FATE-H Statements

Formalization Contribution

Nailin Guan Zixun Guo Wanyi He Yongle Hu Jiedong Jiang Jingting Wang

Mathematical Contribution

Kaiyi Chen Haocheng Fan Yiqin He Yongle Hu Shanxiao Huang Jiedong Jiang Yudong Liu Tian Qiu Yinchong Song Yuefeng Wang Peihang Wu Zhenhua Wu Tianyi Xu Zhehan Xu Huanhuan Yu Huishi Yu Jiahong Yu Zhanhao Yu Xiao Yuan

July 2025

Exercise (1)**.** *Prove that if H is a subgroup of G of index n, then there is a normal subgroup K of G such that $K \leq H$ and $[G : K] \leq n!$*

```
import Mathlib

/- Prove that if $H$ is a subgroup of $G$ of index $n$, then there is a normal
    subgroup $K$ of $G$
such that $K\leq H$ and $[G:K]\leq n!$-/
theorem subgroup_normal_index_le_factorial {G : Type} [Group G] {n : ℕ} (hn :
    n ≠ 0)
     (H : Subgroup G) (hH : H.index = n) :
    ∃ K : Subgroup G, K.Normal ∧ K ≤ H ∧ K.index ≠ 0 ∧ K.index ≤ n.factorial
    := by
  sorry
```

Exercise (2)**.** *Prove that if $\#G = 56$ then G is not simple.*

```
import Mathlib

/- Prove that if $\#G = 56$ then $G$ is not simple.-/
```

```
theorem not_isSimpleGroup_of_card_eq_56 {G : Type} [Group G] (hG : Nat.card G =
     56) :
    ¬ IsSimpleGroup G := by
  sorry
```

Exercise (3)**.** *Prove that if* $\#G = 3393$ *then* G *is not simple.*

```
import Mathlib

/- Prove that if $\#G = 3393$ then $G$ is not simple. -/
theorem not_isSimpleGroup_of_card_eq_3393 {G : Type} [Group G] (h : Nat.card G
    = 3393) : ¬ IsSimpleGroup G := by
  sorry
```

Exercise (4)**.** *Prove that if* p *is a prime and* P *is a non-abelian group of order* p^3*, then* $|Z(P)| = p$ *and* $P/Z(P) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$*.*

```
import Mathlib

/- Prove that if $p$ is a prime and $P$ is a non-abelian group of order $p^3$,
    then $|Z(P)| = p$
and $P/Z(P) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.-/
theorem nonempty_mulEquiv_zMod_prod_zMod {p : ℕ} [Fact p.Prime] {P : Type}
    [Group P] (hp : Nat.card P = p ^ 3)
    (h : ∃ (a b : P), a * b ≠ b * a) : Nat.card (Subgroup.center P) = p ∧
    Nonempty ((P / Subgroup.center P) ≃* Multiplicative ((ZMod p) × (ZMod p)))
    := by
  sorry
```

Exercise (5)**.** *Let* R *be a ring with* $1 \neq 0$*. For two elements* $a, b \in R$*, if* $1 - ab$ *is a unit, then* $1 - ba$ *is a unit.*

```
import Mathlib

/- Let $R$ be a ring with $1 \neq 0$.\nFor two elements $a,b \in R$, if $1-ab$
    is a unit,
then $1-ba$ is a unit. -/
theorem isUnit_one_sub_mul {R : Type} [Ring R] [Nontrivial R] {a b : R} (h :
    IsUnit (1 - a * b)) :
```

```
    IsUnit (1 - b * a) := by
  sorry
```

Exercise (6)**.** *Show that a prime p can be written as $p = a^2 + ab + b^2$ with $a, b \in \mathbb{Z}$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$.*

```
import Mathlib

/-- Show that a prime $p$ can be written as $p = a^2+ab+b^2$ with $a,b \in
    \mathbb{Z}$ if and only
if $p=3$ or $p \equiv 1 \pmod 3$. -/
theorem exists_sum_two_squares_iff_mod_three_eq_one (p : ℕ) (hp : p.Prime) :
    (∃ a b : ℤ, a ^ 2 + a * b + b ^ 2 = p) ↔ p = 3 ∨ p % 3 = 1 := by
  sorry
```

Exercise (7)**.** *Let G be a group and let $K \subseteq H$ be subgroups of G with $K \lhd H$. If $H \lhd G$ and $C_H(K) = 1$, prove that H centralizes $C_G(K)$.*

```
import Mathlib

open Subgroup

/- Let $G$ be a group and let $K\subseteq H$ be subgroups of $G$ with $K \lhd
    H$.
   If $H \lhd G$ and $C_H(K)=1$, prove that $H$ centralizes $C_G(K)$.-/
theorem le_centralizer_centralizer_of_centralizer_eq_bot {G : Type} [Group G]
    (H K : Subgroup G)
    [H.Normal] (h1 : K ≤ H) [(K.subgroupOf H).Normal]
    (h2 : Subgroup.centralizer (K.subgroupOf H) = (⊥ : Subgroup H)) :
    H ≤ Subgroup.centralizer (Subgroup.centralizer (K : Set G) : Set G) := by
  sorry
```

Exercise (8)**.** *Show that if a Sylow 2-subgroup of G is nontrivial and cyclic, then G has a subgroup H with $[G : H] = 2$.*

```
import Mathlib

/-- Show that if a Sylow $2$-subgroup of $G$ is nontrivial and cyclic, then $
    G$ has a subgroup $H$
```

```
with $[G:H] =2$. -/
theorem exists_index_two_of_sylow_two_isCyclic {G : Type} [Group G] [Finite G]
    (P : Sylow 2 G)
    (h1 : P.toSubgroup ≠ ⊥) [IsCyclic P] : ∃ H : Subgroup G, H.index = 2 := by
  sorry
```

Exercise (9). *If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.*

```
import Mathlib

/-- If \( n \) is odd and \( n \geq 3 \), show that the identity is the only
    element of
\( D_{2n} \) which commutes with all elements of \( D_{2n} \). -/
theorem DihedralGroup.centralizer_eq_bot {n : ℕ} (hn : Odd n) (h : n ≥ 3) :
    Subgroup.centralizer ⊤ = (⊥ : Subgroup (DihedralGroup n)) := by
  sorry
```

Exercise (10). *Determine the last two digits of $3^{3^{100}}$.*

```
import Mathlib

/- prove that the last two digits of $3^{3^{100}} is 03-/
theorem three_pow_three_pow_mod_100 : 3 ^ (3 ^ 100) % 100 = 3 := by
  sorry
```

Exercise (11). *Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 in G, then $H \leq Z(G)$.*

```
import Mathlib

/- Let $G$ be a group of order $3825$. Prove that if $H$ is a normal subgroup
    of order $17$ in $G$,
then $H \leq Z(G)$.-/
theorem le_center_of_card_eq_17_of_card_eq_3825 {G : Type} [Group G] (h :
    Nat.card G = 3825)
    (H : Subgroup G) [H.Normal] (hH : Nat.card H = 17) : H ≤ Subgroup.center G
    := by
  sorry
```

Exercise (12)**.** *Prove that* $SL_2(\mathbb{F}_3)/Z(SL_2(\mathbb{F}_3)) < A_4$.

```
import Mathlib

open MatrixGroups

/--
Prove that \( SL_2(\mathbb{F}_3) / Z(SL_2(\mathbb{F}_3)) < A_4 \).
-/
theorem exists_sl_quot_center_monoidHom_alternatingGroup :
    ∃ φ : SL(2,ZMod 3) / Subgroup.center SL(2,ZMod 3) →* alternatingGroup (Fin
    4),
    Function.Injective φ := by
  sorry
```

Exercise (13)**.** *Prove that the number of Sylow* p*-subgroups of* $\mathrm{GL}_2(\mathbb{F}_p)$ *is* $p+1$.

```
import Mathlib

open Matrix

/-- Prove that the number of Sylow $p$-subgroups of $
    \operatorname{GL}_2(\mathbb{F}_p)$ is $p + 1$.
-/
theorem card_sylow_gl_two_eq_add_one (p : ℕ) [Fact p.Prime] :
    Nat.card (Sylow p <| GL (Fin 2) (ZMod p)) = p + 1 := by
  sorry
```

Exercise (14)**.** *Let* S *be any ring and let* $n > 2$ *be an integer. Prove that if* A *is any strictly upper triangular matrix in* $M_n(S)$*, then* $A^n = 0$*. (A strictly upper triangular matrix is one whose entries on and below the main diagonal are all zero.)*

```
import Mathlib

/-- Let $S$ be any ring and let $n>2$ be an integer.
Propose a proof that if $A$ is any strictly upper triangular matrix in $
    M_n(S)$, then $A^n = 0$.
(A strictly upper triangular matrix is one whose entries on and below the main
    diagonal are all
```

```
zero.) -/
theorem pow_eq_zero_of_strictly_upper_triangle {S : Type} [Ring S] (n : ℕ) (hn
    : 2 < n)
     (A : Matrix (Fin n) (Fin n) S) (hA : ∀ (i : Fin n), ∀ (j : Fin n), i ≥ j →
    A i j = 0) :
     A ^ n = 0 := by
  sorry
```

Exercise (15)**.** *Prove that the ring* $\mathbb{Z}[\sqrt{-5}]$ *is not a principal ideal domain.*

```
import Mathlib

/- Prove that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal
    domain. -/
theorem not_isPrincipalIdealRing_Zsqrtd_neg_five : ¬IsPrincipalIdealRing
    (Zsqrtd (-5)) := by
  sorry
```

Exercise (16)**.** *Let* R *be an integral domain and let* i, j *be relatively prime integers. Prove that the ideal* $(x^i - y^j)$ *is a prime ideal in* $R[x, y]$*.*

```
import Mathlib

open MvPolynomial Ideal
/- Let \( R \) be an integral domain and let \( i, j \) be relatively prime
    integers. Prove that the ideal \( (x^i - y^j) \) is a prime ideal in \(
    R[x, y] \).-/
theorem span_pow_sub_pow_isPrime_of_coprime {R : Type} [CommRing R] [IsDomain
    R] {i j : ℕ}
     (hi : i > 0) (hj : j > 0) (h : Nat.Coprime i j) :
     (span {(X 0 ^ i - X 1 ^ j : MvPolynomial (Fin 2) R)}).IsPrime := by
  sorry
```

Exercise (17)**.** *Prove that* $\frac{x^p-1}{x-1}$ *is irreducible in* $\mathbb{Z}[x]$*.*

```
import Mathlib

open Polynomial
```

```
/-- Prove that $\frac{x^{p}-1}{x-1}$ is irreducible in $\mathbb{Z}[x].$ -/
theorem irreducible_X_pow_p_sub_one_div_X_sub_one (p : ℕ) [hp : Fact
    (Nat.Prime p)] :
    Irreducible (((Polynomial.X : ℤ[X]) ^ p - 1) /ₘ (Polynomial.X - 1)) := by
  sorry
```

Exercise (18). *Prove that* $x^2 + y^2 - 1$ *is irreducible in* $\mathbb{Q}[x, y]$.

```
import Mathlib

open MvPolynomial

/- Prove that \( x^2 + y^2 - 1 \) is irreducible in \( \mathbb{Q}[x, y] \).-/
theorem irreducible_pow_two_add_pow_two_sub_one :
    Irreducible ((X 0) ^ 2 + (X 1) ^ 2 - 1 : MvPolynomial (Fin 2) ℚ) := by
  sorry
```

Exercise (19). *Prove that any finite group is isomorphic to a subgroup of* A_n *for some* n.

```
import Mathlib

/-- Prove that any finite group is isomorphic to a subgroup of $A_n$ for some $
   n$. -/
theorem exists_subgroup_alternatingGroup_mulEquiv {G : Type} [Group G] [Finite
   G] :
    ∃ (n : ℕ) (H : Subgroup (alternatingGroup (Fin n))), Nonempty (G ≃* H) :=
   by
  sorry
```

Exercise (20). *Prove that if* G *is a nonabelian group of order* p^3 *(*p *prime), then the center of* G *is the subgroup generated by all elements of the form* $aba^{-1}b^{-1}$ *(*$a, b \in G$*).*

```
import Mathlib

/-- Prove that if $G$ is a nonabelian group of order $p^3$ ($p$ prime),
    then the center of $G$ is the subgroup generated by all elements of
    the form $aba^{-1}b^{-1}$ ($a, b \in G$). -/
```

```
theorem center_eq_commutator_of_pow_three_eq_card {G : Type} [Group G] {p : ℕ}
    [hp : Fact p.Prime]
    (hG : p ^ 3 = Nat.card G) (h : ∃ x y : G, x * y ≠ y * x) :
    Subgroup.center G = commutator G := by
  sorry
```

Exercise (21)**.** *Prove that the order of* $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_9)$ *is 108.*

```
import Mathlib

/- Prove that the order of Aut(Z_3 × Z_9) is 108.-/
theorem card_addAut_eq_108 : Nat.card (AddAut <| ZMod 3 × ZMod 9) = 108 := by
  sorry
```

Exercise (22)**.** *Let* D_8 *be the dihedral group with* 8 *elements. Prove that* $\mathrm{Aut}(D_8) \cong D_8$*.*

```
import Mathlib

/--Let $D_8$ be the dihedral group with $8$ elements. Prove that $
    \mathrm{Aut}(D_8) \cong D_8$.-/
theorem nonempty_mulAut_dihedralGroup_four : Nonempty (MulAut (DihedralGroup
    4) ≃* DihedralGroup 4) := by
  sorry
```

Exercise (23)**.** *Prove that if* $\#G = 1053$ *then* G *is not simple.*

```
import Mathlib

/-- Prove that if $\#G = 1053$ then $G$ is not simple. -/
theorem not_isSimpleGroup_of_card_eq_1053 (G : Type) [Group G]
    [Finite G] (h_card : Nat.card G = 1053) : ¬ IsSimpleGroup G := by
  sorry
```

Exercise (24)**.** *Prove that* $\mathbb{Q}/\mathbb{Z}$ *has no proper subgroups of finite index.*

```
import Mathlib

/--
```

```
Prove that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index.
-/
theorem eq_top_of_finiteIndex (H : AddSubgroup (ℚ / (Int.castAddHom ℚ).range))
    (h_fin : H.FiniteIndex) :
    H = ⊤ := by
  sorry
```

Exercise (25). *Let* $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$*be the set of polynomials in* x *with rational coefficients whose constant term is an integer. Prove that* R *is not a U.F.D.*

```
import Mathlib

open Polynomial
/--Let $R=\mathbb{Z}+x\mathbb{Q}[x]\subset \mathbb{Q}[x]$be the set of
    polynomials in x with rational coefficients
whose constant term is an integer. Prove that $R$ is not a U.F.D.-/
theorem not_uniqueFactorizationMonoid_adjoin_int : ¬ UniqueFactorizationMonoid
    (Algebra.adjoin ℤ ({f | ∃ h : ℚ[X], f = X * h} : Set ℚ[X])) := by
  sorry
```

Exercise (26). *Suppose* G *is a group and* H *is a maximal subgroup of* G*. Show that either* $Z(G) \leq H$ *or* $[G,G] \leq H$*. (A maximal subgroup contains either the center or the commutator subgroup.)*

```
import Mathlib

/--Suppose \( G \) is a group and \( H \) is a maximal subgroup of \( G \).
    Show that either \( Z(G)
\leq H \) or \( [G,G] \leq H \). (A maximal subgroup contains either the
    center or the commutator
 subgroup.)-/
theorem center_le_or_commutator_le_of_isCoatom {G : Type} [Group G] (H :
    Subgroup G)
    (h : IsCoatom H) : Subgroup.center G ≤ H ∨ commutator G ≤ H := by
  sorry
```

Exercise (27). *Let* F *be a field contained in the ring of* $n \times n$ *matrices over* $\mathbb{Q}$*. Prove that* $[F : \mathbb{Q}] \leq n$*.*

```
import Mathlib

/-- Let $F$ be a field contained in the ring of $n \times n$ matrices over $
    \mathbb{Q}$.
Prove that $[F:\mathbb{Q}] \leq n$. -/
theorem rank_le_of_subalgebra_matrix {n : ℕ} (F : Subalgebra ℚ (Matrix (Fin n)
    (Fin n) ℚ))
    (h : IsField F) : Module.rank ℚ F ≤ n := by
  sorry
```

Exercise (28). *Let k be a perfect field of characteristic $p > 0$. Let $F = k(t)$ be the field of rational functions in one variable over k. Show that every finite extension E of F can be generated by one element, that is, there exists $\alpha \in E$ such that $E = F(\alpha)$.*

```
import Mathlib

open IntermediateField

/-- Let $k$ be a perfect field of characteristic $p > 0$.
Let $F = k(t)$ be the field of rational functions in one variable over $k$.
Show that every finite extension $E$ of $F$ can be generated by one element,
    that is,
there exists $\alpha \in E$ such that $E = F(\alpha)$. -/
theorem exists_ratFunc_adjoin_eq_top {k : Type} [Field k] [PerfectField k] {p
    : ℕ} [Fact p.Prime] [CharP k p]
    {E : Type} [Field E] [Algebra (RatFunc k) E] [FiniteDimensional (RatFunc
    k) E] :
    ∃ α : E, (RatFunc k)⟮α⟯ = ⊤ := by
  sorry
```

Exercise (29). *Show that if F has characteristic p, then all degree p Galois extension of F are obtained by adjoining a zero of $x^p - x - a$ for some $a \in F$.*

```
import Mathlib

open IntermediateField Polynomial

```

```
/- Show that if $F$ has characteristic $p$, then all degree $p$ Galois
    extension of $F$ is to
adjoin a zero of $x^p-x-a$ for some $a \in F$.-/
theorem exists_nonempty_adjoin_root_X_pow_p_sub_X_sub_C
    {F E : Type} [Field F] {p : ℕ} [Fact p.Prime] [CharP F p] [Field E]
    [Algebra F E] [IsGalois F E] (h_deg : Module.finrank F E = p) :
    ∃ a : F, Nonempty (AdjoinRoot (X ^ p - X - C a : F[X]) ≃+* E) := by
  sorry
```

Exercise (30)**.** *Let E be the splitting field of*

$$f(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

over $\mathbb{Q}$. Let ζ be a zero of $f(x)$, i.e., a primitive seventh root of 1. Let $\beta = \zeta + \zeta^2 + \zeta^4$. Show that the intermediate field $\mathbb{Q}(\beta)$ is actually $\mathbb{Q}(\sqrt{-7})$.

```
import Mathlib

open Polynomial
open scoped IntermediateField

/-- Let $E$ be the splitting field of
\[
f(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
\]
over $\mathbb{Q}$. Let $\zeta$ be a zero of $f(x)$, i.e., a primitive seventh
    root of $1$.
Let $\beta = \zeta + \zeta^2 + \zeta^4$. Show that the intermediate field $
    \mathbb{Q}(\beta)$
is actually $\mathbb{Q}(\sqrt{-7})$. -/
theorem nonempty_ringEquiv_adjoin_pow_two_add_seven {E : Type} [Field E]
    [Algebra ℚ E]
    [IsCyclotomicExtension {7} ℚ E] (ζ : E)
    (h : IsPrimitiveRoot ζ 7) (β : E) (hb : β = ζ + ζ ^ 2 + ζ ^ 4) :
    Nonempty (ℚ⟮β⟯ ≃+* AdjoinRoot (X ^ 2 + 7 : ℚ[X])) := by
  sorry
```

Exercise (31)**.** *Prove that the primitive n^{th} roots of unity form a basis over $\mathbb{Q}$ for the cyclotomic field of n^{th} roots of unity if and only if n is squarefree.*

```
import Mathlib

/- Prove that the primitive $n^{\textrm{th}}$ roots of unity form a basis over
    $\mathbb{Q}$ for
the cyclotomic field of $n^{\textrm{th}}$ roots of unity if and only if $n$ is
    squarefree.-/
theorem exists_basis_primitiveRoots_iff_squarefree {n : ℕ+} :
    (∃ b : Basis (primitiveRoots n (CyclotomicField n ℚ)) ℚ (CyclotomicField n
    ℚ),
    (b : _ → _) = (↑)) ↔ Squarefree n := by
  sorry
```

Exercise (32). *Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group*

```
import Mathlib

open Polynomial

/- The Galois group of the splitting field of $x^4 - 2x^2 - 2$ over $
    \mathbb{Q}$ is the
dihedral group with eight elements-/
theorem nonempty_galois_mulEquiv_dihedralGroup_four :
    Nonempty (Gal (X ^ 4 - 2 * X ^ 2 - 2 : ℚ[X]) ≃* DihedralGroup 4) := by
  sorry
```

Exercise (33). *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n ($n > 4$) and the splitting field E of $f(x)$ has Galois group S_n over $\mathbb{Q}$. Let α be a zero of $f(x)$ in E. Prove that for any other root β of $f(x)$, there are precisely $(n-1)!$ elements in* $\mathrm{Gal}(E/\mathbb{Q})$ *that takes α to β.*

```
import Mathlib

open Polynomial

/- Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $n$ ($n>4$) and the
    splitting field $E$
of $f(x)$ has Galois group $S_n$ over $\mathbb{Q}$. Let $\alpha$ be a zero of $
    f(x)$ in $E$.
```

```
Prove that for any other root $\beta$ of $f(x)$, there are precisely $(n-1)!$
    elements in
$\mathrm{Gal}(E/\mathbb{Q})$ that takes $\alpha $ to $\beta$ -/
theorem card_gal_map_eq_eq_factorial {n : Nat} (hn : n > 4) (f : ℚ[X]) (hf :
    f.degree = n)
    (hf' : Irreducible f) (h : f.Gal ≃* (Equiv.Perm <| Fin n))
    {a b : SplittingField f} (ha : f.aeval a = 0) (hb : f.aeval b = 0) (neq :
    a ≠ b) :
    Nat.card {h : f.Gal // h a = b} = Nat.factorial (n - 1) := by
  sorry
```

Exercise (34)**.** *Let E be a field of characteristic zero. Consider a prime q and an element $b \in E^{\times}$ that isn' t a q-th power. Let $E' = E(a)$ with $a^q = b$ and $E' \neq E$. Show that $X^q - b$ is reducible over E if and only if $[E' : E] < q$.*

```
import Mathlib

open Polynomial
/- Let \( E \) be a field of characteristic zero. Consider a prime \( q \) and
    an element \( b
\in E^\times \) that isn' t a \( q \)-th power. Let \( E' = E(a) \) with \(
    a^q = b \). Show that
\( X^q - b \) is reducible over \( E \) if and only if \( [E' : E] < q \)-/
theorem not_irreducible_iff_finrank_lt {E E': Type} [Field E] [CharZero E]
    [Field E'] [Algebra E E'] {q : ℕ}
    [Fact q.Prime] {b : E} (hb : b ≠ 0) (not_pow : ∀ c : E, c ^ q ≠ b) {a : E'}
    (ha : a ^ q = algebraMap E E' b) (haE : ⊤ = IntermediateField.adjoin E
    {a}) :
    ¬ Irreducible (X ^ q - C b) ↔ Module.finrank E E' < q := by
  sorry
```

Exercise (35)**.** *Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Show that $\mathbb{Q}(\sqrt{a\sqrt{D}})$ cannot be a cyclic extension of degree 4 over $\mathbb{Q}$.*

```
import Mathlib

open Polynomial IntermediateField
```

```
/- Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$
    be a nonzero rational number.
Show that $\mathbb{Q}(\sqrt{a\sqrt D})$ cannot be a cyclic extension of degree
    $4$ over $\mathbb{Q}$.-/
theorem isEmpty_adjoinRoot_zMod_four {d : ℤ} (hd : Squarefree d) {a : ℚ} (ha :
    a ≠ 0) :
     IsEmpty ((AdjoinRoot ((a⁻¹ • X ^ 2) ^ 2 - C (d : ℚ)) ≃ₐ[ℚ]
       AdjoinRoot ((a⁻¹ • X ^ 2) ^ 2 - C (d : ℚ))) ≃* Multiplicative (ZMod 4))
    := by
  sorry
```

Exercise (36). *Let $f(X) = X^4 - X^2 - 1 \in \mathbb{Q}[X]$, K is the splitting field of f over $\mathbb{Q}$, prove that the number of intermediate fields of $K/\mathbb{Q}$ is 10.*

```
import Mathlib

open Polynomial IntermediateField

/-- Let $f(X)=X^4-X^2-1\in \mathbb{Q}[X]$, $K$ is the splitting field of $f$
    over $\mathbb{Q}$,
prove that the number of intermediate fields of $K/\mathbb{Q}$ is 10. -/
theorem card_intermediateField_splittingField_eq_ten :
     Nat.card (IntermediateField ℚ (X ^ 4 - X ^ 2 - 1 : ℚ[X]).SplittingField) =
    10 := by
  sorry
```

Exercise (37). *Let L/K be a Galois extension of fields such that $\mathrm{Gal}(L/K)$ is cyclic of order n, generated by σ. Write $n = ab$ with $\gcd(a, b) = 1$. Let F_1 be the fixed field of σ^a and F_2 be the fixed field of σ^b. Suppose that $F_1 = K(\alpha)$ and $F_2 = K(\beta)$. Prove that $L = K(\alpha + \beta)$.*

```
import Mathlib

open Polynomial IntermediateField AdjoinRoot

/-- Let $L/K$ be a Galois extension of fields such that $\mathrm{Gal}(L/K)$ is
    cyclic of order $n$,
generated by $\sigma$. Write $n = ab$ with $\gcd(a,b) =1$. Let $F_1$ be the
    fixed field of
```

```
$\sigma^a$ and $F_2$ be the fixed field of $\sigma^b$. Suppose that $F_1 =
    K(\alpha)$ and
$F_2 = K(\beta)$.  Prove that $L = K(\alpha+\beta)$. -/
theorem adjoin_add_eq_top_of_fixedField_zpowers {K L : Type} [Field K]
     [Field L] [Algebra K L] [IsGalois K L] (n a b : ℕ)
     (σ : L ≃ₐ[K] L) (hσ : orderOf σ = n) (cycle : Subgroup.zpowers σ = ⊤) (hn
    : n > 0)
     (hn' : n = a * b) (hab : Nat.Coprime a b) {α β : L}
     (hα : K(α) = IntermediateField.fixedField (Subgroup.zpowers (σ ^ a)))
     (hβ : K(β) = IntermediateField.fixedField (Subgroup.zpowers (σ ^ b))) :
    K(α + β) = ⊤ := by
  sorry
```

Exercise (38). *Let p be a prime number and let F be a field containing p-th roots of unity. Let K be a Galois extension of F with Galois group $\mathbb{Z}/p \times \mathbb{Z}/p$. Show that there exist two elements $\alpha, \beta \in K^\times$ such that $K = F(\alpha, \beta)$ and $a = \alpha^p, b = \beta^p \in F$.*

```
import Mathlib

open IntermediateField

/-Let $p$ be a prime number and let $F$ be a field containing $p$-th roots of
    unity.
Let $K$ be a Galois extension of $F$ with Galois group $\mathbb{Z}_p \times
    \mathbb{Z}_p$.
Show that there exist two elements $\alpha, \beta \in K^\times$ such that
$K= F(\alpha, \beta)$ and $a = \alpha^p, b = \beta^p \in F$.-/
theorem exists_pow_p_mem_algebraMap_and_adjoin_eq_top {p : Nat} [Fact p.Prime]
     {F K : Type} [Field F] (hF : (primitiveRoots p F).Nonempty) [Field K]
     [Algebra F K]
     [IsGalois F K] (hK : (K ≃ₐ[F] K) ≃* Multiplicative (ZMod p × ZMod p)) :
     ∃ (α β : K), α ≠ 0 ∧ β ≠ 0 ∧ α ^ p ∈ (algebraMap F K).range ∧ β ^ p ∈
     (algebraMap F K).range ∧
     IntermediateField.adjoin F {α, β} = ⊤ := by
  sorry
```

Exercise (39). *Prove that a splitting field of $X^{15} - 2$ over $\mathbb{F}_7$ is generated by a primitive 45-th root of unity.*

```
import Mathlib

open Polynomial
/- Prove that a splitting field of \( X^{15} - 2 \) over \( \mathbb{F}_7 \) is
    generated by a
 primitive \( 45 \)-th root of unity.-/
theorem exists_isPrimitiveRoot_and_adjoin_eq_top :
    letI : Fact (Nat.Prime 7) := by decide
    ∃ ζ : (X ^ 15 - 2 : (ZMod 7)[X]).SplittingField, IsPrimitiveRoot ζ 45 ∧
    IntermediateField.adjoin (ZMod 7) {ζ} = ⊤ := by
  sorry
```

Exercise (40). *Let K be the splitting field of an irreducible quintic polynomial $f(x) \in \mathbb{Q}[x]$ and let $\{\alpha_1, \ldots, \alpha_5\}$ be zeros of $f(x)$ in K. Show that if $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \neq K$, then* $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$.

```
import Mathlib

open Polynomial

/- Let $K$ be the splitting field of a irreducible quintic polynomial $f(x)
    \in \mathbb{Q} [x]$
and let $\{\alpha_1, \dots, \alpha_5\}$ be zeros of $f(x)$ in $K$. Show that
    if $\mathbb{Q}
(\alpha_1, \alpha_2, \alpha_3) \neq K$, then $\\mathrm{Gal}(K/\mathbb{Q})
    \cong S_5$.-/
theorem nonempty_gal_mulEquiv_perm_fin_five {f : ℚ[X]} {K : Type} [Field K]
    [Algebra ℚ K]
    [IsSplittingField ℚ K f] (hf1 : Irreducible f) (hf2 : f.natDegree = 5) (a₁
    a₂ a₃ : K)
    (ha1 : a₁ ∈ rootSet f K ∧ a₂ ∈ rootSet f K ∧ a₃ ∈ rootSet f K)
    (ha2 : a₁ ≠ a₂ ∧ a₂ ≠ a₃ ∧ a₃ ≠ a₁)
    (h : IntermediateField.adjoin ℚ {a₁, a₂, a₃} ≠ ⊤) :
    Nonempty (f.Gal ≃* (Equiv.Perm <| Fin 5)) := by
  sorry
```

Exercise (41). *Let p be a prime integer. Suppose that the degree of every finite extension of a field F is divisible by p. Prove that the degree of every finite extension of F is a power of p.*

```
import Mathlib

/-- Let $p$ be a prime integer. Suppose that the degree of every finite
    extension of a field $F$
 is divisible by $p$. Prove that the degree of every finite extension of $F$
    is a power of $p$. -/
theorem exists_finrank_eq_pow_of_dvd_finrank {F : Type} [Field F] (p : ℕ)
    [Fact (Nat.Prime p)]
    (h : ∀ (E : Type) [Field E] [Algebra F E] [FiniteDimensional F E],
    Module.finrank F E ≠ 1 → p ∣ Module.finrank F E)
    (E : Type) [Field E] [Algebra F E] [FiniteDimensional F E] :
    ∃ k, Module.finrank F E = p ^ k := by
  sorry
```

Exercise (42)**.** *Let K be a field with $\operatorname{char}(K) \neq 2$. Consider Galois extensions L/K with $\operatorname{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Let $c \in L^\times$ be a nonsquare, and let $E = L(\sqrt{c})$. Prove that E is Galois over K if and only if for each $\sigma \in \operatorname{Gal}(L/K)$, the ratio $\sigma(c)/c$ is a square in L.*

```
import Mathlib

open IntermediateField AdjoinRoot Polynomial

/--Let \( K \) be a field with \( \operatorname{char}(K) \neq 2 \). Consider
    Galois extensions
\( L/K \) with \( \operatorname{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^2 \).
    Let \( c \in L^\times
\) be a nonsquare, and let \( E = K(\sqrt{c}) \). Prove that \( E \) is Galois
    over \( K \) if and
only if for each \( \sigma \in \operatorname{Gal}(L/K) \), the ratio \(
    \sigma(c)/c \) is a square
in \( L \).-/
theorem isGalois_adjoin_iff_isSquare (K L : Type) [Field K] [Field L] (h : ¬
    CharP K 2) [Algebra K L] [IsGalois K L]
    (f : (L ≃ₐ[K] L) ≃* Multiplicative (ZMod 2 × ZMod 2)) (c : Lˣ) (hc : c.1 ≠
     0)
    (hcs : ¬ IsSquare c.1) [Fact (Irreducible (X ^ 2 - C c.1))] :
    IsGalois K (AdjoinRoot (X ^ 2 - C c.1)) ↔ ∀ σ : (L ≃ₐ[K] L), IsSquare (σ
    c / c) := by
```

```
  sorry
```

Exercise (43)**.** *Let F be a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, where $F/\mathbb{Q}$ is a finite* abelian *Galois extension. Let $\alpha \in F$ and let $f(x) \in \mathbb{Q}[x]$ be its minimal monic polynomial. Assume that $|\alpha| = 1$. Prove that $|\beta| = 1$ for every complex root β of $f(x)$.*

```
import Mathlib

open Polynomial

/-- Let $F$ be a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$,
    where $F/\mathbb{Q}$ is a finite \emph
{abelian} Galois extension. Let $\alpha \in F$ and let $f(x) \in
    \mathbb{Q}[x]$ be its minimal monic
polynomial. Assume that $|\alpha | =1$. Prove that $|\beta| = 1$ for every
    complex root $\beta$ of
$f(x)$. -/
theorem norm_eq_one_of_mem_rootSet (F : IntermediateField ℚ ℂ)
    [FiniteDimensional ℚ F] [IsGalois ℚ F]
    (h : ∀ f g : F ≃ₐ[ℚ] F, f * g = g * f) (α : F) (f : ℚ[X])
    (h_min : f = minpoly ℚ α) (ha : ‖α‖ = 1)
    (β : ℂ) (hb : β ∈ f.rootSet ℂ) : ‖β‖ = 1 := by
  sorry
```

Exercise (44)**.** *Let k be a finite field of size q. Show that the number of degree-19 monic irreducible polynomials over k is $\frac{q^{19}-q}{19}$.*

```
import Mathlib

open Polynomial

/-- Let $k$ be a finite field of size $q$. Show that the number of degree-$19$
    monic irreducible
polynomials over $k$ is $\frac{q^{19} - q}{19}$. -/
theorem card_monic_and_irreducible_and_natDegree_eq_19 {F : Type} (q : ℕ)
    [Field F]
    [Fintype F] (hF : Fintype.card F = q) :
    Nat.card { P : F[X] | P.Monic ∧ Irreducible P ∧ P.natDegree = 19 } =
```

```
    (q ^ 19 - q) / 19 := by
  sorry
```

Exercise (45). *Let F be a field, and let $f, g \in F[x] \setminus \{0\}$ be relatively prime and not both constant. Show that $F(x)$ has finite degree $d = \max(\deg(f), \deg(g))$ over its subfield $F\left(\frac{f}{g}\right)$.*

```
import Mathlib

open IntermediateField Polynomial

/-- Let $F$ be a field, and let $f, g \in F[x] \setminus \{0\}$ be relatively
    prime and not both
constant. Show that $F(x)$ has finite degree $d = \max(\deg(f), \deg(g))$ over
    its subfield $F\left
(\frac{f}{g}\right)$. -/
theorem finrank_adjoin_dvd_eq_max_natDegree (F : Type) [Field F] (f g : F[X])
    (hf : f ≠ 0)
    (hg : g ≠ 0) (hcoprime : IsCoprime f g) (hfg : ¬(f.natDegree = 0 ∧
    g.natDegree = 0)) :
    Module.finrank F((f : RatFunc F) / g) (RatFunc F) = max f.natDegree
    g.natDegree := by
  sorry
```

Exercise (46). *Let α be a non-zero complex number such that $\alpha + \alpha^{-1}$ is contained in a quadratic number field. Let L be the normal closure of $\mathbb{Q}(\alpha)$. Show that $[L : \mathbb{Q}]$ divides 8.*

```
import Mathlib

open IntermediateField
/--Let \( \alpha \) be a non-zero complex number such that \( \alpha +
    \alpha^{-1} \) is contained
in a quadratic number field. Let \( L \) be the normal closure of \(
    \mathbb{Q}(\alpha) \). Show
that \( [L : \mathbb{Q}] \) divides \( 8 \).-/
theorem finrank_dvd_eight_of_add_inv_eq_algebraMap {α : ℂ} {K L : Type} [Field
    K] [NumberField K]
    [Algebra K ℂ] (hk : Module.finrank ℚ K = 2) {a : K} (h : α + α⁻¹ =
    algebraMap K ℂ a)
```

```
    [Field L] [Algebra ℚ L] [IsNormalClosure ℚ ℚ(a) L] : Module.finrank ℚ L ∣
    8 := by
  sorry
```

Exercise (47). *Let* ζ *be a primitive* 9*-th root of unity in* $\mathbb{C}$*, so* $\zeta^9 = 1$*, and let* $\omega = \zeta^3$ *be a primitive* 3*-rd root of unity, so* $\omega^3 = 1$*. If* $\alpha^3 = 3$*, show that* α *is not a cube in* $\mathbb{Q}(\zeta)$*.*

```
import Mathlib

open Algebra

open scoped IntermediateField

/-- Let $\zeta$ be a primitive $9$-th root of unity in $\mathbb{C}$, so $
    \zeta^9 = 1$, and let
$\omega = \zeta^3$ be a primitive $3$-rd root of unity, so $\omega^3 = 1$. If $
    \alpha^3 = 3$,
show that $\alpha$ is not a cube in $\mathbb{Q}(\zeta)$. -/
theorem not_exists_eq_pow_three_of_pow_three_eq_three (α : ℂ) (hα : α ^ 3 = 3)
    (ζ : ℂ)
    (hζ : IsPrimitiveRoot ζ 9) : ¬ ∃ β : ℚ⟮ζ⟯, α = β ^ 3 := by
  sorry
```

Exercise (48). *Prove that the cardinality* $\mathrm{Aut}(\mathbb{C})$ *(i.e. the group of field automorphism of* $\mathbb{C}$*) is infinite.*

```
import Mathlib

/-- Prove that the cardinality $\mathrm{Aut}(\CC)$ (i.e. the group of field
    automorphism of $\CC$)
is infinite. -/
theorem infinite_complex_algEquiv : Infinite (ℂ ≃ₐ[ℚ] ℂ) := by
  sorry
```

Exercise (49). *Prove that every finitely generated extension of* $\mathbb{Q}$ *can be embeded into* $\mathbb{C}$*.*

```
import Mathlib
```

```
/- Prove that every finitely generated extension of $\mathbb{Q}$ can be
    embeded into $\mathbb{C}$-/
theorem exists_algHom_complex_injective {F : Type} [Field F] [Algebra ℚ F]
     (h : (⊤ : IntermediateField ℚ F).FG) : ∃ f : F →ₐ[ℚ] ℂ, Function.Injective
    f := by
  sorry
```

Exercise (50)**.** *Let m be a maximal ideal of $\mathbb{Z}[x_1, \dots, x_n]$ and $F = \mathbb{Z}[x_1, \dots, x_n]/m$. Show that F cannot have characteristic* 0*.*

```
import Mathlib

open MvPolynomial

/-- Let $m$ be a maximal ideal of $\mathbb{Z}[x_1, \dots, x_n]$ and $F =
    \mathbb{Z}[x_1, \dots, x_n]
/m$. Show that $F$ cannot have characteristic $0$. -/
theorem not_charZero_mvPolynomial_quot {n : ℕ} (m : Ideal (MvPolynomial (Fin
    n) ℤ))
     [hm : m.IsMaximal] : ¬ CharZero (MvPolynomial (Fin n) ℤ ⧸ m) := by
  sorry
```

Exercise (51)**.** *Let K/F be a simple algebraic extension. Let $K = F(\theta)$. Let L be an intermediate field of K/F. Show that the minimal polynomial of θ over L: $g(x) = x^r + \alpha_1 x^{r-1} + \cdots + \alpha_r$, satisfies that $F(\alpha_1, \dots, \alpha_r) = L$.*

```
import Mathlib

open IntermediateField

/-- Let $K/F$ be a simple algebraic extension. Let $K = F(\theta)$. Let $L$ be
    an intermediate field
of $K/F$. Show that the minimal polynomial of $\theta$ over $L$: $g(x) =
    x^r+\alpha_1x^{r-1} +
\cdots +\alpha_r$, satisfies that $F(\alpha_1, \dots, \alpha_r) = L$. -/
theorem adjoin_minpoly_coeffs_toSet_eq {F K : Type} [Field F] [Field K]
     [Algebra F K] {θ : K} (L : IntermediateField F K) (h : F⟮θ⟯ = ⊤) :
     IntermediateField.adjoin F (minpoly L θ).coeffs.toSet = L := by
  sorry
```

Exercise (52)**.** *Let q denote a power of a prime p. Show that the extension $\mathbb{F}_q(t^{1/n})$ over $\mathbb{F}_q(t)$ is Galois if and only if $q \equiv 1 \bmod n$.*

```
import Mathlib

open IntermediateField

/-- Let $q$ denote a power of a prime $p$. Show that the extension $
    \mathbb{F}_q(t^{1/n})$ over
$\mathbb{F}_q(t)$ is Galois if and only if $q \equiv 1 \bmod n$. -/
theorem isGalois_galoisField_X_pow_iff_modEq_one (p m n : ℕ) (hn : 1 ≤ n) (hm
    : 1 ≤ m)
    [Fact p.Prime] :  IsGalois (GaloisField p m)((RatFunc.X ^ n : RatFunc
    (GaloisField p m)))
    (RatFunc (GaloisField p m)) ↔ p ^ m ≡ 1 [MOD n] := by
  sorry
```

Exercise (53)**.** *Prove that every field automorphism of $\mathbb{R}$ that fixes $\mathbb{Q}$ is trivial.*

```
import Mathlib

/-- Prove that every field automorphism of $\mathbb{R}$ that fixes $
    \mathbb{Q}$ is trivial. -/
theorem real_algEquiv_eq_one (f : ℝ ≃ₐ[ℚ] ℝ) : f = 1 := by
  sorry
```

Exercise (54)**.** *Let $\mathbb{F}_4$ be the field with 4 elements, t a transcendental over $\mathbb{F}_4$, and $F = \mathbb{F}_4(t^4 + t)$ and $K = \mathbb{F}_4(t)$. Show that K is Galois over F.*

```
import Mathlib

open IntermediateField RatFunc

/-- Let $\mathbb{F}_4$ be the field with $4$ elements, $t$ a transcendental
    over $\mathbb{F}_4$,
and $F =\mathbb{F}_4(t^4 + t)$ and $K =\mathbb{F}_4(t)$. Show that $K$ is
    Galois over $F$. -/
theorem isGalois_galoisField_adjoin_X_pow_four_add_X :
```

```
    IsGalois (GaloisField 2 2)((X ^ 4 + X : RatFunc (GaloisField 2 2)))
    (RatFunc (GaloisField 2 2)) := by
  sorry
```

Exercise (55). *Let K be a field with* $\operatorname{char}(K) \neq 2$. *Consider a Galois extension L/K. Show that* $\operatorname{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$ *if and only if the extensions L/K has the form $L = K(\sqrt{a}, \sqrt{b})$ for $a, b \in K^\times$ such that a, b, and a/b are nonsquares in $K^\times$.*

```
import Mathlib

open IntermediateField

/--
Let $K$ be a field with $\operatorname{char}(K) \neq 2$. Consider a Galois
    extension $L/K$.
Show that $\operatorname{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$ if and
    only if
the extensions $L/K$ has the form $L = K(\sqrt{a}, \sqrt{b})$ for $a, b \in
    K^\times$ such that
$a$, $b$, and $a/b$ are nonsquares in $K^\times$.
-/
theorem exists_pow_two_eq_algebraMap_and_adjoin_eq_top {K L : Type} [Field K]
    [Field L]
    [Algebra K L] [IsGalois K L] (hK : ¬ CharP K 2) : IsKleinFour (L ≃ₐ[K] L)
    ↔
    ∃ a b : Kˣ, ∃ x y : L, x ^ 2 = algebraMap K L a.1 ∧ y ^ 2 = algebraMap K L
    b.1 ∧
    K⟮x, y⟯ = ⊤ ∧ ¬IsSquare a ∧ ¬IsSquare b ∧ ¬IsSquare (a / b) := by
  sorry
```

Exercise (56). *Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$, where Φ_n is the nth cyclotomic polynomial over $\mathbb{Q}$.*

```
import Mathlib

open Polynomial

/- Prove that for $n$ odd, $n>1$, $\Phi_{2n}(x) = \Phi_n(-x)$, where $\Phi_n$
    is the $n$th
```

```
cyclotomic polynomial over \mathbb{Q}.-/
theorem cyclotomic_two_mul_eq_cyclotomic_comp_neg {n : ℕ} (hn : Odd n) (hn' :
    1 < n) :
    Polynomial.cyclotomic (2 * n) ℚ = (Polynomial.cyclotomic n ℚ).comp (-X) :=
    by
  sorry
```

Exercise (57). *If F is a field that is not perfect, show that F has a nontrivial purely inseparable extension.*

```
import Mathlib

/- If $F$ is a field that is not perfect, show that $F$ has a nontrivial
    purely inseparable
extension.-/
theorem exists_isPurelyInseparable_and_bot_lt {F : Type} [Field F] (h : ¬
    PerfectField F) :
    ∃ E : IntermediateField F (AlgebraicClosure F), IsPurelyInseparable F E ∧
    ⊥ < E := by
  sorry
```

Exercise (58). *Show that there is at most one extension $F(\alpha)$ of a field F such that $\alpha^4 \in F$, $\alpha^2 \notin F$, and $F(\alpha) = F(\alpha^2)$.*

```
import Mathlib

open IntermediateField
/--Show that there is at most one extension \( F(\alpha) \) of a field \( F \)
    such that \( \alpha^4
\in F \), \( \alpha^2 \notin F \), and \( F(\alpha) = F(\alpha^2) \).-/
theorem exists_eq_adjoin_and_pow_four_mem_bot_and_not_pow_two_mem_bot (F :
    Type) [Field F] :
    Subsingleton {M : IntermediateField F (AlgebraicClosure F) //
    ∃ α : AlgebraicClosure F, M = F⟮α⟯ ∧ α ^ 4 ∈ (⊥ : IntermediateField F
    (AlgebraicClosure F)) ∧
    ¬ α ^ 2 ∈ (⊥ : IntermediateField F (AlgebraicClosure F)) ∧ F⟮α⟯ = F⟮α ^
    2⟯} := by
  sorry
```

Exercise (59). *Show that $x^7 - 11$ has no root in the splitting field of $x^7 - 12$ over $\mathbb{Q}$.*

```
import Mathlib

/--
Show that \( x^7 - 11 \) has no root in the splitting field of \(x^7 - 12\)
    over \(\mathbb{Q}\).
-/
theorem rootSet_isEmpty_in_splittingField :
    (.X ^ 7 - 11 : Polynomial ℚ).rootSet ((.X ^ 7 - 12 : Polynomial
    ℚ).SplittingField) = ⊥ := by
  sorry
```

Exercise (60). *For a positive integer a, consider the polynomial*

$$f_a = x^6 + 3ax^4 + 3x^3 + 3ax^2 + 1.$$

Let F be the splitting field of f_a. Show that its Galois group is solvable.

```
import Mathlib

open Polynomial
/--For a positive integer $a$, consider the polynomial $$ f_a = x^6 + 3ax^4 +
    3x^3 + 3ax^2 + 1.
 $$ Let $F$ be the splitting field of $f_a$. Show that its Galois group is
    solvable.-/
theorem isSolvable_X_pow_six_add_gal {a : ℤ} (ha : a > 0) : IsSolvable
    (X ^ 6 + C (3 * a : ℚ) * X ^ 4 + C 3 * X ^ 3 + C (3 * a : ℚ) * X ^ 2 + C 1
    : ℚ[X]).Gal:= by
  sorry
```

Exercise (61). *Prove that the polynomial $x^4 + 1$ is not irreducible over any field of positive characteristic.*

```
import Mathlib

open Polynomial
/--Prove that the polynomial $x^4+1$ is not irreducible over any field of
    positive characteristic.-/
```

```
theorem not_irreducible_X_pow_four_add_one {F : Type} [Field F] {p : ℕ} [Fact
    p.Prime]
    [CharP F p] : ¬ Irreducible (X ^ 4 + C 1 : F[X]) := by
  sorry
```

Exercise (62)**.** *Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial with splitting field E over F. Choose $\alpha \in E$ with $f(\alpha) = 0$. Furthermore, for some fixed integer $n \geq 1$, let $g(x)$ be an irreducible polynomial in $F[x]$ with $g(\alpha^n) = 0$. If $\deg(f)/\deg(g) = n$ and if the characteristic of F does not divide n, prove that E contains a primitive nth root of unity.*

```
import Mathlib

/--
Let $F$ be a field and let $f(x) \in F[x]$ be an irreducible polynomial with
    splitting field $E$ over $F$.
Choose $\alpha \in E$ with $f(\alpha) =0$. Furthermore, for some fixed integer
    $n \geq 1$,
let $g(x)$ be an irreducible polynomial in $F[x]$ with $g(\alpha^n)=0$. If $
    \deg(f) / \deg(g) = n$
and if the characteristic of $F$ does not divide $n$, prove that $E$ contains
    a primitive $n$th root of unity.-/
theorem primitiveRoots_not_empty (E F : Type) [Field E] [Field F] [Algebra F E]
    (f : Polynomial F) (h_f_irr : Irreducible f) (h_splitting_field :
    f.IsSplittingField F E)
    (a : E) (ha : f.aeval a = 0) (n : ℕ) (hn : n ≥ 1)
    (g : Polynomial F) (h_g_irr : Irreducible g) (h_ga : g.aeval (a ^ n) = 0)
    (h_deg : f.degree = g.degree * n) (h_char : (n : F) ≠ 0) : primitiveRoots
    n E ≠ ∅ := by
  sorry
```

Exercise (63)**.** *Let $f \in \mathbb{Q}[X]$ and $\xi \in \mathbb{C}$ be a root of unity. Show that $f(\xi) \neq 2^{\frac{1}{4}}$.*

```
import Mathlib

open Polynomial
/--Let \( f \in \mathbb{Q}[X] \) and \( \xi \in \mathbb{C} \) be a root of
    unity. Show that \( f(\xi) \neq 2^{\frac{1}{4}} \).-/
theorem eval₂_algebraMap_ne_two_pow_one_dvd_four {n : ℕ} (hn : 1 ≤ n) (f :
    ℚ[X]) (ξ : ℂˣ)
```

```
    (h : ξ ∈ rootsOfUnity n ℂ) : f.eval₂ (algebraMap ℚ ℂ) ξ ≠ (2 : ℂ) ^ ((1 :
    ℂ) / 4) := by
  sorry
```

Exercise (64)**.** *Let K be a finite extension of a field F, and let $f(x) \in K[x]$. Prove that there exists a nonzero polynomial $g(x) \in K[x]$ such that $f(x)g(x) \in F[x]$.*

```
import Mathlib

open Polynomial
/--Let $K$ be a finite extension of a field $F$, and let $f(x) \in K[x]$.
    Prove that there exists a
nonzero polynomial $g(x) \in K[x]$ such that $f(x)g(x) \in F[x]$.-/
theorem exists_mul_eq_map_algebraMap {F K : Type} [Field F] [Field K] [Algebra
    F K] [FiniteDimensional F K]
    (f : K[X]) : ∃ g ≠ 0, ∃ h : F[X], f * g = h.map (algebraMap F K) := by
  sorry
```

Exercise (65)**.** *Prove that for any $a, b \in \mathbb{F}_{p^n}$ that if $x^3 + ax + b$ is irreducible then $-4a^3 - 27b^2$ is a square in $\mathbb{F}_{p^n}$.*

```
import Mathlib

open Polynomial
/--Prove that for any $a,b \in \mathbb{F}_{p^n}$ that if $x^3+ax+b$ is
    irreducible then $-4a^3-27b^2$ is a
 square in $\mathbb{F}_{p^n}$.-/
theorem isSquare_discriminant_of_irreducible {p n : ℕ} [Fact p.Prime] (a b :
    GaloisField p n)
    (h_irr : Irreducible (X ^ 3 + C a * X + C b)) :
    IsSquare (- 4 * a ^ 3 - 27 * b ^ 2) := by
  sorry
```

Exercise (66)**.** *Prove that, if $n \geq 3$, then $x^{2^n} + x + 1$ is* reducible *in $\mathbb{F}_2$.*

```
import Mathlib

open Polynomial
```

```
/--Prove that, if $n \geq 3$, then $x^{2^n}+x+1$ is \emph{reducible} in $
    \mathbb{F}_2$.-/
theorem not_irreducible_X_pow_two_pow_add_X_add_C_one {n : ℕ} (hn : n ≥ 3) :
    ¬ Irreducible (X ^ 2 ^ n + X + C 1 : (ZMod 2)[X]) := by
  sorry
```

Exercise (67)**.** *Prove that the prime ideals of* $\mathbb{F}_7[\alpha] \otimes_{\mathbb{F}_7} \mathbb{F}_7[\alpha]$ *are principal, where* $\alpha^3 = 2$*.*

```
import Mathlib

open Polynomial

/-
Prove that the prime ideals of $\mathbb{F}_7[\alpha] \otimes_{\mathbb{F}_7}
    \mathbb{F}_7[\alpha]$ are principal, where $\alpha^3 = 2$.
-/
theorem isPrincipal_of_ideal_tensor_zMod_seven
    (p : Ideal (TensorProduct (ZMod 7) (AdjoinRoot (X ^ 3 - 2 : Polynomial
    (ZMod 7)))
    (AdjoinRoot (X ^ 3 - 2 : Polynomial (ZMod 7))))) [p.IsPrime] :
    p.IsPrincipal := sorry
```

Exercise (68)**.** *Let* A *be a Noetherian ring and let* $x \in A$ *be an element which is neither a unit nor a zero-divisor. Prove that the ideals* xA *and* x^nA *for* $n = 1, 2, \dots$ *have the same prime divisors:*

$$\operatorname{Ass}_A(A/xA) = \operatorname{Ass}_A(A/x^nA).$$

```
import Mathlib

open Ideal
/-
Let $A$ be a Noetherian ring and let $x \in A$ be an element which is
neither a unit nor a zero-divisor. Prove that the ideals $xA$ and $x^nA$
for $n = 1, 2, \dots$ have the same prime divisors:
\[
\operatorname{Ass}_A(A/xA) = \operatorname{Ass}_A(A/x^nA).
\]
-/
```

```
theorem associatedPrimes_quot_span_eq_quot_span_pow {A : Type} [CommRing A]
    [IsNoetherianRing A]
    (x : A) (hx : x ∈ nonZeroDivisors A) (hx' : ¬ IsUnit x) (n : ℕ) (h : n ≥
    1) :
    associatedPrimes A (A / span {x}) = associatedPrimes A (A / span {x ^ n})
    := by
  sorry
```

Exercise (69). *Prove that if K is a field of finite degree over $\mathbb{Q}$ and $x_1, \dots, x_n$ are finitely many elements of K, then the subring $\mathbb{Z}[x_1, \dots, x_n]$ they generate over $\mathbb{Z}$ is not equal to K.*

```
import Mathlib

/-- Prove that if $K$ is a field of finite degree over $\mathbb{Q}$ and $x_1,
    \dots, x_n$ are
finitely many elements of $K$, then the subring $\mathbb{Z}[x_1, \dots, x_n]$
    they generate over
$\mathbb{Z}$ is not equal to $K$. -/
theorem int_adjoin_range_ne_top {K : Type} [Field K] [NumberField K] {n : ℕ}
    (x : Fin n → K) :
    Algebra.adjoin ℤ (Set.range x) ≠ ⊤ := by
  sorry
```

Exercise (70). *Show that $\mathbb{Z}[x]/(x^2 + 4)$ is not integrally closed.*

```
import Mathlib

open Polynomial

/-- Show that $\mathbb{Z}[X]/(x^2+4)$ is not integrally closed. -/
theorem not_isIntegrallyClosed_adjoinRoot_pow_two_add_four :
    ¬ IsIntegrallyClosed (AdjoinRoot (X ^ 2 + C 4 : ℤ[X])) := by
  sorry
```

Exercise (71). *Prove that $k[x, y]$ is not a Dedekind ring.*

```
import Mathlib

```

```
open Polynomial

/-- Prove that $k[x,y]$ is not a Dedekind ring. -/
theorem not_isDedekindRing_mvPolynomial_fin_two {k : Type} [Field k] :
    ¬ IsDedekindRing (MvPolynomial (Fin 2) k) := by
  sorry
```

Exercise (72). *Let A be a ring such that for each maximal ideal $\mathfrak{m}$ of A, the local ring $A_{\mathfrak{m}}$ is Noetherian; and for each $x \neq 0$ in A, the set of maximal ideals of A which contain x is finite. Show that A is Noetherian.*

```
import Mathlib

/-- Let $A$ be a ring such that for each maximal ideal $\mathfrak{m}$ of $A$,
    the local ring
$A_{\mathfrak{m}}$ is Noetherian; and for each $x \neq 0$ in $A$, the set of
    maximal ideals of $A$
which contain $x$ is finite. Show that $A$ is Noetherian.-/
theorem isNoetherianRing_of_finite_isMaximal_and_mem {A : Type} [CommRing A]
    (h_local : ∀ (m : Ideal A), [m.IsMaximal] → IsNoetherianRing
    (Localization.AtPrime m))
    (h_finite : ∀ x : A, x ≠ 0 → Set.Finite {m : Ideal A | m.IsMaximal ∧ x ∈
    m}) :
    IsNoetherianRing A := by
  sorry
```

Exercise (73). *If R is a valuation ring, then an R-module A is flat if it is torsion-free.*

```
import Mathlib

/- If $R$ is a valuation ring, then an $R$-module $A$ is flat if it is
    torsion-free.-/
theorem flat_of_noZeroSMulDivisor {R A : Type} [CommRing R] [IsDomain R]
    [ValuationRing R] [AddCommGroup A]
    [Module R A] [NoZeroSMulDivisors R A] : Module.Flat R A := by
  sorry
```

Exercise (74). *If R is a valuation ring, then an R-module A is torision-free if it is flat.*

```lean
import Mathlib

/- If $R$ is a valuation ring, then an $R$-module $A$ is torsion-free if it is
    flat.-/
theorem noZeroSMulDivisors_of_flat {R A : Type} [CommRing R] [IsDomain R]
    [ValuationRing R] [AddCommGroup A]
    [Module R A] [Module.Flat R A] : NoZeroSMulDivisors R A := by
  sorry
```

Exercise (75). *Suppose A and B are commutative rings containing a field k, with B finitely generated over k as a ring. If $\varphi : A \to B$ is a ring homomorphism with $\varphi|_k = Id$ and if $Q \subset B$ is a maximal ideal, prove that $\varphi^{-1}(Q) \subset A$ is a maximal ideal.*

```lean
import Mathlib

/--Suppose \( A \) and \( B \) are commutative rings containing a field \( k
    \), with \( B \)
finitely generated over \( k \) as a ring. If \( \varphi : A \to B \) is a
    ring homomorphism with
\( \varphi|_k = \text{Id} \) and if \( Q \subset B \) is a maximal ideal,
    prove that \( \varphi^{-1}
(Q) \subset A \) is a maximal ideal.-/
theorem comap_isMaximal_of_finiteType {A B k : Type} [CommRing A] [CommRing B]
    [Field k] [Algebra k A] [Algebra k B]
    [Algebra.FiniteType k B] (φ : A →ₐ[k] B) (Q : Ideal B) [hQ : Q.IsMaximal] :
    (Ideal.comap φ Q).IsMaximal := by
  sorry
```

Exercise (76). *Show that a finite torsion-free module over a Dedekind domain is projective.*

```lean
import Mathlib

/- Show that a finite torsion-free module over a Dedekind domain is
    projective. -/
theorem projective_of_noZeroSMulDivisor {R M : Type} [CommRing R]
    [AddCommGroup M] [Module R M]
    [IsDedekindDomain R] [Module.Finite R M] [NoZeroSMulDivisors R M] :
    Module.Projective R M := by
```

```
  sorry
```

Exercise (77)**.** *Let k be a field, A a local k-algebra with maximal ideal $\mathfrak{m}$. Assume that A is a localization of a k-algebra R and that $A/\mathfrak{m} = k$. Prove that there exists maximal ideal $\mathfrak{n}$ of R with $R_{\mathfrak{n}} = A$.*

```
import Mathlib

/--Let \( k \) be a field, \( A \) a local \( k \)-algebra with maximal ideal
    \( \mathfrak{m} \).
Assume that \( A \) is a localization of a \( k \)-algebra \( R \) and that \(
    A / \mathfrak{m} = k
\). Prove that there exists maximal ideal \( \mathfrak{n} \) of \( R \) with
    \( R_{\mathfrak{n}} = A
\).-/
theorem exists_isMaximal_atPrime_of_bijective {k R A : Type} [Field k]
    [CommRing R] [CommRing A] [Algebra k R]
    [Algebra R A] [Algebra k A] [IsScalarTower k R A] [IsLocalRing A]
    (h : Function.Bijective <| (IsLocalRing.residue A).comp (algebraMap k A))
    (S : Submonoid R) [IsLocalization S A] :
    ∃ n : Ideal R, ∃ hn : n.IsMaximal, IsLocalization.AtPrime A n := by
  sorry
```

Exercise (78)**.** *Let R'/R be an integral extension of rings. Show that rad$(R) =$ rad$(R') \cap R$, where rad(R) denotes the nilpotent radical of R.*

```
import Mathlib

/--
Let \( R' / R \) be an integral extension of rings. Show that \( \text{rad}(R)
    = \text{rad}(R') \cap R \),
where $\text{rad}(R)$ denotes the nilpotent radical of $R$.-/
theorem nilpotent_eq_contraction_nilpotent_of_integral (R R' : Type) [CommRing
    R] [CommRing R']
    [Algebra R R'] (int : Algebra.IsIntegral R R') :
    nilradical R = Ideal.comap (algebraMap R R') (nilradical R') := by
  sorry
```

Exercise (79)**.** *Let R be a commutative ring. If all submodules of finitely generated free modules over R are free over R, then R is a PID.*

```
import Mathlib

/--Let \( R \) be a commutative ring. If all submodules of finitely generated
    free modules over
\( R \) are free over \( R \), then \( R \) is a PID.-/
theorem isPrincipalIdealRing_of_forall_free {R : Type} [CommRing R]
    (h : ∀ (M : Type) [AddCommGroup M] [Module R M] [Module.Finite R M]
    [Module.Free R M],
      ∀ (N : Submodule R M), Module.Free R N) :
    IsPrincipalIdealRing R := by
  sorry
```

Exercise (80)**.** *Let $R \subset R'$ be an extension of integral domains, and let $\overline{R}$ be the integral closure of R in R'. Show that for any two monic polynomials $f, g \in R'[t]$ with $f \cdot g \in R[t]$, we have $f, g \in \overline{R}[t]$.*

```
import Mathlib

open Polynomial

/--
Let \( R \subset R' \) be an extension of integral domains, and let \(
    \overline{R} \) be the integral closure of \( R \) in \( R' \).
Show that for any two monic polynomials \( f, g \in R'[t] \) with \( f \cdot g
    \in R[t] \),
we have \( f, g \in \overline{R}[t] \).-/
theorem mem_polynomial_integral_closure_of_prod_mem_polynomial (R S : Type)
    [CommRing R]
    [IsDomain R] [CommRing S] [IsDomain S] [Algebra R S] [NoZeroSMulDivisors R
    S] (f g : S[X])
    (mem : f * g ∈ lifts (algebraMap R S)) (hf : f.Monic) (hg : g.Monic) :
    f ∈ lifts (integralClosure R S).subtype ∧ g ∈ lifts (integralClosure R
    S).subtype := by
  sorry
```

Exercise (81)**.** *Let $R = \mathbb{C}[x_1, \ldots, x_n]/(x_1^2 + x_2^2 + \cdots + x_n^2)$. Then R is not a unique factorization domain for $n = 3$ or 4.*

```
import Mathlib

open MvPolynomial
/--
Let \( R = \mathbb{C}[x_1, \dots, x_n]/(x_1^2 + x_2^2 + \dots + x_n^2) \).
-/
abbrev R (n : ℕ) : Type :=
  MvPolynomial (Fin n) ℂ ⧸ Ideal.span {(∑ i : Fin n, X i ^ 2 : MvPolynomial
    (Fin n) ℂ)}

/--
Let \( R = \mathbb{C}[x_1, \dots, x_n]/(x_1^2 + x_2^2 + \dots + x_n^2) \).
Then \( R \) is not a unique factorization domain for \( n = 3 \) or \( 4 \).-/
theorem not_UFD_of_3_or_4 (n : ℕ) (h : n = 3 ∨ n = 4) [IsDomain (R n)] :
    ¬ UniqueFactorizationMonoid (R n) := by
  sorry
```

Exercise (82). *Let D be a unique factorization domain. Prove that if every nonzero prime ideal of D is maximal, then D is a principal ideal domain.*

```
import Mathlib

/--
Let \( D \) be a unique factorization domain.
Prove that if every nonzero prime ideal of \( D \) is maximal, then \( D \) is
    a principal ideal domain.
-/
theorem isPrincipalIdealRing_of_isPrime_ne_bot_isMaximal {D : Type} [CommRing
    D] [IsDomain D]
    [UniqueFactorizationMonoid D] (h : ∀ P : Ideal D, [P.IsPrime] → P ≠ ⊥ →
    P.IsMaximal) : IsPrincipalIdealRing D := by
  sorry
```

Exercise (83). *Let M be a finitely-generated module over a Dedekind domain. Prove that M is flat if and only if M is torsion-free.*

```
import Mathlib
```

```
/-- Let $M$ be a finitely-generated module over a Dedekind domain. Prove that $
    M$ is flat if and
only if $M$ is torsion-free. -/
theorem flat_iff_noZeroSMulDivisor {R M : Type} [CommRing R] [AddCommGroup M]
    [Module R M] [IsDedekindDomain R] [Module.Finite R M] :
    Module.Flat R M ↔ NoZeroSMulDivisors R M := by
  sorry
```

Exercise (84). *Let A be a Dedekind domain and $\mathfrak{a} \neq 0$ an ideal in A. Show that every ideal in $A/\mathfrak{a}$ is principal.*

```
import Mathlib


/-- Let $A$ be a Dedekind domain and $\mathfrak{a} \neq 0$ an ideal in $A$.
    Show that every ideal in
 $A/\mathfrak{a}$ is principal. -/
theorem isPrincipalIdealRing_quot_of_isDedekind {A : Type} [CommRing A]
    [IsDedekindDomain A] (a : Ideal A) (ha : a ≠ ⊥) :
    IsPrincipalIdealRing (A / a) := by
  sorry
```

Exercise (85). *Let A be a Noetherian ring and let $\mathfrak{a}, \mathfrak{b}$ be ideals in A. If M is any A-module, let $M_{\mathfrak{a}}$, $M_{\mathfrak{b}}$ denote its $\mathfrak{a}$-adic and $\mathfrak{b}$-adic completions respectively. If M is finitely generated, prove that $(M_{\mathfrak{a}})_{\mathfrak{b}} \cong M_{\mathfrak{a}+\mathfrak{b}}$.*

```
import Mathlib


open Submodule
open Finset
open Submodule

/-- Let $A$ be a Noetherian ring and let $\mathfrak{a}, \mathfrak{b}$ be
    ideals in $A$. If $M$ is
any $A$-module, let $M_{\mathfrak{a}}$, $M_{\mathfrak{b}}$ denote its $
    \mathfrak{a}$-adic and
```

```
$\mathfrak{b}$-adic completions respectively. If $M$ is finitely generated,
    prove that
$(M_{\mathfrak{a}})_{\mathfrak{b}} \cong M_{\mathfrak{a} + \mathfrak{b}}$. -/
theorem nonempty_adicCompletion_adicCompletion_linearEquiv {A M : Type}
    [CommRing A]
    [IsNoetherianRing A] (𝒜 : Ideal A) [AddCommGroup M]
    [Module A M] [Module.Finite A M] (ℬ : Ideal A) :
    Nonempty (AdicCompletion ℬ (AdicCompletion 𝒜 M) ≃ₗ[A] AdicCompletion (𝒜 +
    ℬ) M) := by
  sorry
```

Exercise (86). *Let M be an R-module. The following are equivalent:*

1. *M is finitely generated.*
2. *For every family $(Q_\alpha)_{\alpha \in A}$ of R-modules, the canonical map $M \otimes_R (\prod_\alpha Q_\alpha) \to \prod_\alpha (M \otimes_R Q_\alpha)$ is surjective.*

```
import Mathlib

/-- Let $M$ be an $R$-module. The following are equivalent:

\begin{enumerate}
    \item $M$ is finitely generated.
    \item For every family $(Q_{\alpha})_{\alpha \in A}$ of $R$-modules, the
    canonical map
    $M \otimes_{R} \left( \prod_{\alpha} Q_{\alpha} \right) \to \prod_{\alpha}
    (M \otimes_{R}
    Q_{\alpha})$ is surjective.
\end{enumerate} -/
theorem finite_iff_surjective_linearMap {R : Type} [CommRing R]
    (M : Type) [AddCommGroup M] [Module R M] :
    Module.Finite R M ↔ ∀ {α : Type} (Q : α → Type),
    ∀ [(a : α) → AddCommGroup (Q a)] [(a : α) → Module R (Q a)],
        Function.Surjective (LinearMap.pi (
            fun i => LinearMap.lTensor M (
                LinearMap.proj i (φ := Q) (R := R)))) := by
  sorry
```

Exercise (87). *If R is a valuation ring of Krull dimension 1 and K its field of fractions, then there does not exist any rings intermediate between R and K.*

```
import Mathlib

/-- If $R$ is a valuation ring of Krull dimension 1 and $K$ its field of
    fractions, then there do
not exist any rings intermediate between $R$ and $K$. -/
theorem eq_bot_or_eq_top_of_ringKrullDim_eq_one {R K : Type} [CommRing R]
    [IsDomain R]
    [Field K] [Algebra R K] [IsFractionRing R K] [ValuationRing R] (hD :
    ringKrullDim R = 1)
    (S : Subalgebra R K) : S = ⊥ ∨ S = ⊤ := by
  sorry
```

Exercise (88). *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let $x, y \in \mathfrak{m}$ be a regular sequence of length 2. For any $n \geq 2$ show that there do not exist $a, b \in R$ with*

$$x^{n-1}y^{n-1} = ax^n + by^n$$

```
import Mathlib

open RingTheory
/--Let \((R, \mathfrak{m})\) be a Noetherian local ring. Let \(x, y \in
    \mathfrak{m}\) be a regular
sequence of length \(2\). For any \(n \geq 2\) show that there do not exist
    \(a, b \in R\) with
\[
x^{n-1}y^{n-1} = a x^{n} + b y^{n}
\]-/
theorem not_exists_pow_sub_one_mul_pow_sub_one_eq {R : Type} [CommRing R]
    [IsNoetherianRing R]
    [IsLocalRing R] {n : ℕ} {x y : R} (hn : n ≥ 2) (hx : x ∈
    IsLocalRing.maximalIdeal R)
    (hy : y ∈ IsLocalRing.maximalIdeal R) (h : Sequence.IsRegular R [x, y]) :
    ¬ ∃ a b : R, x ^ (n - 1) * y ^ (n - 1) = a * x ^ n + b * y ^ n := by
  sorry
```

Exercise (89). *Let K be a field and L an extension field of K. If P is a prime ideal of $L[X_1, \dots, X_n]$ and $\mathfrak{p} = P \cap K[X_1, \dots, X_n]$, then* $\operatorname{ht}(P) \geq \operatorname{ht}(\mathfrak{p})$.

```
import Mathlib

open MvPolynomial
/--Let \( K \) be a field and \( L \) an extension field of \( K \). If \( P
    \) is a prime ideal of
\( L[X_1, \dots, X_n] \) and \( \mathfrak{p} = P \cap K[X_1, \dots, X_n] \),
    then \(
\operatorname{ht}(P) \geq \operatorname{ht}(\mathfrak{p}) \).-/
theorem primeHeight_le_of_comap_eq {K L : Type} (n : ℕ) [Field K] [Field L]
    [Algebra K L]
     (P : Ideal (MvPolynomial (Fin n) L)) (p : Ideal (MvPolynomial (Fin n) K))
    [P.IsPrime]
     [p.IsPrime] (h : P.comap (MvPolynomial.map (algebraMap K L)) = p) :
    p.primeHeight ≤ P.primeHeight := by
  sorry
```

Exercise (90). *Suppose that R is a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field κ. In this case the projective dimension of κ is* $\geq \dim_\kappa \mathfrak{m}/\mathfrak{m}^2$.

```
import Mathlib

/--
Suppose that \( R \) is a Noetherian local ring with maximal ideal \(
    \mathfrak{m} \) and residue field \( \kappa \).
In this case the projective dimension of \( \kappa \) is \( \geq \dim_{\kappa}
    \mathfrak{m} / \mathfrak{m}^{2} \).-/
theorem not_hasProjectiveDimensionLT_finrank_cotangentSpace {R : Type}
    [CommRing R] [IsLocalRing R]
     [IsNoetherianRing R] :
       ¬ CategoryTheory.HasProjectiveDimensionLT
        (ModuleCat.of R (IsLocalRing.ResidueField R))
          (Module.finrank (IsLocalRing.ResidueField R)
    (IsLocalRing.CotangentSpace R)) := by
  sorry
```

Exercise (91)**.** *If a ring R, not a field, is a maximal proper subring of a field K, show R is a valuation ring of Krull dimension 1.*

```
import Mathlib

/--If a ring \( R \), not a field, is a maximal proper subring of a field \( K
    \), show \( R \) is
a valuation ring of Krull dimension 1.-/
theorem exists_toSubring_eq_and_ringKrullDim_eq_one {K : Type} [Field K] (R :
    Subring K)
     (h : IsCoatom R) (hR : ¬ IsField R) :
     (∃ V : ValuationSubring K, V.toSubring = R) ∧ ringKrullDim R = 1 := by
  sorry
```

Exercise (92)**.** *Let R be a Dedekind domain. Show the following:*

If $P_1, \dots, P_n \in \operatorname{Spec}(R)$ are pairwise distinct, non-zero prime ideals and $e_1, \dots, e_n$ are non-negative integers, there exists $a \in R \setminus \{0\}$ such that

$$(a) = P_1^{e_1} \cdots P_n^{e_n} \cdot J,$$

with $J \subseteq R$ an ideal in whose factorization none of the P_i appear.

```
import Mathlib

/--
Let \( R \) be a Dedekind domain. Show the following:

If \( P_1, \dots, P_n \in \operatorname{Spec}(R) \) are pairwise distinct,
    non-zero prime ideals
and \( e_1, \dots, e_n \) are non-negative integers, there exists \( a \in R
    \setminus \{0\} \) such that
\[
(a) = P_1^{e_1} \cdots P_n^{e_n} \cdot J,
\]
with \( J \subseteq R \) an ideal in whose factorization none of the \( P_i \)
    appear.
-/
theorem exists_factor_principal_ideal (R : Type) [CommRing R]
    [IsDedekindDomain R]
```

```
    (n : ℕ) (p : (Fin n) → PrimeSpectrum R) (h_nonzero : ∀ i, (p i).asIdeal ≠
    ⊥)
    (h_inj : Function.Injective p) (e : (Fin n) → ℕ) :
    ∃ (a : R) (J : Ideal R), a ≠ 0 ∧ Ideal.span {a} = J * ∏ (i : Fin n), (p
    i).1 ^ (e i) ∧
    (∀ (i : Fin n), ¬ ∃ (K : Ideal R), J = K * (p i).1) := by
  sorry
```

Exercise (93). *Let $\mathscr{O}$ be an integral domain in which all nonzero ideals admit a unique factorization into prime ideals. Show that $\mathscr{O}$ is a Dedekind domain.*

```
import Mathlib

/--
Let $\mathcal{O}$ be an integral domain in which all nonzero ideals admit a
    unique factorization into prime ideals.
Show that $\mathcal{O}$ is a Dedekind domain. -/
theorem isDedekindDomain_of_ideal_UFD (O : Type) [CommRing O] [IsDomain O]
    [CancelCommMonoidWithZero (Ideal O)] [UniqueFactorizationMonoid (Ideal O)]
    :
    IsDedekindDomain O := by
  sorry
```

Exercise (94). *Suppose that a ring S is integral over the image of a ring homomorphism $R \to S$. Show that the Krull dimension of M as an S-module is the same as the Krull dimension of M as an R-module.*

```
import Mathlib

/-- Suppose that a ring $S$ is integral over the image of a ring homomorphism $
    R \to S$. Show that
the Krull dimension of $M$ as an $S$-module is the same as the Krull dimension
    of $M$ as an
$R$-module. -/
theorem ringKrullDim_quot_annihilator_eq {R S M : Type} [CommRing R] [CommRing
    S] [AddCommGroup M] [Algebra R S]
    [Module S M] [Module R M] [IsScalarTower R S M] [Algebra.IsIntegral R S] :
    ringKrullDim (S / (Module.annihilator S M)) = ringKrullDim (R /
    (Module.annihilator R M)) := by
```

```
  sorry
```

Exercise (95). *Show that if $x_1, \dots, x_r$ is a regular sequence in R, then so is $x_1^{a_1}, \dots, x_r^{a_r}$ for any positive integers $a_1, \dots, a_r$.*

```
import Mathlib

open RingTheory

/-- Show that if $x_1, \dots, x_r$ is a regular sequence in $R$,
then so is $x_1^{a_1}, \dots, x_r^{a_r}$ for any positive integers $a_1,
    \dots, a_r$. -/
theorem isRegular_ofFn_pow (R M : Type) [CommRing R] [AddCommGroup M] [Module
    R M]
     (rs : List R) (a : Fin rs.length → ℕ+) (h : Sequence.IsRegular M rs) :
     Sequence.IsRegular M (List.ofFn (fun i => rs[i] ^ (a i).1)) := by
  sorry
```

Exercise (96). *Let $I_1, I_2 \subseteq K[x_1, \dots, x_n]$ be two ideals. With y an additional indeterminate, form the ideal*

$$J := \big(y \cdot I_1 \cup (1-y) \cdot I_2\big) K[x_1, \dots, x_n, y] \subseteq K[x_1, \dots, x_n, y].$$

Show that

$$I_1 \cap I_2 = K[x_1, \dots, x_n] \cap J.$$

```
import Mathlib

open Polynomial
/--Let \( I_1, I_2 \subseteq K[x_1, \dots, x_n] \) be two ideals. With \( y \)
    an additional
indeterminate, form the ideal
\[
J := \big( y \cdot I_1 \cup (1 - y) \cdot I_2 \big) K[x_1, \dots, x_n, y]
    \subseteq K[x_1, \dots,
x_n, y].
\]Show that
\[
I_1 \cap I_2 = K[x_1, \dots, x_n] \cap J.
\]-/
```

```
theorem inf_eq_span_X_smul_sup_one_sub_X_smul_comap_C {K : Type} [Field K] (n
    : ℕ)
    (I1 I2 : Ideal (MvPolynomial (Fin n) K)) :
    I1 ⊓ I2 = (Ideal.span {(X : (MvPolynomial (Fin n) K)[X])} • (I1.map C) ⊔
    Ideal.span {(1 - X : (MvPolynomial (Fin n) K)[X])} • (I2.map C) ).comap C
    := by
  sorry
```

Exercise (97). *Prove that* $\sin 1^\circ$ *is algebraic over* $\mathbb{Q}$*.*

```
import Mathlib

open Real

/- Prove that $\sin 1^{\circ}$ is algebraic over $\mathbb{Q}$.-/
theorem isAlgebraic_sin_pi_div_180 : IsAlgebraic ℚ (sin (π / 180)) := by
  sorry
```

Exercise (98). *Let* A *be a Noetherian ring, and suppose that* P *is a height* $r > 0$ *prime ideal generated by* r *elements, which may* ***not*** *be a regular sequence. Show that* P *can be generated by an* A*-sequence.*

```
import Mathlib

open RingTheory
/--Let \( A \) be a Noetherian ring, and suppose that \( P \) is a height \( r
    > 0 \) prime ideal
generated by \( r \) elements, which may **not** be a regular sequence. Show
    that \( P \) can be
generated by an \( A \)-sequence.-/
theorem exists_isRegular_and_eq_ofList {A : Type} [CommRing A]
    [IsNoetherianRing A] (P : Ideal A) [P.IsPrime] (r : ℕ)
    (hr : 0 < r) (h : r = P.primeHeight) (a : Fin r → A) (hP : P = Ideal.span
    (Set.range a)) :
    ∃ b : List A, Sequence.IsRegular A b ∧ P = Ideal.ofList b := by
  sorry
```

Exercise (99). *For a commutative ring* R *and* $n \in \mathbb{N}$ *such that* 2 *is invertible in* R*. If* $A \in SO(2n+1, R)$*, then* $det(I - A) = 0$*.*

```
import Mathlib

/--
For a commutative ring \(R\) and \(n \in \mathbb{N}\) such that \(2\) is
    invertible in \(R\).
If \(A \in SO(2n + 1,  R)\), then \(det(I - A) = 0\).-/
theorem determinant_eq_zero (R : Type) [CommRing R] (n : ℕ) (h2_inv : IsUnit
    (2 : R))
    (A : Matrix.specialOrthogonalGroup (Fin (2 * n + 1)) R) : (1 - A.1).det =
    0 := by
  sorry
```

Exercise (100). *There exists a commutative ring with finite prime spectrum but is not Noetherian.*

```
import Mathlib

/--
There exists a commutative ring with finite prime spectrum but is not
    Noetherian.
-/
theorem exists_finite_primeSpectrum_not_isNoetherianRing :
    ∃ (R : Type) (_ : CommRing R), Finite (PrimeSpectrum R) ∧ ¬
    IsNoetherianRing R := by
  sorry
```