate proposition:

Proposition 0.19. *If $a \in \mathbb{R}$ is constructable, then $[\mathbb{Q}(a) : \mathbb{Q}]$ is a (finite) power of 2.*

Proof. Suppose we have such a sequence $r_1, ..., r_n$ where $a = r_n$. Then clearly $[\mathbb{Q}(r_1) : \mathbb{Q}] \in \{1, 2\}$, because Adding/Subtracting/Multiplying/Dividing keeps r_1 in $\mathbb{Q}$, while taking a square root yields at worst a Quadratic Extension. By the same argument, we have $[\mathbb{Q}(r_1, r_2) : \mathbb{Q}(r_1)] \in \{1, 2\}$, while noting $\mathbb{Q}(r_1, r_2) = \mathbb{Q}(r_2)$. Again we have $[\mathbb{Q}(r_1, r_2, r_3) : \mathbb{Q}(r_1, r_2)] \in \{1, 2\}$, while noting $\mathbb{Q}(r_3) = \mathbb{Q}(r_3, r_2) = \mathbb{Q}(r_3, r_2, r_1)$. So the proof is a consequence of the tower law iterated. ■

Corollary 0.19.1. *$\sqrt[3]{2}$ is not constructable, so a cube's volume cannot be doubled (i.e. length 1).*

Proof. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. ■

Corollary 0.19.2. *π is not constructable, so a circle's area cannot be squared (i.e. radius 1).*

Proof. $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ because π is a transcendental number. ■

Corollary 0.19.3. $\cos(\frac{\pi}{9})$ *is not constructable, so an angle cannot be trisected (i.e. $\frac{\pi}{3}$).*

Proof. Suppose $\beta = \cos(\frac{\pi}{9})$ was constructable. The triple angle formula states $\cos \frac{\pi}{3} = 4\beta^3 - 3\beta$, which simplies to $8\beta^3 - 6\beta - 1 = 0$. Letting $\alpha = 2\beta$ (which is constructable by assumption), we then have $\alpha^3 - 2\alpha - 1 = 0$, so $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, contradicting the fact that α is constructable. ■