Lemma 1. If R is finite and $a \in R$ is not a zero divisor, then a is a unit.

Proof. Since R is finite, the sequence $1, a, a^2...$ must repeat. So we get $m \neq n$ such that $a^m = a^n$.

We reorganize to get $a^m - a^n = 0$, where we assume $m > n$. Then $0 = a^m - a^n = (a^{m-n} - 1)a^n$, and so as a is not a zero divisor, we must have that... □

Lemma (Quotient Integral Domain). Let R be a commutative ring, and I an ideal. Then R/I is an integral domain if I is prime, i.e. for $a, b \in R$ where $ab \in I$, then either $a \in I$ or $b \in I$.

Lemma (Quotient Field). Let R be a ring and $I \neq R$ an ideal. Then R/I is a field if and only if I is maximal, i.e. there is no ideal $J \neq I$ such that:

$$I \subset J \subset R$$

Theorem (Polynomial Division Algorithm). Let R be a commutative ring, $f, g \in R[x]$ with the leading coefficient of g a unit in R. Then there exists unique polynomials $q, r \in R[x]$ such that:

$$f = gq + r \text{ and } \deg(r) < \deg(g)$$

Proof. (i) *(Existence)* First, if $\deg f < \deg g$, we can take $q = 0$ and $r = f$.

Suppose then that $\deg f \geq \deg g$. Let $n = \deg f, m = \deg g$. We express f, g as the following:

$$f = \sum_{i=0}^{n} a_i x^i,\ g = \sum_{i=0}^{m} b_i x^i$$

By assumption, b_m is a unit. Consider then the polynomial $f_2 = f - g a_n b_m^{-1} x^{n-m}$. Then, by construction, we have $\deg f_2 < \deg f$. It's either then that $\deg f_n < \deg g$ or $\deg(f_2) \geq \deg g$. Let $\deg f_2 = n_2$, c_2 the leading coefficient of f_2, then consider $f_3 = f_2 -$ □

Theorem :). Let R be a commutative ring. Let $g \in R[x]$ have leading coeff. a unit, and let $I = (g)$ be the principal ideal generated by g. Then every element of $R[x]/I$ has a unique representative with degree strictly less than the degree of g.

Definition (Monic Polynomial). A polynomial is monic if it has leading coefficient 1.

Definition :). Let F be a field. Then the greatest common divisor of two polynomials is the highest degree monic polynomial that divides both f and g.

Theorem :). Let F be a field. Let $f, g \in F[x]$ and suppose that a t least one is non-zero, i.e. g. Then $\gcd(f, g)$ exists. Moreover, there exists $A, B \in F[x]$ such that $\gcd(f, g) = Af + Bg$.

Theorem :). Let F be a field, and let $I \subseteq F[x]$ an ideal. If $f, g \in I$, then $\gcd(f, g) \in I$.

Proof. By the Euclidean algorithm. □

Theorem :). Let F be field, and let I be an ideal of $F[x]$. Then I is principal.

Proof. Descent on gcds □

Theorem :). Let R be a commutative ring. Then a nonzero element $f \in R[x]$ is irreducible if f cannot be expressed as a product of polynomials with strictly lesser degrees.

Theorem :). Let F be a field, and let $f \in F[x]$ be a non-constant polynomial. Then $F[x]/(f)$ is a field if and only if f is irreducible.

Theorem :). For F a field"
Every ideal in $F[x]$ is principal.

(b) ${}^{F[x]}/_{(f)}$ is a field if and only if f is irreducible.

(c) Every element of ${}^{F[x]}/_{(f)}$ has a unique representation with degree less than degree of f.

(d) Inverses are found by Euclidean algorithm.

We can kinda think of ${}^{\mathbb{Q}}/_{(f)}$ as $\{a + b\alpha + c\alpha^2\}$ for some scalars in $\mathbb{Q}$ where α is a root of f.

Theorem :). Let p be a prime. Then there a field of order p^2.

Proof. Note that the if there is a field of order p^2, it is characteistic p, so there is a copy of $\mathbb{F}_p$ living in that field F.

Our goal here is to find an irreducible polynomial in $\mathbb{F}_p[x]$ with degree 2.

We may assume without loss of generality that the polynomial we are looking for is monic, i.e.

$$f = x^2 + c_1 x + c_0$$

Note there are p^2 choices for f. We claim exactly $\frac{p^2+p}{2}$ are reducible, so $\frac{p^2-p}{2}$ are irreducible.

If f is reducible, then:

$$f = (x - a)(x - b)$$

If $a \neq b$, $p(p-1)/2$ choices. If $a = b$, there are p choices. Thus we have $\frac{p^2+p}{2}$ choices for reducible. □

Theorem :). For every prime power p^k, there is a field of order p^k.

Definition (Field Extension). Given two fields K and F, we say K is an extension of F is there is a nonzero homomorphism $F \to K$, we write ${}^{K}/_{F}$ (not quotient).

Theorem I. f $\rho : F \to K$ is a homomorphism, then it is injective, as the kernel is an ideal but the only ideals in fields are the trivial ideal or the field itself, where we assumed the kernel is not the whole field.

Definition G. iven a field extension K/F, an element $\alpha \in K$ is algebraic if there exists a non-zero polynomial $f \in F[x]$ such that $f(\alpha) = 0$.

Definition (Algebraic Field). A field extension K/F is algebraic if every $\alpha \in K$ is algebraic over F. Otherwise, it is transcendental.

Theorem :). If K/F is a field extension, then K is a vector space over F.

Definition T. he extension K/F is called finite as its a finite dimensional vector space. It's dimension is called the degree of the extension.

Theorem I. f F is a field and $f \in F[x]$ is irreducible with $\deg f = n$, and we set $K = F[x]/(f)$ then $[K : F] = \deg(f) = n$.

Theorem L. et K be a finite extension (i.e. the dimension of K as a vector space over F is finite) of F. Then K is algebraic over F.

Definition I. f K/F is an extension and $\alpha \in K$ is algebraic over F, the minimal polynomial of α is the smallest degree monic polynomial in $F[x]$ of which α is a root.

Theorem :). Let K/F ane extension of fields, $\alpha \in K$ algebraic over F, and $f, g \in F[x]$ such that $f(\alpha) = 0 = g(\alpha)$. Then if $\phi = \gcd(f, g)$, we have $\phi(\alpha) = 0$.

Proof. straightforward by using Bezout's gcd identity on phi and plugging in α □

Theorem :). Let K/F be an extension of fields, and $\alpha \in K$ algebraic over F. Then the minimal polynomial of α exists, is unique, and is irreducible.

Theorem :). Given a field F, $F[x]$ is a principal ideal domain.

Theorem :). Let $f \in \mathbb{Z}[x]$ be monic. Then f is irreducible in $\mathbb{Q}[x]$ if and only if it cannot be written as $f = gh$, with $g, h \in \mathbb{Z}$,

$$1 \leq \deg g, \deg h \leq \deg f - 1$$

Theorem :). Let $f \in \mathbb{Z}[x]$ be monic, and suppose there is some prime p such that when f is reduced mod p, it is irreducible in $\mathbb{F}_p[x]$. Then f is irreducible in $\mathbb{Z}[x]$, and so it is irreducible in $\mathbb{Q}[x]$.

Example: recall cayley's theorem as synergistic with roots over splitting field; i.e. $\mathrm{Gal}(f)$ embeds into S_n. So Galois groups are inextricably related to permutation of roots.

Example: Consider $f = x^4 - 2 \in \mathbb{Q}[x]$. Splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$. Functions in Galois group are determined by how they permute roots. The Galois group here is D_4.

Example: Usually; $|\mathrm{Gal}(f)| = [L : F]$. In this example, we know it is 8 by applying degree formula

You can also just think that $\mathbb{Q}(\sqrt[4]{2})$ is precisely ${}^{\mathbb{Q}[x]}/_{(x^4-2)}$, which is clearly a degree 4 extension. So deg 4 times degree 2.

Theorem galois lemma 1. Let F be a field, $f \in F[x]$ irreducible, L the splitting field of F, and α, α' two roots of f in L.

Then there is a unique isomorphism $\varphi : F(\alpha) \to F(\alpha')$ fixing F and s.t. $\varphi(\alpha) = \alpha'$.

Proof. trivial □

Example: why useful? go back to example with $x^4 - 2$ over $\mathbb{Q}$.

Theorem galois lemma 2. Let $\varphi : K \to K'$ an isomorphism of fields. Then the extension of ϕ to $\phi : K[x] \to K'[x]$ such that $\phi(x) = x$ is an isomorphism.