FATE-X Statements

Formalization Contribution

Nailin Guan 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)**.** *Let R be a UFD with two nonassociate prime elements p and q such that every prime element is an associate of either p or q. Prove that R is a PID.*

```
import Mathlib

namespace Problem1

/--
Let $R$ be a UFD with two nonassociate prime elements $p$ and $q$ such that every prime
element is an associate of either $p$ or $q$. Prove that $R$ is a PID.
-/
theorem isPrincipalIdealRing_of_associated_or_associated {R : Type} [CommRing R] [IsDomain R]
    [UniqueFactorizationMonoid R] {p q : R} (hp : Prime p) (hq : Prime q) (hpq : ¬ Associated p q)
    (h : ∀ {x : R}, Prime x → Associated x p ∨ Associated x q) :
    IsPrincipalIdealRing R := by
  sorry

end Problem1
```

Exercise (2)**.** *Let G be a finite group and L a maximal subgroup of G. Suppose L is non-Abelian and simple. Then there exist at most two minimal normal subgroups in G.*

```
import Mathlib

namespace Problem2

```

```
/--
Let $G$ be a finite group and $L$ a maximal subgroup of $G$. Suppose $L$ is non-Abelian and simple.
Then there exist at most two minimal normal subgroups in $G$.
-/
theorem card_minimal_normal_subgroup_le_2 (G : Type) [Group G] [Finite G]
    (L : Subgroup G) (h_ne_top : L ≠ ⊤) (h_maximal : IsMax (⟨L, h_ne_top⟩ : {H : Subgroup G // H ≠
    ⊤}))
    (h_simple : IsSimpleGroup L) (h_non_comm : ∃ (x y : L), x * y ≠ y * x) :
    {H : {H : Subgroup G // H.Normal} | IsMin H}.ncard ≤ 2 := by
  sorry

end Problem2
```

Exercise (3). *Let H be a subgroup of finite index of a group G. Show that there exists a subset S of G, such that S is both a set of representatives of the left and the right cosets of H in G.*

```
import Mathlib

namespace Problem3

/--
Let $H$ be a subgroup of finite index of a group $G$. Show that there exists a subset $S$ of $G$,
such that $S$ is both a set of representatives of the left and the right cosets of $H$ in $G$.
-/
theorem exists_leftCoset_rightCoset_representative
    (G : Type) [Group G] (H : Subgroup G) [H.FiniteIndex] :
    ∃ S : Set G, Subgroup.IsComplement S H ∧ Subgroup.IsComplement H S := by
  sorry

end Problem3
```

Exercise (4). *Let p be an odd prime number, and let G be a finite group of order $p(p+1)$. Assume that G does not have a normal Sylow p-subgroup. Prove that $p+1$ is a power of 2.*

```
import Mathlib

namespace Problem4

/--
Let $p$ be an odd prime number, and let $G$ be a finite group of order $p(p + 1)$. Assume that $G$
does not have a normal Sylow $p$-subgroup. Prove that $p + 1$ is a power of $2$.
-/
theorem add_one_eq_two_pow_of_sylow_subgroup_not_normal (p : ℕ) (h_odd : Odd p) (G : Type)
    (hp : p.Prime) [Finite G] [Group G] (h_card : Nat.card G = p * (p + 1))
    (h_sylow : ∀ (H : Sylow p G), ¬ H.Normal) : ∃ (n : ℕ), p + 1 = 2 ^ n := by
  sorry

end Problem4
```

Exercise (5). *Let p be a prime, let G be a finite p-group. Let A be a maximal normal abelian subgroup of G. Prove that A is also a maximal abelian subgroup of G.*

```
import Mathlib

namespace Problem5

/--
Let \(p\) be a prime, let \(G\) be a finite p-group. Let A be a maximal normal abelian subgroup
of \(G\). Prove that A is also a maximal abelian subgroup of \(G\).
-/
theorem maximal_abelian_normal_subgroup_of_p_group_is_maximal_abelian_subgroup
    (p : ℕ) (hp : p.Prime) (G : Type) [Group G] [Finite G] (h_pgroup : IsPGroup p G)
    (H : Subgroup G) (h_normal : H.Normal) (h_comm : IsMulCommutative H)
    (h_maximal_normal_abelian : ∀ (K : Subgroup G), K.Normal → IsMulCommutative K → H ≤ K → H = K) :
    ∀ (K : Subgroup G), IsMulCommutative K → H ≤ K → H = K := by
  sorry

end Problem5
```

Exercise (6). *Prove that if $\#G = 396$ then G is not simple.*

```
import Mathlib

namespace Problem6

/--
Prove that if $\#G = 396$ then $G$ is not simple.
-/
theorem not_isSimpleGroup_of_card_eq_396 (G : Type) [Group G]
    [Finite G] (h_card : Nat.card G = 396) : ¬ IsSimpleGroup G := by
  sorry

end Problem6
```

Exercise (7). *Prove that if $\#G = 1785$ then G is not simple.*

```
import Mathlib

namespace Problem7

/--
Prove that if $\#G = 1785$ then $G$ is not simple.
-/
theorem not_isSimpleGroup_of_card_eq_1785 (G : Type) [Group G]
    [Finite G] (h_card : Nat.card G = 1785) : ¬ IsSimpleGroup G := by
  sorry

end Problem7
```

Exercise (8)**.** *Let $A, B \in \mathbb{Q}^\times$ be rational numbers. Consider the quaternion ring*

$$D_{A,B,\mathbb{R}} = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mid a, b, c, d \in \mathbb{R}\}$$

in which the multiplication satisfies relations: $\boldsymbol{i}^2 = A$, $\boldsymbol{j}^2 = B$, and $\boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}$.

Show that $D_{A,B,\mathbb{R}}$ is either isomorphic to $\mathbb{H}$ (Hamilton quaternion) or isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ as $\mathbb{R}$-algebras.

```
import Mathlib

namespace Problem8

open Quaternion

/--
Let $A, B \in \mathbb{Q}^\times$ be rational numbers. Consider the quaternion ring
$$
D_{A, B, \mathbb{R}} = \{a+b\boldsymbol{i} +c\boldsymbol{j}+d\boldsymbol{k}\;|\; a,b,c,d \in
\mathbb{R}\}$$
in which the multiplication satisfies relations: $\boldsymbol{i}^2 = A$, $\boldsymbol{j}^ 2 = B$,
and $\boldsymbol{i}\boldsymbol{j}= -\boldsymbol{j}\boldsymbol{i} = \boldsymbol{k}$.
Show that $D_{A, B, \mathbb{R}}$ is either isomorphic to $\mathbb{H}$ (Hamilton quaternion) or
isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ as $\mathbb{R}$-algebras.
-/
theorem quaternionAlgebra_isomorphic_to_matrix_ring_or_quaternion_ring
    (A B : ℚ) (ha : A ≠ 0) (hb : B ≠ 0) :
    ((Nonempty (ℍ[ℝ, A, B] ≃ₐ[ℝ] ℍ[ℝ, -1, -1])) ∨ (Nonempty (ℍ[ℝ, A, B] ≃ₐ[ℝ] Matrix (Fin 2) (Fin 2)
     ℝ)))
    ∧ IsEmpty (Matrix (Fin 2) (Fin 2) ℝ ≃ₐ[ℝ] ℍ[ℝ, -1, -1]) := by
  sorry

end Problem8
```

Exercise (9)**.** *Let G be a finite group and let $\mathrm{Syl}_p(G)$ denote its set of Sylow p-subgroups. Suppose that S and T are distinct members of $\mathrm{Syl}_p(G)$ chosen so that $\#(S \cap T)$ is maximal among all such intersections. Prove that the normalizer $N_G(S \cap T)$ does not admit normal Sylow p-subgroup.*

```
import Mathlib

namespace Problem9

/--
Let $G$ be a finite group and let $\mathrm{Syl}_p(G)$ denote its set of Sylow $p$-subgroups.
Suppose that $S$ and $T$ are distinct members of
$\mathrm{Syl}_p(G)$ chosen so that $\#(S \cap T)$ is maximal
among all such intersections. Prove that the normalizer $N_G(S \cap  T)$ does not admit normal
Sylow $p$-subgroup.
-/
theorem sylow_subgroup_not_normal_of_maximal_intersection (G : Type) [Finite G] [Group G]
```

```
    (p : ℕ) [Fact (Nat.Prime p)] (S T : Sylow p G) (h_ne : S ≠ T)
    (h_maximal : ∀ (S' T' : Sylow p G), S' ≠ T' →
    ((S' : Set G) ⊓ T').ncard ≤ ((S : Set G) ⊓ T).ncard) :
    ∀ (P : Sylow p ((S : Subgroup G) ⊓ T).normalizer), ¬ P.Normal := by
  sorry

end Problem9
```

Exercise (10). *Let $A = \mathbb{R}[X,Y]/(X^2+Y^2+1)$. Then it is a principal ideal domain.*

```
import Mathlib

namespace Problem10

/--
Let \( A = \mathbb{R}[X, Y]/(X^2 + Y^2 + 1) \). Then it is a principal ideal domain.
-/
theorem isPrincipalIdealRing_quot_X_pow_two_plus_Y_pow_two_plus_one :
    IsPrincipalIdealRing ((MvPolynomial (Fin 2) ℝ) /
    Ideal.span {(.X 0 ^ 2 + .X 1 ^ 2 + .C 1 : (MvPolynomial (Fin 2) ℝ))}) := by
  sorry

end Problem10
```

Exercise (11). *Let $A = \mathbb{R}[X,Y]/(X^2+Y^2+1)$. Then it is not a Euclidean domain.*

```
import Mathlib

namespace Problem11

/--
Definition of a Euclidean norm taking value in \(\mathbb{N}\).
-/
class EuclideanNormNat (R : Type) [CommRing R] extends Nontrivial R where
  quotient : R → R → R
  quotient_zero : ∀ a, quotient a 0 = 0
  remainder : R → R → R
  quotient_mul_add_remainder_eq : ∀ a b, b * quotient a b + remainder a b = a
  norm : R → ℕ
  remainder_lt : ∀ (a) {b}, b ≠ 0 → norm (remainder a b) < norm b
  mul_left_not_lt : ∀ (a) {b}, b ≠ 0 → ¬ norm (a * b) < norm a

/--
Let \( A = \mathbb{R}[X, Y]/(X^2 + Y^2 + 1) \). Then it is not a Euclidean domain.
-/
theorem not_isomorphic_euclideanDomain : IsEmpty <| EuclideanNormNat (((MvPolynomial (Fin 2) ℝ) /
    Ideal.span {(.X 0 ^ 2 + .X 1 ^ 2 + .C 1: MvPolynomial (Fin 2) ℝ)})) := by
  sorry

end Problem11
```

Exercise (12). *Prove that the ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a principal ideal domain.*

```
import Mathlib

namespace Problem12

/--
Prove that the ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a principal ideal domain.
-/
theorem isPrincipalIdealRing_of_quadratic_integer_19 :
    IsPrincipalIdealRing (Algebra.adjoin ℤ {(1 + (Real.sqrt 19) * Complex.I) / 2}) ∧ IsDomain
     (Algebra.adjoin ℤ {(1 + (Real.sqrt 19) * Complex.I) / 2}) := by
  sorry

end Problem12
```

Exercise (13). *Let $(R,+,\cdot)$ be a (not necessarily commutative) ring. If we know that R is not a field and $x^2 = x$ for any $x \in R$, where x is not invertible. Prove that $x^2 = x$ for any x.*

```
import Mathlib

namespace Problem13

/--
Let $(R,+,\cdot)$ be a (not necessarily commutative) ring.
If we know that $R$ is not a field and $x^2=x$ for any $x\in R,$
where $x$ is not invertible. Prove that $x^2=x$ for any $x.$
-/
theorem sq_eq_self_of_not_unit {R : Type} [Ring R] (h : ¬ IsField R)
    (h2 : ∀ x : R, ¬ IsUnit x → x^2 = x) (x : R) : x^2 = x := by
  sorry

end Problem13
```

Exercise (14). *Show that if R is a unique factorization domain such that the quotient field of R is isomorphic to $\mathbb{R}$, then R is isomorphic to $\mathbb{R}$.*

```
import Mathlib

namespace Problem14

/--
Show that if $R$ is a unique factorization domain such that the quotient field of $R$ is isomorphic
to $\mathbb{R}$, then R is isomorphic to $\mathbb{R}$.
-/
theorem isomorphic_real_of_fractionRing_isomorphic_real_of_UFD (R : Type) [CommRing R] [IsDomain R]
    [UniqueFactorizationMonoid R] (h : Nonempty ((FractionRing R) ≃+* ℝ)) :
    Nonempty (R ≃+* ℝ) := by
  sorry
```

```
end Problem14
```

Exercise (15). *Let p, q, r be three distinct prime numbers, t a positive integer. Let G be a finite group, H a normal subgroup of G such that the cardinality of G/H is r^t. Suppose that there exists a composition series*

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H,$$

of H that satisfies $n = 2$, $H_1/H_0 = \mathbb{Z}/p\mathbb{Z}$, $H_2/H_1 = \mathbb{Z}/q\mathbb{Z}$. Further suppose that there exists a composition series

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G,$$

and positive integers $i < j \leq n$ such that $G_i/G_{i-1} = \mathbb{Z}/q\mathbb{Z}$, $G_j/G_{j-1} = \mathbb{Z}/p\mathbb{Z}$. Show that there exists a composition series

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H,$$

of H that satisfies $n = 2$, $H_1/H_0 = \mathbb{Z}/q\mathbb{Z}$, $H_2/H_1 = \mathbb{Z}/p\mathbb{Z}$.

```
import Mathlib

namespace Problem15

/--
A subgroup `H₁` is a maximal normal subgroup of `H₂` if it is contained in `H₂`,
and `H₁` is maximal normal in `H₂`.
-/
structure Subgroup.IsMaximalNormal {G : Type} [Group G] (H₁ H₂ : Subgroup G) : Prop where
  le : H₁ ≤ H₂
  subgroupOf_normal : (H₁.subgroupOf H₂).Normal
  is_maximal : ∀ H : Subgroup G, H₁ ≤ H → H ≤ H₂ → (H.subgroupOf H₂).Normal → (H = H₁ ∨ H = H₂)

def Subgroup.IsMaximalNormal.setRel {G : Type} [Group G] : SetRel (Subgroup G) (Subgroup G) :=
  fun (H₁, H₂) ↦ Subgroup.IsMaximalNormal H₁ H₂

/--
A normal subgroup composition series of a group `G` is a *maximal* finite chain of normal subgroups
\[
\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G
\]
such that each quotient `G_{i+1}/G_i` is a simple group.
-/
structure NormalSubgroupCompositionSeries (G : Type) [Group G] : Type where
  toRelSeries : RelSeries (Subgroup.IsMaximalNormal.setRel (G := G))
  maximal : ∀ s : RelSeries (Subgroup.IsMaximalNormal.setRel (G := G)),
      s.length ≤ toRelSeries.length

/--
The \(i\)-th factor of a normal subgroup composition series, which is the quotient of the
```

```
\(i + 1\)-th subgroup by the previous one.
-/
def StepwiseQuotient {G : Type} [Group G] (s : NormalSubgroupCompositionSeries G)
    (i : Fin s.toRelSeries.length) : Type :=
  s.toRelSeries i.succ / (s.toRelSeries i.castSucc).subgroupOf _

/--
The \(i\)-th factor of a normal subgroup composition series is a group.
-/
instance {G : Type} [Group G] (s : NormalSubgroupCompositionSeries G)
    (i : Fin s.toRelSeries.length) : Group (StepwiseQuotient s i) :=
  QuotientGroup.Quotient.group _ (nN := (s.toRelSeries.step i).subgroupOf_normal)

/--
Let $p,q,r$ be three distinct prime numbers, $t$ a positive integer. Let $G$ be a finite group,
$H$ a normal subgroup of $G$ such that the cardinality of $G/H$ is $r^{t}$.
Suppose that there exists a composition series
\[
\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H,
\]
of $H$ that satisfies $n=2$, $H_1/H_0 = \mathbb{Z}/p\mathbb{Z}$,
$H_2/H_1 = \mathbb{Z}/q\mathbb{Z}$. Further suppose that there exists a composition series
\[
\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G,
\]
and positive integers $i < j\leq n$ such that $G_{i}/G_{i-1} = \mathbb{Z}/q\mathbb{Z}$,
$G_{j}/G_{j-1} = \mathbb{Z}/p\mathbb{Z}$. Show that there exists a composition series
\[
\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H,
\]
of $H$ that satisfies $n=2$, $H_1/H_0 = \mathbb{Z}/q\mathbb{Z}$,
$H_2/H_1 = \mathbb{Z}/p\mathbb{Z}$.
-/
theorem exists_swap_stepwiseQuotient {p q r t : ℕ} (hp : p.Prime) (hq : q.Prime) (hr : r.Prime)
    (ht : 0 < t) (G : Type) [Group G] [Fintype G] (H : Subgroup G) [H.Normal]
    (hH : Nat.card (G / H) = r ^ t) (Hs : NormalSubgroupCompositionSeries H)
    (hHs: Hs.toRelSeries.length = 2) (hHs0 : StepwiseQuotient Hs ⟨0, by omega⟩ ≃* ZMod p)
    (hHs1 : StepwiseQuotient Hs ⟨1, by omega⟩ ≃* ZMod q)
    (Gs : NormalSubgroupCompositionSeries G) (i j : Fin Gs.toRelSeries.length) (hij : i < j)
    (hGi : StepwiseQuotient Gs i ≃* ZMod q) (hGj : StepwiseQuotient Gs j ≃* ZMod p) :
    ∃ (Hs' : NormalSubgroupCompositionSeries H) (hlen : Hs'.toRelSeries.length = 2),
    Nonempty (StepwiseQuotient Hs' ⟨0, by omega⟩  ≃* ZMod q) ∧
    Nonempty (StepwiseQuotient Hs' ⟨1, by omega⟩  ≃* ZMod p) := by
  sorry

end Problem15
```

Exercise (16)**.** *Let p be a prime and let F be a field. Let K be a finite Galois extension of F whose Galois group is a p-group (i.e., the degree $[K : F]$ is a power of p). Such an extension is called a* p-extension *(note that p-extensions are Galois by definition). Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.*

```lean
import Mathlib

namespace Problem16

/--
A Galois extension such that the degree of the extension is a power of a prime \( p \) is
called a p-extension.
-/
class IsPExtension (F E : Type) [Field F] [Field E] [Algebra F E]
    (p : ℕ) : Prop extends IsGalois F E where
    rank_eq_pow : ∃ (n : ℕ), Module.rank F E = p ^ n

/--
Let $p$ be a prime and let $F$ be a field.
Let $K$ be a finite Galois extension of $F$ whose Galois group is a $p$-group (i.e., the degree
$[K : F]$ is a power of $p$). Such an extension is called a \emph{$p$-extension} (note that
$p$-extensions are Galois by definition). Let $L$ be a $p$-extension of $K$. Prove that the
Galois closure of $L$ over $F$ is a $p$-extension of $F$.
-/
theorem normalClosure_isPExtension_of_isPExtension (F E : Type) [Field F] [Field E]
    [Algebra F E] (L : IntermediateField F E) (K : IntermediateField F L) (p : ℕ) (hp : p.Prime)
    [IsPExtension F K p] [IsGalois K L] [IsPExtension K L p]
    (h_normalClosure : IsNormalClosure F L E) : IsPExtension F E p := by
  sorry

end Problem16
```

Exercise (17). *Let K be a subfield of $\mathbb{C}$ maximal with respect to the property that $\sqrt{2} \notin K$. Deduce that $[\mathbb{C} : K]$ is countable (and not finite).*

```lean
import Mathlib

namespace Problem17

/--
Let $K$ be a subfield of $\mathbb{C}$ maximal with respect to the property that $\sqrt 2 \notin K$.
Deduce that $[\mathbb{C} : K]$ is countable (and not finite).
-/
theorem countable_index_of_maximal_subfield_sqrt_2_nmem
    (K : Subfield ℂ) (h_nmem : (Real.sqrt 2 : ℂ) ∉ K)
    (h : ∀ (L : Subfield ℂ), K ≤ L → (Real.sqrt 2 : ℂ) ∉ L → K = L) :
    Module.rank K ℂ = Cardinal.aleph0 := by
  sorry

end Problem17
```

Exercise (18). *Let E be a subfield of $\mathbb{R}$ and let K/E be a finite Galois extension of odd degree > 1. Prove that K cannot be E-embedded into a radical tower that is a subfield of $\mathbb{R}$.*

```
import Mathlib

namespace Problem18

/--
Let \( E \) be a commutative ring, \( F \) be an \( E \)-algebra, then we say \( F \) is
a radical extension over \( E \), if \( F \) is generated by a single element \( x \in F \)
over \( E \) such that \( x ^ n - e = 0 \) for some \( e \in E \).
-/
def IsRadicalExtension (E F : Type) [CommRing E] [CommRing F] [Algebra E F] : Prop :=
    ∃ (x : F), Algebra.adjoin E {x} = ⊤ ∧ (∃ (n : ℕ) (e : E), n ≥ 1 ∧ x ^ n - (algebraMap E F) e =
     0)

/--
An algebra is said to be a radical tower over the base ring if it can be written as
composition of radical extensions.
-/
inductive IsRadicalTower : ∀ (E : Type) (F : Type) [CommRing E] [CommRing F] [Algebra E F], Prop
  | of_isRadicalExtension (E : Type) (F : Type)
      [CommRing E] [CommRing F] [Algebra E F] : IsRadicalExtension E F → IsRadicalTower E F
  | of_composition (E : Type) (F : Type) [CommRing E] [CommRing F] [Algebra E F] (F' : Subalgebra E
     F) :
      IsRadicalExtension F' F → IsRadicalTower E F' → IsRadicalTower E F

/--
Let \( E \) be a subfield of \( \mathbb{R} \) and let \( K/E \) be a finite Galois extension of
odd degree \( > 1 \). Prove that \( K \) cannot be \( E \)-embedded into a radical tower that is
a subfield of \( \mathbb{R} \).
-/
theorem isEmpty_embedding_intermediateField_of_odd_degree_galois (E : Subfield ℝ) (K : Type)
    [Field K] [Algebra E K] [IsGalois E K] (n : ℕ) (h_odd : Odd n) (hn : n > 1) (h_deg_eq :
     Module.rank E K = n)
    (K' : IntermediateField E ℝ) (h_radical : IsRadicalTower E K') :
    IsEmpty (K →ₐ[E] K') := by
  sorry

end Problem18
```

Exercise (19). *Let* $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ *and consider the extension* $E = \mathbb{Q}(\alpha)$. *Show that* $\mathrm{Gal}(E/\mathbb{Q}) \cong Q_8$, *the quaternion group of order* 8.

```
import Mathlib

namespace Problem19

/--
Let $E$ denote the algebra $\mathbb{Q}(\sqrt{(2+\sqrt 2)(3+\sqrt 3)})
-/
abbrev E : Type := (Algebra.adjoin ℚ {Real.sqrt ((2 + Real.sqrt 2) * (3 + Real.sqrt 3))})

/--
```

```
Let $\alpha = \sqrt{(2+\sqrt 2)(3+\sqrt 3)}$ and consider the extension $E =\mathbb{Q}(\alpha)$.
Show that $\mathrm{Gal}(E/\mathbb{Q}) \cong Q_8$, the quaternion group of order $8$.
-/
theorem galoisGroup_iso_quaternion_group : Nonempty ((E ≃ₐ[ℚ] E) ≃* (QuaternionGroup 2)) := by
  sorry

end Problem19
```

Exercise (20). *Let p be a prime number. Let L/K be a finite extension of fields of characteristic p, and let $\sigma : x \mapsto x^p$ denote the p-Frobenius endomorphism on L, which of course stabilizes K. Prove that if $[L : K\sigma(L)] \leq p$, then L/K can be generated by one element.*

```
import Mathlib

namespace Problem20

/--
Let $p$ be a prime number. Let $L/K$ be a finite extension of fields of characteristic $p$,
and let $\sigma:x\mapsto x^p$ denote the $p$-Frobenius endomorphism on $L$, which of course
stabilizes $K$. Prove that if $[L:K\sigma(L)] \leq p$, then $L/K$ can be generated by one element.
-/
theorem generated_single_elem_of_degree_le_p (p : ℕ) [Fact (Nat.Prime p)]
    (K L : Type) [Field K] [Field L] [CharP L p] [Algebra K L] [FiniteDimensional K L]
    (h : Module.rank (IntermediateField.adjoin K ((frobenius L p).range : Set L)) L ≤ p) :
    ∃ (x : L), IntermediateField.adjoin K {x} = ⊤ := by
  sorry

end Problem20
```

Exercise (21). *Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial. Suppose that K is a splitting field for $f(x)$ over F and assume that there exists an element $\alpha \in K$ such that both α and $\alpha + 1$ are roots of $f(x)$. Prove that there exists an intermediate field E between K and F such that $[K : E]$ is equal to the characteristic of F. (In particular, the characteristic of F is not zero)*

```
import Mathlib

namespace Problem21

open Polynomial

/--
Let $F$ be a field and let $f(x) \in F[x]$ be an irreducible polynomial.
Suppose that $K$ is a splitting field for $f(x)$ over $F$ and assume that there exists an element
$\alpha \in K$ such that both $\alpha$ and $\alpha+1$ are roots of $f(x)$.
Prove that there exists an intermediate field $E$ between $K$ and $F$ such that $[K:E]$
is equal to the characteristic of $F$. (In particular, the characteristic of $F$ is not zero)
-/
```

```
theorem intermediateField_rank_eq_ringChar (F : Type) [Field F] (f : Polynomial F) (hf : Irreducible
     f)
    (K : Type) [Field K] [Algebra F K] (hK : f.IsSplittingField F K) (α : K)
    (hα : f.aeval α = 0) (hα1 : f.aeval (α + 1) = 0) :
    ∃ (E : IntermediateField F K), Module.rank E K = ringChar F := by
  sorry

end Problem21
```

Exercise (22). *Let F be a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, where $F/\mathbb{Q}$ is a finite* abelian *Galois extension. Prove that F contains only finitely many algebraic integers (i.e. elements in F whose minimal polynomial over $\mathbb{Q}$ have coefficients in $\mathbb{Z}$) having absolute value 1, and each of the algebraic integers is a root of unity.*

```
import Mathlib

namespace Problem22

/--
Let $F$ be a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, where $F/\mathbb{Q}$
is a finite \emph{abelian} Galois extension. Prove that $F$ contains only finitely many algebraic
integers (i.e. elements in $F$ whose minimal polynomial over $\mathbb{Q}$ have coefficients in
$\mathbb{Z}$) having absolute value $1$, and each of the algebraic integers is a root of unity.
-/
theorem finite_algebraic_integers_of_finite_module
    (F : IntermediateField ℚ ℂ) (h_fin : Module.Finite ℚ F) [IsGalois ℚ F]
    (h : IsMulCommutative (F ≃ₐ[ℚ] F)) : {x : F | IsIntegral ℤ x ∧ ‖(x : ℂ)‖ = 1}.Finite ∧
    (∀ x : F, IsIntegral ℤ x → ‖(x : ℂ)‖ = 1 → ∃ n,  x ^ n = 1) := by
  sorry

end Problem22
```

Exercise (23). *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial, n_p is the number of solutions of $f(X)$ in $\mathbb{F}_p$, show that*

$$\lim_{s \to 1^+} \frac{\sum\limits_{p \ prime} \frac{n_p}{p^s}}{\sum\limits_{p \ prime} \frac{1}{p^s}} = 1$$

.

```
import Mathlib

namespace Problem23

local instance (p : Nat.Primes) : NeZero p.1 := ⟨p.2.ne_zero⟩
local instance (p : Nat.Primes) : IsDomain (ZMod p) := @ZMod.instIsDomain p ⟨p.2⟩

/--
```

```
Let $f(X)\in\mathbb{Z}[X]$ be an irreducible polynomial, $n_p$ is the number of solutions of
$f(X)$ in $\mathbb{F}_p$, show that $$\lim\limits_{s\rightarrow 1^{+}}\frac{\sum
\limits_{p\textbf{ prime}}\frac{n_p}{p^s}}{\sum\limits_{p\textbf{ prime}}\frac{1}{p^s}}=1$$.
-/
theorem ratio_tendsto_one_of_irreducible (f : Polynomial ℤ) (h_irr : Irreducible f) :
    Function.rightLim
    (fun (s : ℝ) ↦
    (tsum (fun p : Nat.Primes ↦ (f.rootSet (ZMod p)).ncard * ((p : ℝ) ^ (-s)))) /
    (tsum (fun p : Nat.Primes ↦ (p : ℝ) ^ (-s)))) 1 = 1 := by
  sorry

end Problem23
```

Exercise (24). *Let $p_1, \dots, p_r$ be r different prime numbers. Prove that the Galois group of $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$ over $\mathbb{Q}$ is $(\mathbb{Z}/2\mathbb{Z})^r$, here $\mathbb{Z}/2\mathbb{Z}$ is the cyclic group of order 2.*

```
import Mathlib

namespace Problem24

/--
The field $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$
for a finite list of integers $p_1, \dots, p_r$.
-/
abbrev RatAdjoinSqrt {I : Type} (p : I → ℕ) : Type :=
  Algebra.adjoin ℚ (Set.range (fun i ↦ Real.sqrt (p i)))

/--
Let $p_1, \dots, p_r$ be $r$ different prime numbers.
Prove that the Galois group of $K =\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$ over $\mathbb{Q}$
is $(\mathbb{Z}/2\mathbb{Z})^r$, here $\mathbb{Z}/2\mathbb{Z}$ is the cyclic group of order 2.
-/
theorem galoisGroup_iso_of_distinct_primes {I : Type} [Finite I] (p : I → ℕ)
    (hp : ∀ (i : I), (p i).Prime) (h_inj : p.Injective) :
    Nonempty ((RatAdjoinSqrt p ≃ₐ[ℚ] RatAdjoinSqrt p) ≃* (Multiplicative (I → (ZMod 2)))) := by
  sorry

end Problem24
```

Exercise (25). *Prove that the automorphism group of $\mathbb{F}_2(t)$ is isomorphic to S_3, and its fixed field is $\mathbb{F}_2(u)$ with*

$$u = \frac{(t^4 - t)^3}{(t^2 - t)^5} = \frac{(t^2 + t + 1)^3}{(t^2 - t)^2}$$

.

```
import Mathlib

namespace Problem25
```

```
/--
Prove that the automorphism group of $\mathbb{F}_2(t)$ is isomorphic to $S_3$, and its fixed field is
$\mathbb{F}_2(u)$ with $$u = \frac{(t^4-t)^3}{(t^2-t)^5} = \frac{(t^2+t+1)^3}{(t^2-t)^2}$$.
-/
theorem fixedField_eq_algebra_adjoin :
    Nonempty ((RatFunc (ZMod 2) ≃+* RatFunc (ZMod 2)) ≃* (Equiv.Perm (Fin 3))) ∧
    IntermediateField.fixedField (F := ZMod 2) (E := RatFunc (ZMod 2)) ⊤ =
    IntermediateField.adjoin (ZMod 2) {((.X ^ 4 - .X) ^ 3 / (.X ^ 2 - .X) ^ 5 : (RatFunc (ZMod 2)))}
     := by
  sorry

end Problem25
```

Exercise (26). *Let $K/\mathbb{Q}$ be a finite extension. Let H be a closed subgroup of the absolute Galois group $G(K)$ of K. If H is finite, then the cardinality of H is either one or two.*

```
import Mathlib

namespace Problem26

/--
Let $K/\mathbb{Q}$ be a finite extension.
Let $H$ be a closed subgroup of the absolute Galois group $G(K)$ of $K$.
If $H$ is finite, then the cardinality of $H$ is either one or two.
-/
theorem card_one_or_two_of_finite_closed_subgroup_of_absoluteGaloisGroup
    (K : Type) [Field K] [Algebra ℚ K] [Module.Finite ℚ K]
    (H : Subgroup (Field.absoluteGaloisGroup K))
    (h_closed : IsClosed (H : Set (Field.absoluteGaloisGroup K)))
    (h_fin : Finite H) : Nat.card H = 1 ∨ Nat.card H = 2 := by
  sorry

end Problem26
```

Exercise (27). *Let p be a prime number. Let $K/\mathbb{Q}$ be a finite extension, such that the p^2th root of unity is contained in K. Let L/K be a Galois extension of degree p, show that there exists a Galois extension L'/L of degree p, such that the extension L'/K is Galois.*

```
import Mathlib

namespace Problem27

/--
Let $p$ be a prime number. Let $K/\mathbb{Q}$ be a finite extension, such that the $p^{2}$th
root of unity is contained in $K$. Let $L/K$ be a Galois extension of degree $p$, show that there
exists a Galois extension $L'/L$ of degree $p$, such that the extension $L'/K$ is Galois.
-/
theorem isGalois_and_rank_eq_of_isPrimitiveRoot_sq (p : ℕ) (hp : p.Prime) {K : Type} [Field K]
    [NumberField K] {ζ : K} (h : IsPrimitiveRoot ζ (p^2))
```

```
    {L : IntermediateField K (AlgebraicClosure K)} [IsGalois K L]
    (hdeg : Module.rank K L = p) :
    ∃ (L' : Type) (_ : Field L') (_ : Algebra K L')
    (_ : Algebra L L') (_ : IsScalarTower K L L'),
    IsGalois K L' ∧ IsGalois L L' ∧ Module.rank L L' = p := by
  sorry

end Problem27
```

Exercise (28). *Let $K/\mathbb{Q}$ be a finite extension. Let g be a nontrivial element of the absolute Galois group $G(K)$ of K. Show that g admits an infinite number of conjugates.*

```
import Mathlib

namespace Problem28

/--
Let $K/\mathbb{Q}$ be a finite extension.
Let $g$ be a nontrivial element of the absolute Galois group $G(K)$ of $K$.
Show that $g$ admits an infinite number of conjugates.
-/
theorem infinite_conj_of_ne_1_absoluteGaloisGroup (K : Type)
    [Field K] [Algebra ℚ K] [Module.Finite ℚ K] (g : Field.absoluteGaloisGroup K) (h : g ≠ 1) :
    {g' : Field.absoluteGaloisGroup K | IsConj g g'}.Infinite := by
  sorry

end Problem28
```

Exercise (29). *Let $K/\mathbb{Q}$ be a finite extension. Let g be an element of the absolute Galois group $G(K)$ of K. Show that the subgroup generated by g is closed in $G(K)$ if and only if g is torsion.*

```
import Mathlib

namespace Problem29

/--
Let $K/\mathbb{Q}$ be a finite extension. Let $g$ be an element of the absolute Galois group
$G(K)$ of $K$. Show that the subgroup generated by $g$ is closed in $G(K)$ if and only if $g$
is torsion.
-/
theorem isClosed_zpowers_iff_isOfFinOrder (K : Type)
    [Field K] [Algebra ℚ K] [Module.Finite ℚ K] (g : Field.absoluteGaloisGroup K) :
    IsClosed ((Subgroup.zpowers g) : Set (Field.absoluteGaloisGroup K)) ↔ IsOfFinOrder g := by
  sorry

end Problem29
```

Exercise (30). *Let A be a subring of a ring B, such that the set $B \setminus A$ is closed under multiplication. Show that A is integrally closed in B.*

```
import Mathlib

namespace Problem30

/--
Let \( A \) be a subring of a ring \( B \), such that the set \( B \setminus A \) is closed under
multiplication. Show that \( A \) is integrally closed in \( B \).
-/
theorem integrallyClosedIn_of_complement_multiplicatively_closed (B : Type) [CommRing B] (A : Subring
    B)
    (h : ∀ (x y : B), x ∉ A → y ∉ A → x * y ∉ A) : IsIntegrallyClosedIn A B := by
  sorry

end Problem30
```

Exercise (31). *Let $R = \mathbb{C}[x_1, \dots, x_n]/(x_1^2 + x_2^2 + \cdots + x_n^2)$. Then R is a unique factorization domain for $n \geq 5$.*

```
import Mathlib

namespace Problem31

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 a unique factorization domain for \( n \geq 5 \).
-/
theorem UFD_of_ge_5 (n : ℕ) (h : n ≥ 5) :
    ∃ (h : IsDomain (R n)), UniqueFactorizationMonoid (R n) := by
  sorry

end Problem31
```

Exercise (32). *Let A be a Noetherian local ring such that its completion $\widehat{A}$ is a unique factorization domain. Then A is a unique factorization domain.*

```
import Mathlib

namespace Problem32

open IsLocalRing
```

```
/--
Let \( A \) be a Noetherian local ring such that its completion \( \widehat{A} \) is a unique
factorization domain. Then \( A \) is a unique factorization domain.
-/
theorem UFD_of_adicCompletion_UFD (R : Type) [CommRing R] [IsLocalRing R] [IsNoetherianRing R]
    [IsDomain (AdicCompletion (maximalIdeal R) R)]
    [UniqueFactorizationMonoid (AdicCompletion (maximalIdeal R) R)] :
    ∃ (h : IsDomain R), UniqueFactorizationMonoid R := by
  sorry

end Problem32
```

Exercise (33)**.** *Let $A \subset B$ be commutative rings such that B is finitely generated as a module over A. If B is a noetherian ring, show that A is also a noetherian ring.*

```
import Mathlib

namespace Problem33

/--
Let $A\subset B$ be commutative rings such that $B$ is finitely generated as a module over $A$.
If $B$ is a noetherian ring, show that $A$ is also a noetherian ring.
-/
theorem isNoetherianRing_of_fg_of_isNoetherianRing (B : Type) [CommRing B] [IsNoetherianRing B]
    (A : Subring B) (h : Module.Finite A B) : IsNoetherianRing A := by
  sorry

end Problem33
```

Exercise (34)**.** *If R is a valuation ring of Krull dimension ≥ 2, then the formal power series ring $R[[X]]$ is not integrally closed.*

```
import Mathlib

namespace Problem34

open PowerSeries

/--
If \( R \) is a valuation ring of Krull dimension \( \geq 2 \),
then the formal power series ring \( R[[X]] \) is not integrally closed.
-/
theorem powerSeries_not_integrallyClosed_of_two_lt_ringKrullDim (R : Type) [CommRing R]
    [IsDomain R] [ValuationRing R] (two_lt : 2 ≤ ringKrullDim R) :
    ¬ (IsIntegrallyClosed R⟦X⟧) := by
  sorry

end Problem34
```

Exercise (35). *A commutative ring whose prime ideals are finitely generated is Noetherian.*

```
import Mathlib

namespace Problem35

/--
A commutative ring whose prime ideals are finitely generated is Noetherian.
-/
theorem noetherian_of_prime_ideals_fg (R : Type) [CommRing R]
    (h_fg : ∀ (p : Ideal R), p.IsPrime → p.FG) : IsNoetherianRing R := by
  sorry

end Problem35
```

Exercise (36). *If R is Noetherian and M and N are finitely generated R-modules, show that*

$$\operatorname{Ass} \operatorname{Hom}_R(M, N) = \operatorname{Supp} M \cap \operatorname{Ass} N,$$

where $\operatorname{Supp} M$ *is the set of all primes containing the annihilator of* M*.*

```
import Mathlib

namespace Problem36

/--
If \( R \) is Noetherian and \( M \) and \( N \) are finitely generated \( R \)-modules, show that
\[
\operatorname{Ass} \operatorname{Hom}_R(M, N) = \operatorname{Supp} M \cap \operatorname{Ass} N,
\]
where \( \operatorname{Supp} M \) is the set of all primes containing the annihilator of \( M \).
-/
theorem associatedPrimes_hom_eq_support_inter_associatedPrimes (R : Type) [CommRing R]
    [IsNoetherianRing R] (M N : Type) [AddCommGroup M] [AddCommGroup N] [Module R M] [Module R N]
    [Module.Finite R M] [Module.Finite R N] : associatedPrimes R (M →ₗ[R] N) =
    {p | p ∈ associatedPrimes R N ∧ Module.annihilator R M ≤ p} := by
  sorry

end Problem36
```

Exercise (37). *Let* $R = \mathbb{C}[x_{11}, x_{12}, \dots, x_{1n}, x_{21}, x_{22}, \dots, x_{2n}, \dots, x_{n1}, x_{n2}, \dots, x_{nn}]/(\det(x_{ij}) - 1)$, *show that R is a unique factorization domain.*

```
import Mathlib

namespace Problem37

/--
Let $R=\mathbb{C}[x_{11},x_{12},\dots,x_{1n},x_{21},x_{22},\dots,
```

```
x_{2n},\dots,x_{n1},x_{n2},\dots,x_{nn}]/(\det(x_{ij})-1)$.
-/
abbrev QuotDetSubOne (n : ℕ) : Type := MvPolynomial ((Fin n) × (Fin n)) ℂ / Ideal.span {
      Matrix.det (fun (i : Fin n) ↦ (fun (j : Fin n) ↦ (.X ⟨i, j⟩ : (MvPolynomial ((Fin n) × (Fin
    n)) ℂ)))) - .C 1}

/--
Let $R=\mathbb{C}[x_{11},x_{12},\dots,x_{1n},x_{21},x_{22},\dots,
x_{2n},\dots,x_{n1},x_{n2},\dots,x_{nn}]/(\det(x_{ij})-1)$,
show that $R$ is a unique factorization domain.
-/
theorem ufd_quotDetSubOne (n : ℕ) (h : n ≥ 1) : ∃ (h : IsDomain (QuotDetSubOne n)),
    UniqueFactorizationMonoid (QuotDetSubOne n) := by
  sorry

end Problem37
```

Exercise (38). *Let k be a field, and let $R = k[t]/(t^2)$. Set*

$$p(x) = tx^3 + tx^2 - x^2 - x \in R[x].$$

Show that $S = R[x]/(p)$ is a free R-module of rank 2.

```
import Mathlib

namespace Problem38

open Polynomial DualNumber

/--
Let \( k \) be a field, and let \( R = k[t]/(t^2) \). Set
\[
p(x) = tx^3 + tx^2 - x^2 - x \in R[x].
\]
Let \( S = R[x]/(p) \).
-/
abbrev S (k : Type) [Field k] : Type := ((DualNumber k)[X] / Ideal.span {((C ε) * X^3 + (C ε) * X^2 -
    X^2 - X : (DualNumber k)[X])})

/--
\(S\) has a \(R\) module structure inherited from R[x].
-/
noncomputable instance (k : Type) [Field k] : Module (DualNumber k) (S k) := Module.compHom _ C

/--
Let \( k \) be a field, and let \( R = k[t]/(t^2) \). Set
\[
p(x) = tx^3 + tx^2 - x^2 - x \in R[x].
\]
Show that \( S = R[x]/(p) \) is a free \( R \)-module of rank \( 2 \).
-/
```

```
theorem free_dualNumber_and_rank_eq_2 (k : Type) [Field k] :
    Module.Free (DualNumber k) (S k) ∧ Module.rank (DualNumber k) (S k) = 2 := by
  sorry

end Problem38
```

Exercise (39). *Let R be a normal Noetherian domain, K its fraction field, L/K a finite field extension, and $\overline{R}$ the integral closure of R in L. Prove that only finitely many primes $\mathfrak{P}$ of $\overline{R}$ lie over a given prime $\mathfrak{p}$ of R.*

```
import Mathlib

namespace Problem39

/--
Let \( R \) be a normal Noetherian domain, \( K \) its fraction field, \( L/K \) a finite
field extension, and \( \overline{R} \) the integral closure of \( R \) in \( L \).
Prove that only finitely many primes \( \mathfrak{P} \) of \( \overline{R} \) lie over a given
prime \( \mathfrak{p} \) of \( R \).
-/
theorem finite_primes_lies_over_of_finite_extension (R : Type) [CommRing R] [IsDomain R]
    [IsNoetherianRing R] [IsIntegrallyClosed R] (L : Type) [Field L] [Algebra R L]
    [Algebra (FractionRing R) L] [IsScalarTower R (FractionRing R) L]
    [FiniteDimensional (FractionRing R) L] (p : Ideal R) [p.IsPrime] :
    (p.primesOver (integralClosure R L)).Finite := by
  sorry

end Problem39
```

Exercise (40). *Let A be a reduced local ring with residue field k and finite set Σ of minimal primes. For each $\mathfrak{p} \in \Sigma$, set $K(\mathfrak{p}) = \mathrm{Frac}(A/\mathfrak{p})$. Let P be a finitely generated module. Show that P is free of rank r if and only if $\dim_k(P \otimes_A k) = r$ and $\dim_{K(\mathfrak{p})}(P \otimes_A K(\mathfrak{p})) = r$ for each $\mathfrak{p} \in \Sigma$.*

```
import Mathlib

namespace Problem40

open TensorProduct

/--
Let $A$ be a reduced local ring with residue field $k$ and finite set $\Sigma$ of minimal primes.
For each $\mathfrak{p}\in\Sigma$, set $K(\mathfrak{p})=\mathrm{Frac}(A/\mathfrak{p})$.
Let $P$ be a finitely generated module. Show that $P$ is free of rank $r$ if and only if
$\dim_k(P\otimes_A k) = r$ and $\dim_{K(\mathfrak{p})}(P\otimes_A K(\mathfrak{p})) = r$
for each $\mathfrak{p}\in\Sigma$.
-/
theorem free_of_rank_iff (R : Type) [CommRing R] [IsLocalRing R] [IsReduced R]
    (h : (minimalPrimes R).Finite) (r : ℕ) (M : Type) [AddCommGroup M] [Module R M] [Module.Finite R
     M] :
```

```
    Module.Free R M ∧ Module.rank R M = r ↔
    (Module.rank (IsLocalRing.ResidueField R) ((IsLocalRing.ResidueField R) ⊗[R] M) = r ∧
    ∀ p ∈ minimalPrimes R,
    Module.rank (FractionRing (R / p)) ((FractionRing (R / p)) ⊗[R] M) = r) := by
  sorry

end Problem40
```

Exercise (41). *Let k be a field, $A := k[X_1, X_2, \dots]$ a polynomial ring, $m_1 < m_2 < \cdots$ positive integers with $m_{i+1} - m_i > m_i - m_{i-1}$ for $i > 1$. Set*

$$\mathfrak{p}_i := (X_{m_i+1}, \dots, X_{m_{i+1}})$$

and $S := A - \bigcup_{i \geq 1} \mathfrak{p}_i$. Show that $S^{-1}A$ is noetherian with infinite krull dimension.

```
import Mathlib

namespace Problem41

/--
The multiplicative subset generated by elements
not in a given family of ideals.
-/
def compl_all {α R : Type} [CommRing R] (I : α → Ideal R) : Submonoid R :=
  Submonoid.closure (⋃ (i : α), (I i : Set R))ᶜ

/--
The ideal generated by a set of single
variables in a multivariate polynomial ring.
-/
def ideal_x {α : Type} (R : Type) [CommRing R] (J : Set α) : Ideal (MvPolynomial α R) :=
  Ideal.span ((MvPolynomial.X)'' J)

/--
Let \( A := k[X_1, X_2, \dots] \).
Set \[\mathfrak{p}_i := (X_{m_i+1}, \dots, X_{m_{i+1}})\] and
\( S := A - \bigcup_{i \geq 1} \mathfrak{p}_i \).
This is the ring  \( S^{-1}A \).
-/
abbrev SInvA (k : Type) [Field k] (m : ℕ → ℕ) : Type := (Localization (compl_all fun (n : ℕ) ↦
     ideal_x k (Set.Ioc (m n) (m (n + 1)))))

/--
Let \( k \) be a field, \( A := k[X_1, X_2, \dots] \) a polynomial ring, \( m_1 < m_2 < \cdots \)
positive integers with \( m_{i+1} - m_i > m_i - m_{i-1} \) for \( i > 1 \). Set
\[\mathfrak{p}_i := (X_{m_i+1}, \dots, X_{m_{i+1}})\]
and \( S := A - \bigcup_{i \geq 1} \mathfrak{p}_i \).
Show that  \( S^{-1}A \) is noetherian with infinite krull dimension.
-/
theorem isNoetherianRing_and_krullDim_eq_top (k : Type) [Field k] (m : ℕ → ℕ) (h : StrictMono m)
     (h_diff_mono : StrictMono (fun (i : ℕ) ↦ m (i + 1) - m i)) :
```

```
    IsNoetherianRing (SInvA k m) ∧
    ringKrullDim (SInvA k m) = ⊤ := by
  sorry

end Problem41
```

Exercise (42)**.** *Let k be any field. Suppose that $A = k[[x,y]]/(f)$ and $B = k[[u,v]]/(g)$, where $f = xy$ and $g = uv + \delta$ with $\delta \in (u,v)^3$. Show that A and B are isomorphic.*

```
import Mathlib

namespace Problem42

/--
Let \(k\) be any field. Suppose that \(A = k[[x,y]]/(f)\) and \(B = k[[u,v]]/(g)\),
where \(f = xy\) and \(g = uv + \delta\) with \(\delta \in (u,v)^{3}\). Show that \(A\) and \(B\)
are isomorphic.
-/
theorem nonEmpty_ringEquiv_of_sub_in_cube (k : Type) [Field k]
    (g : MvPowerSeries (Fin 2) k) (hg : g - .X 0 * .X 1 ∈ (Ideal.span {MvPowerSeries.X 0, .X 1}) ^ 3)
     :
    Nonempty (((MvPowerSeries (Fin 2) k) / Ideal.span {(.X 0 * .X 1 : (MvPowerSeries (Fin 2) k))}) ≃+
     *
    ((MvPowerSeries (Fin 2) k) / Ideal.span {g})) := by
  sorry

end Problem42
```

Exercise (43)**.** *Let A be a reduced Noetherian local ring,* $\mathrm{Char}\ A = p$*. Show that the absolute Frobenius $F_A\colon A \to A, a \mapsto a^p$ is flat if and only if A is regular.*

```
import Mathlib

namespace Problem43

open IsLocalRing

/--
A commutative local noetherian ring $R$ is regular if $\dim m/m^2 = \dim R$.
-/
class IsRegularLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  reg : Module.finrank (ResidueField R) (CotangentSpace R) = ringKrullDim R

/--
Let $A$ be a reduced Noetherian local ring, $\mathrm{Char}\ A = p$.
Show that the absolute Frobenius $F_A\colon A\to A, a\mapsto a^p$ is flat if and only if $A$ is
regular.
-/
```

```
theorem IsRegularLocalRing.frobenius_flat {A : Type} [CommRing A] [IsNoetherianRing A]
    [IsLocalRing A] [IsReduced A] (p : ℕ) [Fact p.Prime] [CharP A p] :
    (frobenius A p).Flat ↔ IsRegularLocalRing A := by
  sorry

end Problem43
```

Exercise (44). *Let k be a field, and set $A = k[X, Y, Z]/(X^2 - Y^2, Y^2 - Z^2, XY, YZ, ZX)$. Show that A is not a global complete intersection.*

```
import Mathlib

namespace Problem44

open MvPolynomial

/--
Let $k$ be a field. Let $S$ be a finite type $k$-algebra. We say that $S$ is a
\textit{global complete intersection over $k$} if there exists a presentation
$S = k[x_1, \dots, x_n]/(f_1, \dots, f_c)$ such that $\dim(S) = n - c$.
-/
class IsGlobalCompleteIntersection (k : Type) [Field k] (S : Type) [CommRing S] [Algebra k S] :
    Prop extends Algebra.FiniteType k S where
  isGlobalCompleteIntersection : ∃ n : ℕ, ∃ rs : List (MvPolynomial (Fin n) k),
    Nonempty (S ≃ₐ[k] (MvPolynomial (Fin n) k) / Ideal.ofList rs) ∧ ringKrullDim S + rs.length = n

/--
Let \( k \) be a field, and set \( A = k[X, Y, Z]/(X^2 - Y^2, Y^2 - Z^2, XY, YZ, ZX) \).
Show that \( A \) is not a global complete intersection.
-/
theorem quot_x2_sub_y2_y2_sub_z2_xy_yz_zx_not_global_complete_intersection (k : Type) [Field k] :
    ¬ IsGlobalCompleteIntersection k (MvPolynomial (Fin 3) k / Ideal.span
    ({(X 0)^ 2 - (X 1)^2, (X 1)^2 - (X 2)^2, (X 0) * (X 1), (X 1) * (X 2), (X 2) * (X 0)} :
    Set (MvPolynomial (Fin 3) k))) := by
  sorry

end Problem44
```

Exercise (45). *Let k be a field and $A = k[x_1, \dots, x_r]$ the polynomial ring in r variables. Let M be a graded module over A, and let*

$$0 \to K \to L_{r-1} \to \cdots \to L_0 \to M \to 0$$

be an exact sequence of graded homomorphisms of graded modules, such that $L_0, \dots, L_{r-1}$ are free. Then K is free. Gradings of modules are by $\mathbb{Z}_{\geq 0}$.

```
import Mathlib
```

```
namespace Problem45

/--
A linear map `f` between graded modules is a graded homomorphism if it respects the
grading structure.
-/
def IsGradedHom {R M N ι : Type} [CommRing R] [AddCommGroup M] [AddCommGroup N]
    [Module R M] [Module R N] (�� : ι → Submodule R M) (�� : ι → Submodule R N)
    (f : M ₗ→[R] N) : Prop := ∀ (i : ι) (x : �� i), f x ∈ �� i

/--
Let $k$ be a field and $A = k[x_1, \dots, x_r]$ the polynomial ring in $r$ variables. Let $M$ be
a graded module over $A$, and let
\[
0 \to K \to L_{r-1} \to \cdots \to L_0 \to M \to 0
\]
be an exact sequence of graded homomorphisms of graded modules, such that $L_0, \dots, L_{r-1}$
are free. Then $K$ is free. {Gradings of modules are by $\mathbb{Z}_{\geq 0}$.}
-/
theorem free_of_free_resolution {k : Type} [Field k] {r : ℕ}
    (C : ChainComplex (ModuleCat.{0} (MvPolynomial (Fin r) k)) ℕ)
    (hC : ∀ (n : ℕ), n > (r + 1) → CategoryTheory.Limits.IsZero (C.X n))
    (�� : ∀ (n : ℕ), (ℕ → Submodule (MvPolynomial (Fin r) k) (C.X n)))
    [hM : ∀ (n : ℕ), DirectSum.Decomposition (�� n)]
    [hM' : ∀ (n : ℕ), SetLike.GradedSMul (MvPolynomial.homogeneousSubmodule (Fin r) k) (�� n)]
    (h_exact : C.Acyclic)
    (h_gr : ∀ (i j : ℕ), IsGradedHom (�� i) (�� j) (C.d i j).hom)
    (h_free : ∀ (n : ℕ), 1 ≤ n ∧ n ≤ r → Module.Free (MvPolynomial (Fin r) k) (C.X n)) :
    Module.Free (MvPolynomial (Fin r) k) (C.X (r + 1)) := by
  sorry

end Problem45
```

Exercise (46). *Let M be an R-module. Then M is flat if and only if the following condition holds: if P is a finitely presented R-module and $f : P \to M$ a R-linear map, then there is a free finite R-module F and module maps $h : P \to F$ and $g : F \to M$ such that $f = g \circ h$.*

```
import Mathlib

namespace Problem46

/--
Let \(M\) be an \(R\)-module. Then \(M\) is flat if and only if the following condition holds:
if \(P\) is a finitely presented \(R\)-module and \(f: P \to M\) a \(R\)-linear map,
then there is a free finite \(R\)-module \(F\) and module maps \(h: P \to F\) and \(g: F \to M\)
such that \(f = g \circ h\).
-/
theorem module_flat_iff (R : Type) [CommRing R] (M : Type) [AddCommGroup M] [Module R M] :
    Module.Flat R M ↔
    ∀ P : Type, ∀ (_ : AddCommGroup P), ∀ (_ : Module R P), ∀ f : P ₗ→[R] M,
     Module.FinitePresentation R P →
```

```
    ∃ (F : Type) (_ : AddCommGroup F) (_ : Module R F), Module.Finite R F ∧ Module.Free R F ∧
    ∃ h : P ₗ→[R] F, ∃ g : F ₗ→[R] M, f = g.comp h := by
  sorry

end Problem46
```

Exercise (47). *Show that the ring $A = k[x, y]/(y^2 - f(x))$ is a Dedekind domain and the class group of the ring A is not trivial, where k is a field of characteristic not 2, $f(x) = (x - t_1) \dots (x - t_n)$ with $t_1, \dots, t_n \in k$ distinct and $n \geq 3$ is an odd integer.*

```
import Mathlib

namespace Problem47

/--
The ring \(A = k[x,y]/(y^{2} - f(x))\),
where \(k\) is a field and \(f(x) = (x - t_{1})\ldots(x - t_{n})\).
-/
abbrev A {k : Type} [Field k] {n : ℕ} (t : (Fin n) → k) : Type := (MvPolynomial (Fin 2) k) /
    Ideal.span {(.X 1 ^ 2) - ∏ (m : Fin n), (.X 0 - .C (t m) : (MvPolynomial (Fin 2) k))}


/--
Show that the ring \(A = k[x,y]/(y^{2} - f(x))\) is a Dedekind domain and the class group of the
ring \(A\) is not trivial, where \(k\) is a field of characteristic not 2,
\(f(x) = (x - t_{1})\ldots(x - t_{n})\) with \(t_{1},\ldots,t_{n} \in k\) distinct and
\(n \geq 3\) is an odd integer.
-/
theorem isEmpty_isomorphism_UFD_of_quotient (k : Type) [Field k] (h_char : ¬ CharP k 2)
    (n : ℕ) (h_ge : n ≥ 3) (h_odd : Odd n) (t : (Fin n) → k) (h_inj : Function.Injective t) :
    ∃ _ : IsDedekindDomain (A t), Nontrivial (ClassGroup (A t)) := by
  sorry

end Problem47
```

Exercise (48). *A commutative ring A is absolutely flat if every A-module is flat. Prove that A is absolutely flat if and only if every principal ideal is idempotent.*

```
import Mathlib

namespace Problem48

/--
A commutative ring \( A \) is \textit{absolutely flat} if every \( A \)-module is flat.
-/
class IsAbsolutelyFlat (R : Type) [CommRing R] : Prop where
  out {|P : Type|} [AddCommGroup P] [Module R P] : Module.Flat R P

/--
```

```
Prove that \( A \) is absolutely flat if and only if every principal ideal is idempotent.
-/
theorem isAbsolutelyFlat_iff_principal_ideal_idempotent (R : Type) [CommRing R] :
    IsAbsolutelyFlat R ↔ (∀ I : Ideal R, I.IsPrincipal → I ^ 2 = I) := by
  sorry

end Problem48
```

Exercise (49). *Let A be a commutative ring. Prove that every principal ideal of A is idempotent if and only if every finitely generated ideal is a direct summand of A.*

```
import Mathlib

namespace Problem49

/--
Let \( A \) be a commutative ring. Prove that every principal ideal of \( A \) is idempotent
if and only if every finitely generated ideal is a direct summand of \( A \).
-/
theorem principal_ideal_idempotent_iff_fg_ideal_is_direct_summand (A : Type) [CommRing A] :
    (∀ I : Ideal A, I.IsPrincipal → I ^ 2 = I) ↔
    (∀ I : Ideal A, I.FG → (∃ J : Ideal A, I ⊔ J = ⊤ ∧ I ⊓ J = ⊥ )) := by
  sorry

end Problem49
```

Exercise (50). *Let $(A, \mathfrak{m}, K)$ be a complete local ring containing a field, and suppose that $\mathfrak{m}$ is finitely generated over A. Then A is Noetherian.*

```
import Mathlib

namespace Problem50

/--
Let \((A, \mathfrak{m}, K)\) be a complete local ring containing a field,
and suppose that \(\mathfrak{m}\) is finitely generated over \(A\). Then \(A\) is Noetherian.
-/
theorem isNoetherianRing_of_isLocalRing_of_field_inj_of_adicComplete_of_maximalIdeal_finite
    (R : Type) [CommRing R] [IsLocalRing R] [IsAdicComplete (IsLocalRing.maximalIdeal R) R]
    (k : Type) [Field k] [Algebra k R] [NoZeroSMulDivisors k R]
    (hfg : (IsLocalRing.maximalIdeal R).FG) : IsNoetherianRing R := by
  sorry

end Problem50
```

Exercise (51). *A Noetherian topological ring in which the topology is defined by an ideal contained in the Jacobson radical is called a Zariski ring. Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, and $\widehat{A}$ the $\mathfrak{a}$-adic completion of A. Prove that $\widehat{A}$ is faithfully flat over A if and only if A is a Zariski ring for the $\mathfrak{a}$-topology.*

```
import Mathlib

namespace Problem51

/--
A Noetherian topological ring in which the topology is defined by an ideal contained in the
Jacobson radical is called a \textit{Zariski ring}.
Let \( A \) be a Noetherian ring, \( \mathfrak{a} \) an ideal of \( A \), and \( \widehat{A} \)
the \( \mathfrak{a} \)-adic completion of $A$.
Prove that \( \widehat{A} \) is faithfully flat over \( A \) if and only if \( A \) is a Zariski
ring for the \( \mathfrak{a} \)-topology.
-/
theorem adicCompletion_faithfullyFlat_iff (A : Type) [CommRing A] [IsNoetherianRing A]
    (I : Ideal A) : Module.FaithfullyFlat A (AdicCompletion I A) ↔ I ≤ Ring.jacobson A := by
  sorry

end Problem51
```

Exercise (52). *Let R be a ring, $\mathfrak{m}$ is an ideal in the Jacobson radical of R, and $G_1, G_2 \in R[x]$ are polynomials such that G_1 is monic. If $G_i \mod \mathfrak{m}$ gnerate the unit ideal of $R/\mathfrak{m}[x]$, then G_1, G_2 together generate the unit ideal of $R[x]$.*

```
import Mathlib

namespace Problem52

/--
Let $R$ be a ring, \( \mathfrak{m} \) is an ideal in the Jacobson radical of \( R \),
and \( G_{1}, G_{2} \in R[x] \) are polynomials such that $G_1$ is monic.
If $G_i \mod \mathfrak{m}$ gnerate the unit ideal of $R/\mathfrak{m}[x]$,
then \( G_{1}, G_{2} \) together generate the unit ideal of \( R[x] \).
-/
theorem generate_unit_ideal_of_quotient (R : Type) [CommRing R] (m : Ideal R)
    (h_le_jac : m ≤ Ring.jacobson R) (G₁ G₂ : Polynomial R) (h_monic : G₁.Monic)
    (h_gen : Ideal.span {G₁.map (Ideal.Quotient.mk m), G₂.map (Ideal.Quotient.mk m)} = ⊤) :
    Ideal.span {G₁, G₂} = ⊤ := by
  sorry

end Problem52
```

Exercise (53). *Let k be a field, and set $A = k[X, Y, Z]/(X^2 - Y^2, Y^2 - Z^2, XY, YZ, ZX)$. Show that A is Gorenstein.*

```
import Mathlib

namespace Problem53

open IsLocalRing ModuleCat CategoryTheory MvPolynomial
```

```
instance (R : Type) [CommRing R] : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives.{0} (ModuleCat.{0} R)

/--
A Noetherian local ring $R$ is a Gorenstein ring if $\mathrm{inj}.\dim_R R < +\infty$.
-/
class IsGorensteinLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  injDim_le_infity :
    ∃ n : ℕ, ∀ i : ℕ, n ≤ i →
    Subsingleton (Abelian.Ext.{0} (of.{0} R (ResidueField R)) (of.{0} R R) i)

/--
A Noetherian ring is a Gorenstein ring if its localization at every maximal ideal is a
  Gorenstein local ring.
-/
class IsGorensteinRing (R : Type) [CommRing R] : Prop extends IsNoetherianRing R where
  localization_maximal_isGorensteinLocalRing :
    ∀ m : Ideal R, (_ : m.IsMaximal) → IsGorensteinLocalRing (Localization.AtPrime m)

/--
Let \( k \) be a field, and set \( A = k[X, Y, Z]/(X^2 - Y^2, Y^2 - Z^2, XY, YZ, ZX) \).
Show that \( A \) is Gorenstein.
-/
theorem isGorensteinRing_quot_x2_sub_y2_y2_sub_z2_xy_yz_zx (k : Type) [Field k] :
    IsGorensteinRing <| MvPolynomial (Fin 3) k / Ideal.span ({(X 0)^ 2 - (X 1)^2, (X 1)^2 - (X 2)^2,
    (X 0) * (X 1), (X 1) * (X 2), (X 2) * (X 0)} : Set (MvPolynomial (Fin 3) k)) := by
  sorry

end Problem53
```

Exercise (54). *Let A be a $\mathbb{Q}$-algebra. Suppose that $x \in A$ and $D \in \operatorname{Der}(A)$ are such that $Dx = 1$ and $\bigcap_{n=1}^{\infty} x^n A = (0)$. Show that x is a non-zero-divisor of A.*

```
import Mathlib

namespace Problem54

/--
Let \( A \) be a $\mathbb{Q}$-algebra.
Suppose that \( x \in A \) and \( D \in \operatorname{Der}(A) \) are such that \( Dx = 1 \) and
\( \bigcap_{n=1}^{\infty} x^n A = (0) \).
Show that \( x \) is a non-zero-divisor of \( A \).
-/
theorem not_zero_divisor_of_hausdorff_of_der_eq_one (A : Type) [CommRing A] [Algebra ℚ A]
    (x : A) (D : Derivation ℤ A A) (h_dx : D x = 1) (h_hausdorff : IsHausdorff (Ideal.span {x}) A) :
    x ∈ nonZeroDivisors A := by
  sorry

end Problem54
```

Exercise (55). *A module M over a ring R is stably free if there exists a free finitely generated module F over R such that*

$$M \oplus F$$

is a free module. Prove that if M is stably free and not finitely generated then M is free.

```
import Mathlib

namespace Problem55

/--
A module \( M \) over a ring \( R \) is \textit{stably free} if there exists a free finitely
generated module \( F \) over \( R \) such that
\[
M \oplus F
\]
is a free module.
-/
def IsStablyFree (R : Type) (M : Type) [CommRing R] [AddCommGroup M] [Module R M] : Prop :=
    ∃ (N : Type) (_ : AddCommGroup N) (_ : Module R N),
    Module.Finite R N ∧ Module.Free R N ∧ Module.Free R (M × N)

/--
Prove that if $M$ is stably free and not finitely generated then $M$ is free.
-/
theorem stablyFree_iff_free_of_not_fg (R : Type) (M : Type) [CommRing R] [AddCommGroup M]
    [Module R M] (h : ¬ Module.Finite R M) : Module.Free R M ↔ IsStablyFree R M := by
  sorry

end Problem55
```

Exercise (56). *Let $R \to S$ be a faithfully flat ring map. Let M be an R-module. If the S-module $S \otimes_R M$ is projective, then M is projective.*

```
import Mathlib

namespace Problem56

/--
Let \( R \to S \) be a faithfully flat ring map. Let \( M \) be an \( R \)-module.
If the \( S \)-module \( S \otimes_{R} M \) is projective, then \( M \) is projective.
-/
theorem projective_of_faithfullyFlat_base_change (R S M : Type) [CommRing R] [CommRing S]
    [Algebra R S] [Module.FaithfullyFlat R S] [AddCommGroup M] [Module R M]
    [Module.Projective S (TensorProduct R S M)] : Module.Projective R M := by
  sorry

end Problem56
```

Exercise (57). *Let A be a domain and K its field of fractions. $x \in K$ is called almost integral if there exists an element $r \in A, r \neq 0$ such that $rx^n \in A$ for all $n \geq 0$. A is called completely integrally closed if every almost integral element of K is contained in A. Show that if A is completely integrally closed, so is $A[X]$.*

```
import Mathlib

namespace Problem57

/--
Let \( A \) be a domain and \( K \) its field of fractions.
\( x \in K \) is called almost integral if there exists an element \( r\in A, r \ne 0 \)
such that \( rx^n \in A \) for all \( n \ge 0 \).
-/
def IsAlmostIntegral {A : Type} [CommRing A] [IsDomain A] (x : FractionRing A) : Prop :=
  ∃ r : A, r ≠ 0 ∧ ∀ n : ℕ, ∃ y : A, r • (x ^ n) = algebraMap A (FractionRing A) y

/--
\( A \) is called \textit{completely integrally closed} if every almost integral element
of \( K \) is contained in \( A \).
-/
def IsCompletelyIntegrallyClosed (A : Type) [CommRing A] [IsDomain A] : Prop :=
  ∀ x : FractionRing A, IsAlmostIntegral x → ∃ y : A, x = algebraMap A (FractionRing A) y

/--
Let \( A \) be a domain. Show that if \( A \) is completely integrally closed, so is \( A[X] \).
-/
theorem completely_integrally_closed_polynomial_ring {A : Type} [CommRing A] [IsDomain A]
    (h : IsCompletelyIntegrallyClosed A) : IsCompletelyIntegrallyClosed (Polynomial A) := by
  sorry

end Problem57
```

Exercise (58). *Suppose that $(R, \mathfrak{P})$ is a local Noetherian ring, and let $(S, \mathfrak{Q})$ be a local Noetherian R-algebra such that $\mathfrak{P}S \subseteq \mathfrak{Q}$. If M is a finitely generated S-module, show that M is flat as an R-module if $M/\mathfrak{P}^n M$ is flat as an $R/\mathfrak{P}^n$-module for every n.*

```
import Mathlib

namespace Problem58

open TensorProduct

/--
Suppose that $(R, \mathfrak{P})$ is a local Noetherian ring,
and let $(S, \mathfrak{Q})$ be a local Noetherian $R$-algebra such that
$\mathfrak{P}S \subseteq \mathfrak{Q}$.
If $M$ is a finitely generated $S$-module, show that $M$ is flat as an $R$-module
if $M / \mathfrak{P}^n M$ is flat as an $R / \mathfrak{P}^n$-module for every $n$.
```

```
-/
theorem flat_of_flat_over_quotient (R S : Type) [CommRing R] [CommRing S]
    [IsLocalRing R] [IsLocalRing S] [IsNoetherianRing R] [IsNoetherianRing S] [Algebra R S]
    (h_map : Ideal.map (algebraMap R S) (IsLocalRing.maximalIdeal R) ≤ IsLocalRing.maximalIdeal S)
    (M : Type) [AddCommGroup M] [Module S M] [Module R M] [IsScalarTower R S M] [Module.Finite S M]
    (h_flat_quotient : ∀ (n : ℕ), Module.Flat (R / (IsLocalRing.maximalIdeal R) ^ n) ((R /
     (IsLocalRing.maximalIdeal R) ^ n) ⊗[R] M)) :
    Module.Flat R M := by
  sorry

end Problem58
```

Exercise (59). *Let k be a field, X and Y indeterminates, and suppose that α is a positive irrational number. Show the map $v : k[X,Y] \to \mathbb{R} \cup \{\infty\}$ defined by*

$$v\left(\sum c_{n,m} X^n Y^m\right) = \min\{n + m\alpha \mid c_{n,m} \neq 0\}$$

determines a valuation of $k(X,Y)$ with value group $\mathbb{Z} + \mathbb{Z}\alpha$.

```
import Mathlib

namespace Problem59

/--
Let \( k \) be a field, \( X \) and \( Y \) indeterminates, and suppose that \( \alpha \) is a
positive irrational number. Show the map \( v: k[X, Y] \rightarrow \mathbb{R} \cup \{\infty\} \)
defined by
\[
v\left(\sum c_{n,m} X^n Y^m\right) = \min\{n + m\alpha \mid c_{n,m} \neq 0\}
\]
determines a valuation of \( k(X, Y) \) with value group \( \mathbb{Z} + \mathbb{Z}\alpha \).
-/
theorem exists_unique_valuation_eq (α : ℝ) (h_pos : α > 0) (h_irr : Irrational α)
    (k : Type) [Field k] : ∃! (v : AddValuation (FractionRing (MvPolynomial (Fin 2) k)) (WithTop ℝ)),
    ∀ (f : MvPolynomial (Fin 2) k), v (algebraMap _ _ f) = Finset.inf (Finset.image (fun s ↦ ((s 0 +
     α * s 1) : WithTop ℝ)) f.support) id := by
  sorry

end Problem59
```

Exercise (60). *Let R be a Noetherian domain, and suppose that for every maximal ideal P of R the ring R_P is factorial. Let $I \subset R$ be an ideal. Prove that I is an invertible module iff I has pure codimension 1. (We say that an ideal I in a ring R has pure codimension 1 if every associated prime ideal of I has codimension 1. We include the case when I has no associated primes at all—that is, when $I = R$.)*

```
import Mathlib

namespace Problem60

open Problem60

/--
For a Noetherian domain \( R \), we say that an ideal \( I \subset R \) is invertible if
it is it not the zero ideal and there exists an ideal \( N \) such that \( N \cdot I \) is principal
and \( N \) is not the zero ideal.
-/
def Ideal.Invertible {R : Type} [CommRing R] [IsDomain R] (I : Ideal R) : Prop :=
    I ≠ ⊥ ∧ ∃ (N : Ideal R), (N * I).IsPrincipal ∧ N ≠ ⊥

/--
Let $R$ be a Noetherian domain, and suppose that for every maximal ideal $P$ of $R$ the ring $R_P$
is factorial. Let $I \subset R$ be an ideal. Prove that $I$ is an invertible module iff
$I$ has pure codimension $1$. (We say that an ideal $I$ in a ring $R$ has pure codimension $1$ if
every associated prime ideal of $I$ has codimension $1$. We include the case when $I$ has no
associated primes at all---that is, when $I = R$.)
-/
theorem invertible_iff_codimension_one (R : Type) [CommRing R] [IsDomain R] [IsNoetherianRing R]
    (h_ufd : ∀ (p : Ideal R), (h : p.IsMaximal) → UniqueFactorizationMonoid (Localization.AtPrime p))
    (I : Ideal R) : I.Invertible ↔ ∀ (p : associatedPrimes R I), ringKrullDim (R / p.1) = 1 := by
  sorry

end Problem60
```

Exercise (61). *Let $R \to S$ be a ring map. Let $I \subset R$ be an ideal. Assume*

1. $I^2 = 0$,
2. *$R \to S$ is flat, and*
3. *$R/I \to S/IS$ is formally smooth.*

Show $R \to S$ is formally smooth.

```
import Mathlib

namespace Problem61

/--
Let \( R \to S \) be a ring map. Let \( I \subset R \) be an ideal. Assume
\begin{enumerate}
    \item \( I^{2} = 0 \),
    \item \( R \to S \) is flat, and
    \item \( R/I \to S/IS \) is formally smooth.
\end{enumerate}
Show \( R \to S \) is formally smooth.
```

```
-/
theorem formallySmooth_of_formallySmooth_quotient (R S : Type) [CommRing R] [CommRing S]
    [Algebra R S] [Module.Flat R S] (I : Ideal R) (h : I ^ 2 = 0)
    [Algebra.FormallySmooth (R / I) (S / (I.map (algebraMap R S)))] :
    Algebra.FormallySmooth R S := by
  sorry

end Problem61
```

Exercise (62). *Let $\varphi : R \to S$ be a smooth ring map. Let $\sigma : S \to R$ be a left inverse to φ. Set $I = \operatorname{Ker}(\sigma)$. If I/I^2 is free, show $S^\wedge \cong R[[t_1, \ldots, t_d]]$ as R-algebras, where $S^\wedge$ is the I-adic completion of S.*

```
import Mathlib

namespace Problem62

/--
Let \( \varphi: R \to S \) be a smooth ring map. Let \( \sigma: S \to R \) be a left inverse
to \( \varphi \). Set \( I = \operatorname{Ker}(\sigma) \). If \( I / I^{2} \) is free,
show \( S^{\wedge} \cong R[[t_{1}, \ldots, t_{d}]] \) as \( R \)-algebras,
where \( S^{\wedge} \) is the \( I \)-adic completion of \( S \).
-/
theorem adicCompletion_equiv_of_smooth (R S : Type) [CommRing R] [CommRing S]
    [Algebra R S] [Algebra.Smooth R S] (σ : S →+* R)
    (h : Function.LeftInverse σ (algebraMap R S)) (hf : Module.Free R (RingHom.ker σ).Cotangent) :
    ∃ d : ℕ, Nonempty (AdicCompletion (RingHom.ker σ) S ≃ₐ[R] MvPowerSeries (Fin d) R) := by
  sorry

end Problem62
```

Exercise (63). *Let $R \to S$ be a formally unramified ring map. Show there exists a surjection of R-algebras $S' \to S$ whose kernel is an ideal of square zero with the following universal property: Given any commutative diagram*

$$\begin{tikzcd} S \arrow[r, "a"] & A/I \\ R \arrow[u] \arrow[r, "b"] & A \arrow[u] \end{tikzcd}$$

where $I \subset A$ is an ideal of square zero, there is a unique R-algebra map $\alpha' : S' \to A$ such that $S' \to A \to A/I$ is equal to $S' \to S \to A/I$.

```
import Mathlib

namespace Problem63

/--
```

```
The universal property:
Given any commutative diagram
\[
\begin{tikzcd}
S \arrow[r, "a"] & A/I \\
R \arrow[u] \arrow[r, "b"] & A \arrow[u]
\end{tikzcd}
\]
where \( I \subset A \) is an ideal of square zero, there is a unique \( R \)-algebra map
\( \alpha': S' \to A \) such that \( S' \to A \to A/I \) is equal to \( S' \to S \to A/I \).
-/
def UniversalProperty.liftOfSqZeroIdeal {R S S' : Type} [CommRing R] [CommRing S] [CommRing S']
    [Algebra R S] [Algebra R S'] (f : S' →ₐ[R] S) :=
  ∀ (A : Type) [CommRing A] [Algebra R A] (I : Ideal A) (g : S →ₐ[R] /AI),
  I^2 = 0 → (g.toRingHom.comp (algebraMap R S) = (Ideal.Quotient.mk I).comp (algebraMap R A)) →
  ∃! (g' : S' →ₐ[R] A), (Ideal.Quotient.mk I).comp g'.toRingHom  = g.comp f

/--
Let \( R \to S \) be a formally unramified ring map. Show there exists a surjection of
\( R \)-algebras \( S' \to S \) whose kernel is an ideal of square zero with the following
universal property:
Given any commutative diagram
\[
\begin{tikzcd}
S \arrow[r, "a"] & A/I \\
R \arrow[u] \arrow[r, "b"] & A \arrow[u]
\end{tikzcd}
\]
where \( I \subset A \) is an ideal of square zero, there is a unique \( R \)-algebra map
\( \alpha': S' \to A \) such that \( S' \to A \to A/I \) is equal to \( S' \to S \to A/I \).
-/
theorem surjection_of_formally_unramified (R S : Type) [CommRing R] [CommRing S]
    [Algebra R S] [Algebra.FormallyUnramified R S] :
    ∃ (S' : Type) (_ : CommRing S') (_ : Algebra R S') (f : S' →ₐ[R] S), (RingHom.ker f) ^ 2 = 0 ∧
     UniversalProperty.liftOfSqZeroIdeal f := by
  sorry

end Problem63
```

Exercise (64). *Prove that the homogeneous coordinate ring of a smooth rational quartic in three-space*

$$R = k[s^4, s^3t, st^3, t^4] \subset k[s,t]$$

is not Cohen-Macaulay.

```
import Mathlib

namespace Problem64

section
```

```
open CategoryTheory Abelian Problem64

variable {R : Type} [CommRing R]

instance : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives (ModuleCat R)

noncomputable def moduleDepth (N M : ModuleCat.{0} R) : ℕ∞ :=
  sSup {n : ℕ∞ | ∀ i : ℕ, i < n → Subsingleton (CategoryTheory.Abelian.Ext.{0} N M i)}

noncomputable def Ideal.depth (I : Ideal R) (M : ModuleCat.{0} R) : ℕ∞ :=
  moduleDepth (ModuleCat.of R (R ⧸ I)) M

noncomputable def IsLocalRing.depth [IsLocalRing R] (M : ModuleCat.{0} R) : ℕ∞ :=
  (IsLocalRing.maximalIdeal R).depth M

variable (R)

class IsCohenMacaulayLocalRing : Prop extends IsLocalRing R where
  depth_eq_dim : ringKrullDim R = IsLocalRing.depth (ModuleCat.of R R)

class IsCohenMacaulayRing : Prop where
  CM_localize : ∀ p : Ideal R, ∀ (_ : p.IsPrime), IsCohenMacaulayLocalRing (Localization.AtPrime p)

end

open MvPolynomial

/--
Prove that the homogeneous coordinate ring of a smooth rational quartic in three-space
\[
R=k[s^4, s^3t, st^3, t^4] \subset k[s,t]
\]
is not Cohen-Macaulay.
-/
theorem homogeneous_coordinate_ring_not_isCohenMacaulayRing (k : Type) [Field k] :
    ¬ IsCohenMacaulayRing (Algebra.adjoin k ({(X 0) ^ 4, (X 0) ^ 3 * X 1,
      X 0 * (X 1) ^ 3, (X 1) ^ 4} : Set (MvPolynomial (Fin 2) k))) := by
  sorry

end Problem64
```

Exercise (65). *If A is a Neotherian Gorenstein ring, then so is the polynomial ring $A[X]$.*

```
import Mathlib

namespace Problem65

open IsLocalRing ModuleCat CategoryTheory Polynomial

instance (R : Type) [CommRing R] : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives.{0} (ModuleCat.{0} R)
```

```
/--
A Noetherian local ring $R$ is a Gorenstein ring if $\mathrm{inj}.\dim_R R < +\infty$.
-/
class IsGorensteinLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  injDim_le_infity :
    ∃ n : ℕ, ∀ i : ℕ, n ≤ i →
    Subsingleton (Abelian.Ext.{0} (of.{0} R (ResidueField R)) (of.{0} R R) i)

/--
A Noetherian ring is a Gorenstein ring if its localization at every maximal ideal is a
  Gorenstein local ring.
-/
class IsGorensteinRing (R : Type) [CommRing R] : Prop extends IsNoetherianRing R where
  localization_maximal_isGorensteinLocalRing :
    ∀ m : Ideal R, (_ : m.IsMaximal) → IsGorensteinLocalRing (Localization.AtPrime m)

/--
If \( A \) is a Neotherian Gorenstein ring, then so is the polynomial ring \( A[X] \).
-/
theorem Polynomial.isGorensteinRing {R : Type} [CommRing R] [IsGorensteinRing R] :
    IsGorensteinRing R[X] := by
  sorry

end Problem65
```

Exercise (66). *Show that if an ideal I in a Noetherian ring R can be generated by a regular sequence, then it can be generated by a set of elements that is a regular sequence in any order.*

```
import Mathlib

namespace Problem66

open RingTheory

/--
Show that if an ideal $I$ in a Noetherian ring $R$ can be generated by a regular sequence,
then it can be generated by a set of elements that is a regular sequence in any order.
-/
theorem exists_eq_ofList_and_isRegular_of_perm {R : Type} [CommRing R] [IsNoetherianRing R] (I :
     Ideal R) (rs : List R)
    (gen : I = Ideal.ofList rs) (h₂ : Sequence.IsRegular R rs) : ∃ rs' : List R,
    I = Ideal.ofList rs' ∧ (∀ l : List R, (l.Perm rs') → Sequence.IsRegular R l) := by
  sorry

end Problem66
```

Exercise (67). *Let A be the ring $k[[x_1, \ldots, x_n]]$, where k is a field, $n \in \mathbb{N}$, $n \neq 0$. Show that there is **no** isomorphism*

$$A \otimes_k A \cong k[[x_1, \ldots, x_n, y_1, \ldots, y_n]].$$

```lean
import Mathlib

namespace Problem67

open scoped TensorProduct

/--
Let $A$ be the ring $k[[x_1, \dots, x_n]]$, where $k$ is a field, $n \in \mathbb{N}$, $n \ne 0$.
Show that there is \textbf{no} isomorphism
\[
A \otimes_k A \cong k[[x_1, \dots, x_n, y_1, \dots, y_n]].
\]
-/
theorem isEmpty_mvPowerSeries_tensor_mvPowerSeries_algEquiv
    {k : Type} [Field k] (n : ℕ) (hn : n ≠ 0) :
    IsEmpty ((MvPowerSeries (Fin n) k) ⊗[k] (MvPowerSeries (Fin n) k) ≃ₐ[k]
    (MvPowerSeries (Fin (n + n)) k)) := by
  sorry

end Problem67
```

Exercise (68). *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. For any $f \in \mathfrak{m}$ such that f is not nilpotent, A_f is Jacobson.*

```lean
import Mathlib

namespace Problem68

/--
Let $A$ be a Noetherian local ring with maximal ideal $\mathfrak{m}$.
For any $f\in \mathfrak{m}$ such that $f$ is not nilpotent, $A_f$ is Jacobson.
-/
theorem localization_jacobson_of_one_lt_ringKrullDim (R : Type) [CommRing R] [IsLocalRing R]
    [IsNoetherianRing R] (f : R) (hf : f ∈ IsLocalRing.maximalIdeal R) (ne0 : ¬ IsNilpotent f) :
    IsJacobsonRing (Localization.Away f) := by
  sorry

end Problem68
```

Exercise (69). *If R is a regular local ring with maximal ideal $\mathfrak{m}$ and $P \in \mathrm{Spec}(R[x])$ is a prime ideal with $\mathfrak{m} = P \cap R$, then $R[x]_P$ is regular.*

```lean
import Mathlib

namespace Problem69

open IsLocalRing Polynomial

/--
```

```
A commutative local noetherian ring $R$ is regular if $\dim m/m^2 = \dim R$.
-/
class IsRegularLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  reg : Module.finrank (ResidueField R) (CotangentSpace R) = ringKrullDim R

/--
Let \( A \) be a Noetherian ring.
If \( R \) is a regular local ring with maximal ideal \( \mathfrak{m} \) and
\( P \in \operatorname{Spec}(R[x]) \) is a prime ideal with \( \mathfrak{m} = P \cap R \),
then \( R[x]_P \) is regular.
-/
theorem IsRegularLocalRing.regularAtPrime {R : Type} [CommRing R] [IsRegularLocalRing R]
    (P : Ideal R[X]) [P.IsPrime] [P.LiesOver (maximalIdeal R)] :
    IsRegularLocalRing (Localization.AtPrime P) := by
  sorry

end Problem69
```

Exercise (70). *All rings considered are noetherian. Show that if R is an integral domain contained in the local ring (S, Q), then there is a minimal prime of S contracting to 0 in R.*

```
import Mathlib

namespace Problem70

/--
All rings considered are noetherian.
Show that if \( R \) is an integral domain contained in the local ring \( (S, Q) \),
then there is a minimal prime of \( S \) contracting to \( 0 \) in \( R \).
-/
theorem exists_minimalPrime_map_zero (R S : Type) [CommRing R] [IsDomain R] [IsNoetherianRing R]
    [CommRing S] [IsNoetherianRing S] [IsLocalRing S] [Algebra R S] [NoZeroSMulDivisors R S] :
    ∃ (p : minimalPrimes S), Ideal.comap (algebraMap R S) p.1 = ⊥ := by
  sorry

end Problem70
```

Exercise (71). *Let G be a finite group acting as automorphisms of an algebra R over a field of characteristic 0. Show that if R is Cohen-Macaulay, then the ring of invariants R^G is Cohen-Macaulay.*

```
import Mathlib

namespace Problem71

section

variable (A B : Type) [CommRing A] [CommRing B] [Algebra A B]
```

```
variable (G : Type) [Monoid G] [MulSemiringAction G B] [SMulCommClass G A B]

/--
The set of fixed points under a group action, as a subring.
-/
def FixedPoints.subring : Subring B where
  __ := FixedPoints.addSubgroup G B
  __ := FixedPoints.submonoid G B

/--
The set of fixed points under a group action, as a subalgebra.
-/
def FixedPoints.subalgebra : Subalgebra A B where
  __ := FixedPoints.addSubgroup G B
  __ := FixedPoints.submonoid G B
  algebraMap_mem' r := by simp

end

section

open CategoryTheory Abelian Problem71

variable {R : Type} [CommRing R]

instance : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives (ModuleCat R)

noncomputable def moduleDepth (N M : ModuleCat.{0} R) : ℕ∞ :=
  sSup {n : ℕ∞ | ∀ i : ℕ, i < n → Subsingleton (CategoryTheory.Abelian.Ext.{0} N M i)}

noncomputable def Ideal.depth (I : Ideal R) (M : ModuleCat.{0} R) : ℕ∞ :=
  moduleDepth (ModuleCat.of R (R ⧸ I)) M

noncomputable def IsLocalRing.depth [IsLocalRing R] (M : ModuleCat.{0} R) : ℕ∞ :=
  (IsLocalRing.maximalIdeal R).depth M

variable (R)

class IsCohenMacaulayLocalRing : Prop extends IsLocalRing R where
  depth_eq_dim : ringKrullDim R = IsLocalRing.depth (ModuleCat.of R R)

class IsCohenMacaulayRing : Prop where
  CM_localize : ∀ p : Ideal R, ∀ (_ : p.IsPrime), IsCohenMacaulayLocalRing (Localization.AtPrime p)

end

/--
Let \( G \) be a finite group acting as automorphisms of an algebra \( R \) over a field of
characteristic \( 0 \). Show that if \( R \) is Cohen-Macaulay, then the ring of invariants
\( R^G \) is Cohen-Macaulay.
-/
theorem fixedPoints_isCohenMacaulayRing {R : Type} [CommRing R] (k : Type) [Field k]
```

```
    [CharZero k] [Algebra k R] [IsNoetherianRing R] [IsCohenMacaulayRing R]
    (G : Subgroup (R ≃ₐ[k] R)) [Finite G] :
    IsCohenMacaulayRing (FixedPoints.subalgebra k R G) := by
  sorry

end Problem71
```

Exercise (72). *Let R be a Noetherian ring. Let M be a Cohen-Macaulay module over R. Then $M \otimes_R R[x_1, \ldots, x_n]$ is a Cohen-Macaulay module over $R[x_1, \ldots, x_n]$.*

```
import Mathlib

namespace Problem72

/--
The krull dimension of module, defined as `krullDim` of its support.
-/
noncomputable def Module.supportDim (R : Type) [CommRing R] (M : Type) [AddCommGroup M]
    [Module R M] : WithBot ℕ∞ :=
  Order.krullDim (Module.support R M)

section

open CategoryTheory Abelian Problem72

variable {R : Type} [CommRing R]

instance : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives (ModuleCat R)

noncomputable def moduleDepth (N M : ModuleCat.{0} R) : ℕ∞ :=
  sSup {n : ℕ∞ | ∀ i : ℕ, i < n → Subsingleton (CategoryTheory.Abelian.Ext.{0} N M i)}

noncomputable def Ideal.depth (I : Ideal R) (M : ModuleCat.{0} R) : ℕ∞ :=
  moduleDepth (ModuleCat.of R (R ⧸ I)) M

noncomputable def IsLocalRing.depth [IsLocalRing R] (M : ModuleCat.{0} R) : ℕ∞ :=
  (IsLocalRing.maximalIdeal R).depth M

class ModuleCat.IsCohenMacaulay [IsLocalRing R] (M : ModuleCat.{0} R) : Prop where
  depth_eq_dim : Subsingleton M ∨ Module.supportDim R M = IsLocalRing.depth M

variable (R)

class Module.IsCohenMacaulay (M : Type) [AddCommGroup M] [Module R M] : Prop where
  depth_eq_dim : ∀ p : Ideal R, ∀ (_ : p.IsPrime), (ModuleCat.of (Localization.AtPrime p)
    (LocalizedModule.AtPrime p M)).IsCohenMacaulay

end

open TensorProduct
```

```
noncomputable instance (R : Type) [CommRing R] (M : Type) [AddCommGroup M] [Module R M] (n : ℕ) :
    Module (MvPolynomial (Fin n) R) ((MvPolynomial (Fin n) R) ⊗[R] M) := leftModule

/--
Let \( R \) be a Noetherian ring. Let \( M \) be a Cohen-Macaulay module over \( R \).
Then \( M \otimes_R R[x_1, \dots, x_n] \) is a Cohen-Macaulay module over \( R[x_1, \dots, x_n] \).
-/
theorem isCohenMacaulay_extendScalars_over_mvPolynomial_of_isCohenMacaulay
    (R : Type) [CommRing R] (M : Type) [AddCommGroup M] [Module R M]
    [IsNoetherianRing R] [Module.IsCohenMacaulay R M] (n : ℕ) :
    Module.IsCohenMacaulay (MvPolynomial (Fin n) R) ((MvPolynomial (Fin n) R) ⊗[R] M) := by
  sorry

end Problem72
```

Exercise (73). *If I is an homogeneous ideal of $k[x_0, \dots, x_n]$, $R = k[x_0, \dots, x_n]/I$, then R is Cohen-Macaulay if and only if R_P is Cohen-Macaulay, where $P = (x_0, \dots, x_n)$.*

```
import Mathlib

namespace Problem73

section

open CategoryTheory Abelian Problem73

variable {R : Type} [CommRing R]

instance : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives (ModuleCat R)

noncomputable def moduleDepth (N M : ModuleCat.{0} R) : ℕ∞ :=
  sSup {n : ℕ∞ | ∀ i : ℕ, i < n → Subsingleton (CategoryTheory.Abelian.Ext.{0} N M i)}

noncomputable def Ideal.depth (I : Ideal R) (M : ModuleCat.{0} R) : ℕ∞ :=
  moduleDepth (ModuleCat.of R (R / I)) M

noncomputable def IsLocalRing.depth [IsLocalRing R] (M : ModuleCat.{0} R) : ℕ∞ :=
  (IsLocalRing.maximalIdeal R).depth M

variable (R)

class IsCohenMacaulayLocalRing : Prop extends IsLocalRing R where
  depth_eq_dim : ringKrullDim R = IsLocalRing.depth (ModuleCat.of R R)

class IsCohenMacaulayRing : Prop where
  CM_localize : ∀ p : Ideal R, ∀ (_ : p.IsPrime), IsCohenMacaulayLocalRing (Localization.AtPrime p)

end

attribute [local instance] MvPolynomial.gradedAlgebra
```

```
/--
If $I$ is an homogeneous ideal of $k[x_0, \dots, x_n]$, \( R = k[x_0, \dots, x_n]/I \),
then \( R \) is Cohen-Macaulay if and only if \( R_P \) is Cohen-Macaulay, where
\( P = (x_0, \dots, x_n) \).
-/
theorem mvPolynomial_quotient_isCohenMacaulayRing_iff (k : Type) [Field k] (n : ℕ)
    (R : Type) [CommRing R] (f : (MvPolynomial (Fin n) k) →+* R) (surj : Function.Surjective f)
    (homo : (RingHom.ker f).IsHomogeneous (MvPolynomial.homogeneousSubmodule (Fin n) k))
    (le : RingHom.ker f ≤ RingHom.ker MvPolynomial.constantCoeff) :
    IsCohenMacaulayRing R ↔
    IsCohenMacaulayRing (Localization.AtPrime ((RingHom.ker MvPolynomial.constantCoeff).map f)
      (hp := Ideal.map_isPrime_of_surjective surj le (H := RingHom.ker_isPrime _))) := by
  sorry

end Problem73
```

Exercise (74). *Let R be a regular local ring and let $x_1, \dots, x_c$ be a regular sequence in R. Let $y \in R$, $y \notin (x_1, \dots, x_c)$, and set $J := ((x_1, \dots, x_c) : y)$. Prove that R/J is Gorenstein.*

```
import Mathlib

namespace Problem74

open IsLocalRing ModuleCat CategoryTheory

instance (R : Type) [CommRing R] : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives.{0} (ModuleCat.{0} R)

/--
A commutative local noetherian ring $R$ is regular if $\dim m/m^2 = \dim R$.
-/
class IsRegularLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  reg : Module.finrank (ResidueField R) (CotangentSpace R) = ringKrullDim R

/--
A Noetherian local ring $R$ is a Gorenstein ring if $\mathrm{inj}.\dim_R R < +\infty$.
-/
class IsGorensteinLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  injDim_le_infity :
    ∃ n : ℕ, ∀ i : ℕ, n ≤ i →
    Subsingleton (Abelian.Ext.{0} (of.{0} R (ResidueField R)) (of.{0} R R) i)

/--
A Noetherian ring is a Gorenstein ring if its localization at every maximal ideal is a
  Gorenstein local ring.
-/
class IsGorensteinRing (R : Type) [CommRing R] : Prop extends IsNoetherianRing R where
  localization_maximal_isGorensteinLocalRing :
    ∀ m : Ideal R, (_ : m.IsMaximal) → IsGorensteinLocalRing (Localization.AtPrime m)
variable {R : Type} [CommRing R]
```

```
/--
Let $R$ be a regular local ring and let $x_1, \dots, x_c$ be a regular sequence in $R$.
Let $y \in R$, $y \notin (x_1, \dots, x_c)$, and set $J := ((x_1, \dots, x_c) : y)$. P
rove that $R/J$ is Gorenstein.
-/
theorem IsRegularLocalRing.gorensteinAtRegularSequence {R : Type} [CommRing R]
    [IsRegularLocalRing R] {rs : List R} (reg : RingTheory.Sequence.IsRegular R rs) (y : R)
    (h : y ∉ Ideal.ofList rs) : IsGorensteinRing (R / (Ideal.ofList rs / Ideal.span {y})) := by
  sorry

end Problem74
```

Exercise (75). *Let A be a graded Noetherian ring, with A_0 a field and A generated by A_1. Show that A is Cohen-Macaulay if and only if for all homogeneously prime $\mathfrak{p}$, $(A_{\mathfrak{p}})_0$ is Cohen-Macaulay.*

```
import Mathlib

namespace Problem75

open IsLocalRing ModuleCat CategoryTheory Problem75

section

variable {R : Type} [CommRing R]

instance : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives (ModuleCat R)

noncomputable def moduleDepth (N M : ModuleCat.{0} R) : ℕ∞ :=
  sSup {n : ℕ∞ | ∀ i : ℕ, i < n → Subsingleton (CategoryTheory.Abelian.Ext.{0} N M i)}

noncomputable def Ideal.depth (I : Ideal R) (M : ModuleCat.{0} R) : ℕ∞ :=
  moduleDepth (ModuleCat.of R (R / I)) M

noncomputable def IsLocalRing.depth [IsLocalRing R] (M : ModuleCat.{0} R) : ℕ∞ :=
  (IsLocalRing.maximalIdeal R).depth M

variable (R)

class IsCohenMacaulayLocalRing : Prop extends IsLocalRing R where
  depth_eq_dim : ringKrullDim R = IsLocalRing.depth (ModuleCat.of R R)

class IsCohenMacaulayRing : Prop where
  CM_localize : ∀ p : Ideal R, ∀ (_ : p.IsPrime), IsCohenMacaulayLocalRing (Localization.AtPrime p)

end

/--
Let $A$ be a graded Noetherian ring, with $A_0$ a field and $A$ generated by $A_1$.
Show that $A$ is Cohen-Macaulay if and only if for all homogeneously prime $\mathfrak{p}$,
$(A_{\mathfrak{p}})_0$ is Cohen-Macaulay.
```

```
-/
theorem gradedAlgebra_isCohenMacaulay_iff_homogeneously_localize {A : Type} [CommRing A]
    [IsNoetherianRing A]
   (𝒜 : ℕ → Submodule ℤ A) [GradedAlgebra 𝒜] (h : IsField (𝒜 0)) (h1 : Algebra.adjoin (𝒜 0) (𝒜
    1) = (⊤ : Subalgebra (𝒜 0) A)) : IsCohenMacaulayRing A ↔
   ∀ p : Ideal A, (_ : p.IsPrime) → p.IsHomogeneous 𝒜 →
   IsCohenMacaulayLocalRing (HomogeneousLocalization.AtPrime 𝒜 p) := by
  sorry

end Problem75
```

Exercise (76). *Let A be a Noetherian UFD of dimension $d \leq 3$. Prove that A is catenary.*

```
import Mathlib

namespace Problem76

open List

/--
A ring $R$ is said to be \textit{catenary} if for any pair of prime ideals $\mathfrak{p} \subset
  \mathfrak{q}$, there exists an integer bounding the lengths of all finite chains of prime ideals
  $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_e =
  \mathfrak{q}$ and all maximal such chains have the same length.
-/
def IsCatenary (R : Type) [CommRing R] : Prop :=
  ∀ p q : PrimeSpectrum R, p ≤ q →
  ∃ n : ℕ, ∀ (l : LTSeries (PrimeSpectrum R)), l.head = p → l.last = q →
  (∀ l' : LTSeries (PrimeSpectrum R), l'.head = p → l'.last = q → l.toList <+ l'.toList → l' = l) →
  l.toList.length = n

/--
Let $A$ be a Noetherian UFD of dimension $d \leq 3$. Prove that $A$ is catenary.
-/
theorem IsCatenary.of_noetherian_ufd_of_dim_le_three {A : Type} [CommRing A] [IsNoetherianRing A]
   [IsDomain A] [UniqueFactorizationMonoid A] (h : ringKrullDim A ≤ 3) : IsCatenary A := by
  sorry

end Problem76
```

Exercise (77). *Let A be a Noetherian ring, $P \subset Q$ prime ideals such that $\operatorname{ht} P = h$, $\operatorname{ht} Q/P = d$, where $d > 1$. Prove that there exist infinitely many intermediate primes P', $P \subset P' \subset Q$ such that $\operatorname{ht} P' = h + 1$ and $\operatorname{ht} Q/P' = d - 1$.*

```
import Mathlib

namespace Problem77

/--
```

```
Let $A$ be a Noetherian ring, $P \subset Q$ prime ideals such that
$\operatorname{ht} P = h$, $\operatorname{ht} Q/P = d$, where $d > 1$.
Prove that there exist infinitely many intermediate primes $P'$, $P \subset P' \subset Q$
such that $\operatorname{ht} P' = h + 1$ and $\operatorname{ht} Q/P' = d - 1$.
-/
theorem infinite_intermediate_primes (R : Type) [CommRing R] [IsNoetherianRing R] (P Q : Ideal R)
    (le : P ≤ Q) [P.IsPrime] [Q.IsPrime] (h d : ℕ) (lt : 1 < d) (ht1 : P.height = h)
    (ht2 : (Q.map (Ideal.Quotient.mk P)).height = d) :
    {P' : Ideal R | P ≤ P' ∧ P' ≤ Q ∧ P'.IsPrime ∧ P'.height = h + 1 ∧
      (Q.map (Ideal.Quotient.mk P')).height = d - 1}.Infinite := by
  sorry

end Problem77
```

Exercise (78). *Let A be a local Cohen–Macaulay (CM) ring that is a quotient of a regular local ring. If A is a UFD, then A is Gorenstein.*

```
import Mathlib

namespace Problem78

open IsLocalRing ModuleCat CategoryTheory Problem78

section

variable {R : Type} [CommRing R]

instance : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives (ModuleCat R)

noncomputable def moduleDepth (N M : ModuleCat.{0} R) : ℕ∞ :=
  sSup {n : ℕ∞ | ∀ i : ℕ, i < n → Subsingleton (CategoryTheory.Abelian.Ext.{0} N M i)}

noncomputable def Ideal.depth (I : Ideal R) (M : ModuleCat.{0} R) : ℕ∞ :=
  moduleDepth (ModuleCat.of R (R / I)) M

noncomputable def IsLocalRing.depth [IsLocalRing R] (M : ModuleCat.{0} R) : ℕ∞ :=
  (IsLocalRing.maximalIdeal R).depth M

variable (R)

class IsCohenMacaulayLocalRing : Prop extends IsLocalRing R where
  depth_eq_dim : ringKrullDim R = IsLocalRing.depth (ModuleCat.of R R)

class IsCohenMacaulayRing : Prop where
  CM_localize : ∀ p : Ideal R, ∀ (_ : p.IsPrime), IsCohenMacaulayLocalRing (Localization.AtPrime p)

end

/--
A commutative local noetherian ring $R$ is regular if $\dim m/m^2 = \dim R$.
-/
```

```
class IsRegularLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  reg : Module.finrank (ResidueField R) (CotangentSpace R) = ringKrullDim R

/--
A Noetherian local ring $R$ is a Gorenstein ring if $\mathrm{inj}.\dim_R R < +\infty$.
-/
class IsGorensteinLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  injDim_le_infity :
    ∃ n : ℕ, ∀ i : ℕ, n ≤ i →
    Subsingleton (Abelian.Ext.{0} (of.{0} R (ResidueField R)) (of.{0} R R) i)

/--
A Noetherian ring is a Gorenstein ring if its localization at every maximal ideal is a
  Gorenstein local ring.
-/
class IsGorensteinRing (R : Type) [CommRing R] : Prop extends IsNoetherianRing R where
  localization_maximal_isGorensteinLocalRing :
    ∀ m : Ideal R, (_ : m.IsMaximal) → IsGorensteinLocalRing (Localization.AtPrime m)

/--
Let $A$ be a local Cohen–Macaulay (CM) ring that is a quotient of a regular local ring.
If $A$ is a UFD, then $A$ is Gorenstein.
-/
theorem IsCohenMacaulayLocalRing.isGorensteinRing_of_ufd {A B : Type} [CommRing A]
    [IsCohenMacaulayLocalRing A] [IsDomain A] [UniqueFactorizationMonoid A] [CommRing B]
    [IsRegularLocalRing B] {f : B →+* A} (hf : Function.Surjective f) :
    IsGorensteinRing A := by
  sorry

end Problem78
```

Exercise (79). *Let B be a regular local ring and $I \subset B$ an ideal such that B/I is Gorenstein but not a complete intersection. Show that I cannot have height* 0 *or* 1.

```
import Mathlib

namespace Problem79

open IsLocalRing ModuleCat CategoryTheory

instance (R : Type) [CommRing R] : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives.{0} (ModuleCat.{0} R)

/--
A commutative local noetherian ring $R$ is regular if $\dim m/m^2 = \dim R$.
-/
class IsRegularLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  reg : Module.finrank (ResidueField R) (CotangentSpace R) = ringKrullDim R
```

```
/--
A Noetherian local ring $R$ is a Gorenstein ring if $\mathrm{inj}.\dim_R R < +\infty$.
-/
class IsGorensteinLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  injDim_le_infity :
    ∃ n : ℕ, ∀ i : ℕ, n ≤ i →
    Subsingleton (Abelian.Ext.{0} (of.{0} R (ResidueField R)) (of.{0} R R) i)

/--
A Noetherian ring is a Gorenstein ring if its localization at every maximal ideal is a
  Gorenstein local ring.
-/
class IsGorensteinRing (R : Type) [CommRing R] : Prop extends IsNoetherianRing R where
  localization_maximal_isGorensteinLocalRing :
    ∀ m : Ideal R, (_ : m.IsMaximal) → IsGorensteinLocalRing (Localization.AtPrime m)

/--
A Noetherian local ring $A$ is a local complete intersection if every surjection of local rings
$R \to \widehat{A}$ with $R$ a regular local ring, the kernel of $R \to \hat{A}$ is generated by a
regular sequence.
-/
@[stacks 09Q3]
class IsLocalCompleteIntersectionRing (A : Type) [CommRing A] : Prop extends
    IsLocalRing A, IsNoetherianRing A where
  out (R : Type) [CommRing R] [IsRegularLocalRing R]
    (f : R →+* (AdicCompletion (maximalIdeal A) A)) (_ : IsLocalHom f) (_ : Function.Surjective f) :
      ∃ (rs : List R), RingTheory.Sequence.IsRegular R rs ∧ RingHom.ker f = Ideal.ofList rs

/--
Let $B$ be a regular local ring and $I \subset B$ an ideal such that
$B/I$ is Gorenstein but not a local complete intersection.
Show that $I$ cannot have height $0$ or $1$.
-/
theorem IsLocalRing.not_isCompleteIntersection.height_not_zero_and_not_one (B : Type) [CommRing B]
    [IsRegularLocalRing B] (I : Ideal B) [IsGorensteinRing (B / I)]
    (hc : ¬ IsLocalCompleteIntersectionRing (B / I)) : I.height ≠ 0 ∧ I.height ≠ 1 := by
  sorry

end Problem79
```

Exercise (80). *Consider the ideal $I \subset k[x_1, \ldots, x_6]$ generated by the following polynomials:*

$$f_1 = x_2x_4 + x_3x_6,$$

$$f_2 = x_3x_5 + x_1x_6,$$

$$f_3 = x_1x_2 - x_2x_5 + x_3x_5 - x_5x_6,$$

$$f_4 = x_2x_3 + x_2x_4 + x_2x_6 + x_6^2,$$

$$f_5 = x_3^2 + x_3x_4 + x_3x_6 - x_4x_6,$$

$$f_6 = x_1x_3 + x_1x_4 + x_4x_5 + x_1x_6.$$

Prove that R/I is Cohen–Macaulay of dimension 3.

```
import Mathlib

namespace Problem80

section

open CategoryTheory Abelian Problem80

variable {R : Type} [CommRing R]

instance : CategoryTheory.HasExt.{0} (ModuleCat.{0} R) :=
  CategoryTheory.hasExt_of_enoughProjectives (ModuleCat R)

noncomputable def moduleDepth (N M : ModuleCat.{0} R) : ℕ∞ :=
  sSup {n : ℕ∞ | ∀ i : ℕ, i < n → Subsingleton (CategoryTheory.Abelian.Ext.{0} N M i)}

noncomputable def Ideal.depth (I : Ideal R) (M : ModuleCat.{0} R) : ℕ∞ :=
  moduleDepth (ModuleCat.of R (R / I)) M

noncomputable def IsLocalRing.depth [IsLocalRing R] (M : ModuleCat.{0} R) : ℕ∞ :=
  (IsLocalRing.maximalIdeal R).depth M

variable (R)

class IsCohenMacaulayLocalRing : Prop extends IsLocalRing R where
  depth_eq_dim : ringKrullDim R = IsLocalRing.depth (ModuleCat.of R R)

class IsCohenMacaulayRing : Prop where
  CM_localize : ∀ p : Ideal R, ∀ (_ : p.IsPrime), IsCohenMacaulayLocalRing (Localization.AtPrime p)

end

open MvPolynomial

abbrev target_ring_aux (k : Type) [Field k] :=
    (MvPolynomial (Fin 6) k) / Ideal.span ({
    X 1 * X 3 + X 2 * X 5, X 2 * X 4 + X 0 * X 5, X 0 * X 1 - X 1 * X 4 + X 2 * X 4 - X 4 * X 5,
    X 1 * X 2 + X 1 * X 3 + X 1 * X 5 + (X 5)^2, (X 2)^2 + X 2 * X 3 + X 2 * X 5 - X 3 * X 5,
    X 0 * X 2 + X 0 * X 3 + X 3 * X 4 + X 0 * X 5} : Set (MvPolynomial (Fin 6) k))

/--
Consider the ideal \( I \subset k[x_1, \dots, x_6] \) generated by the following polynomials:
\[
\begin{aligned}
f_1 &= x_2x_4 + x_3x_6, \\
f_2 &= x_3x_5 + x_1x_6, \\
f_3 &= x_1x_2 - x_2x_5 + x_3x_5 - x_5x_6, \\
f_4 &= x_2x_3 + x_2x_4 + x_2x_6 + x_6^2, \\
f_5 &= x_3^2 + x_3x_4 + x_3x_6 - x_4x_6, \\
f_6 &= x_1x_3 + x_1x_4 + x_4x_5 + x_1x_6.
\end{aligned}
```

```
\]
Prove that \( R/I \) is Cohen–Macaulay of dimension \( 3 \).
-/
theorem isCohenMacaulayRing_of_dimension_three (k : Type) [Field k] :
    IsCohenMacaulayRing (target_ring_aux k) ∧ (ringKrullDim (target_ring_aux k) = 3) := by
  sorry

end Problem80
```

Exercise (81). *Let A be a local Noetherian ring, $I \subset A$ an ideal. Show that I is generated by a regular sequence if and only if I/I^2 is free over A/I and $\operatorname{pd}_A I < \infty$.*

```
import Mathlib

namespace Problem81

/--
Let \( A \) be a local Noetherian ring, \( I \subset A \) an ideal. Show that
\( I \) is generated by a regular sequence if and only if \( I/I^2 \) is free over \( A/I \) and
\( \operatorname{pd}_A I < \infty \).
-/
theorem generated_by_regular_sequence_iff (R : Type) [CommRing R] [IsLocalRing R]
    [IsNoetherianRing R] (I : Ideal R) (netop : I ≠ ⊤) :
    ∃ (rs : List R), (RingTheory.Sequence.IsRegular R rs) ∧ Ideal.ofList rs = I ↔
    Module.Free (R ⧸ I) I.Cotangent ∧
    (∃ n, CategoryTheory.HasProjectiveDimensionLE (ModuleCat.of R I) n) := by
  sorry

end Problem81
```

Exercise (82). *Let A be a Noetherian complete local ring of dimension d, of mixed characteristic (i.e., $\mathrm{Char} A = 0$ and $\mathrm{Char} A/\mathfrak{m}$), and let $p = char(A/\mathfrak{m})$. Assume that $ht(p \cdot A) = 1$. Prove that A is a finitely generated module over a subring $B \subset A$ such that*

$$B \cong C[[x_1, \dots, x_{d-1}]],$$

where C is a discrete valuation ring (DVR).

```
import Mathlib

namespace Problem82

open IsLocalRing

/--
Let \( A \) be a Noetherian complete local ring of dimension \( d \), of mixed characteristic
(i.e., $\mathrm{Char} A = 0$ and $\mathrm{Char} A / \mathfrak{m}$), and let
\( p = \text{char}(A/\mathfrak{m}) \). Assume that \( \text{ht}(p \cdot A) = 1 \).
```

```
Prove that \( A \) is a finitely generated module over a subring \( B \subset A \) such that
\[
B \cong C[[x_1, \dots, x_{d-1}]],
\]
where \( C \) is a discrete valuation ring (DVR).
-/
theorem subring_iso_mvPowerSeries_over_DVR (d : ℕ) (A : Type) [CommRing A] [IsLocalRing A]
    [IsNoetherianRing A] [IsAdicComplete (maximalIdeal A) A] (dim : ringKrullDim A = d)
    {p : ℕ} (hp : p.Prime) [CharZero A] [CharP (ResidueField A) p]
    (ht : (Ideal.span {(p : A)}).height = 1) :
    ∃ B : Subring A, Module.Finite B A ∧
    ∃ (C : Type) (_ : CommRing C) (_ : IsDomain C), IsDiscreteValuationRing C ∧
    Nonempty (B ≃+* MvPowerSeries (Fin (d - 1)) C) := by
  sorry

end Problem82
```

Exercise (83). *Let $f\colon A \to B$ be a flat local homomorphism of Noetherian rings, having maximal ideals $\mathfrak{M}_A$ and $\mathfrak{M}_B$ respectively. Prove that if A and $B/\mathfrak{M}_A B$ are regular, then B is regular.*

```
import Mathlib

namespace Problem83

open IsLocalRing

/--
A commutative local noetherian ring $R$ is regular if $\dim m/m^2 = \dim R$.
-/
class IsRegularLocalRing (R : Type) [CommRing R] : Prop extends
    IsLocalRing R, IsNoetherianRing R where
  reg : Module.finrank (ResidueField R) (CotangentSpace R) = ringKrullDim R

/--
Let \( f \colon A \to B \) be a flat local homomorphism of Noetherian rings,
having maximal ideals \( \mathfrak{M}_A \) and \( \mathfrak{M}_B \) respectively.
Prove that if \( A \) and \( B/\mathfrak{M}_A B \) are regular, then \( B \) is regular.
-/
theorem IsRegularLocalRing.flat_local_of_regular {A B : Type} [CommRing A] [CommRing B]
    [IsRegularLocalRing A] [IsNoetherianRing B] [IsLocalRing B] {f : A →+* B} (hfl : IsLocalHom f)
    (hff : f.Flat) [IsRegularLocalRing (B ⧸ (maximalIdeal A).map f)] : IsRegularLocalRing B := by
  sorry

end Problem83
```

Exercise (84). *For a projective module M over a commutative ring R, there exists a free R-module N, such that $M \oplus N$ is free.*

```
import Mathlib
```

```
namespace Problem84

/--
For a projective module \(M\) over a commutative ring \(R\),
there exists a free \(R\)-module \(N\), such that \(M \oplus N\) is free.
-/
theorem exists_directSum_free_free_of_projective (R M : Type) [CommRing R] [AddCommGroup M]
    [Module R M] [Module.Projective R M] : ∃ (N : Type) (_ : AddCommGroup N) (_ : Module R N),
    Module.Free R N ∧ Module.Free R (N × M) := by
  sorry

end Problem84
```

Exercise (85). *There exists a transfinite Euclidean domain such that it cannot be given a Euclidean norm taking value in* $\mathbb{N}$.

```
import Mathlib

namespace Problem85

/--
Definition of a Euclidean norm taking value in \(\mathbb{N}\).
-/
class EuclideanNormNat (R : Type) [CommRing R] extends Nontrivial R where
  quotient : R → R → R
  quotient_zero : ∀ a, quotient a 0 = 0
  remainder : R → R → R
  quotient_mul_add_remainder_eq : ∀ a b, b * quotient a b + remainder a b = a
  norm : R → ℕ
  remainder_lt : ∀ (a) {b}, b ≠ 0 → norm (remainder a b) < norm b
  mul_left_not_lt : ∀ (a) {b}, b ≠ 0 → ¬ norm (a * b) < norm a

/--
There exists a transfinite Euclidean domain such that it cannot be given a Euclidean norm taking
value in \(\mathbb{N}\).
-/
theorem exist_euclideanDomain_not_norm_nat :
    ∃ (R : Type) (_ : EuclideanDomain R), IsEmpty (EuclideanNormNat R) := by
  sorry

end Problem85
```

Exercise (86). *For a commutative ring* A, $dimA[x, y] + dimA \leq 2 * dimA[x]$.

```
import Mathlib

namespace Problem86

/--
```

```
For a commutative ring \( A \), \( dim A[x, y] + dim A \le 2 * dim A[x]\).
-/
theorem dimension_convex (A : Type) [CommRing A] :
    ringKrullDim (MvPolynomial (Fin 2) A) + ringKrullDim A ≤ 2 * ringKrullDim (Polynomial A) := by
  sorry

end Problem86
```

Exercise (87). *There exists two commutative rings R, S, such that $R[x]$ is isomorphic to $S[x]$ but R is not isomorphic to S.*

```
import Mathlib

namespace Problem87

/--
There exists two commutative rings \(R, S\), such that \(R[x]\) is isomorphic to \(S[x]\) but \(R\)
is not isomorphic to \(S\).
-/
theorem exists_polynomial_ringEquiv_isEmpty_ringEquiv :
    ∃ (R S : Type) (_ : CommRing R) (_ : CommRing S),
    Nonempty ((Polynomial R) ≃+* (Polynomial S)) ∧ IsEmpty (R ≃+* S) := by
  sorry

end Problem87
```

Exercise (88). *$\mathbb{C}[x, y, z]/(x^2 + y^3 + z^7)$ is a UFD.*

```
import Mathlib

namespace Problem88

/--
The ring $R = \mathbb{C}[x, y, z] / (x^2 + y^3 + z^7)$.
-/
abbrev R : Type := (MvPolynomial (Fin 3) ℂ) / Ideal.span {(.X 0 ^ 2 + .X 1 ^ 3 + .X 2 ^ 7 :
     MvPolynomial (Fin 3) ℂ)}

/--
$\mathbb{C}[x, y, z] / (x^2 + y^3 + z^7)$ is a UFD.
-/
theorem quotient_not_UFD :
    ∃ (h : IsDomain R),
    (UniqueFactorizationMonoid R) := by
  sorry

end Problem88
```

Exercise (89). *Prove that if $\#G = 336$ then G is not simple.*

```
import Mathlib

namespace Problem89

/--
Prove that if $\#G = 336$ then $G$ is not simple.
-/
theorem not_isSimpleGroup_of_card_eq_336 (G : Type) [Group G]
    [Finite G] (h_card : Nat.card G = 336) : ¬ IsSimpleGroup G := by
  sorry

end Problem89
```

Exercise (90). *Given a field k, there exists some $n > 0$, there exists some subfield $K \subseteq k(x_1, \cdots, x_n)$, such that $K \cap k[X_1, \cdots, x_n]$ is not a finitely generated k-algebra.*

```
import Mathlib

namespace Problem90

/--
Given a field $k$, there exists some $n > 0$, there exists some subfield
$K \subseteq k(x_1, \cdots ,x_n) $, such that $K \cap k [X_1, \cdots, x_n]$ is not a finitely
generated $k$-algebra.
-/
theorem not_finiteType_inf_algebraMap_range (k : Type) [Field k] :
    ∃ (n : ℕ) (K : IntermediateField k (FractionRing (MvPolynomial (Fin n) k))),
    ¬ Algebra.FiniteType k (K.toSubalgebra ⊓ (Algebra.algHom k (MvPolynomial (Fin n) k)
    (FractionRing (MvPolynomial (Fin n) k))).range :
    Subalgebra k (FractionRing (MvPolynomial (Fin n) k))) := by
  sorry

end Problem90
```

Exercise (91). *Let k be a field, $A := k[x, y]/(xy(x + y - 1))$, then $\operatorname{Pic} A \cong k^\times$.*

```
import Mathlib

namespace Problem91

open CategoryTheory MvPolynomial

/--
The Picard group of a commutative ring R consists of the invertible R-modules,
  up to isomorphism.
-/
abbrev CommRing.Pic (R : Type) [CommRing R] : Type 1 := (Skeleton <| ModuleCat.{0} R)ˣ

/--
```

```
Let $ k $ be a field, $ A := k[x, y]/(xy(x + y - 1)) $, then $ \mathrm{Pic}\ A \cong k^{\times} $.
-/
theorem pic_three_lines {k : Type} [Field k] : Nonempty <|
    CommRing.Pic (MvPolynomial (Fin 2) k / Ideal.span ({(X 0) * (X 1) * (X 0 + X 1 - 1)} :
    Set (MvPolynomial (Fin 2) k))) ≃* kˣ := by
  sorry

end Problem91
```

Exercise (92). *Let A be a commutative ring with identity, $\dim A = 1$. Then all possible sequences for $a_n = dim A[x_1, \ldots, x_n] (n \in \mathbb{N})$ are exactly the sequences of the form: $a_n = 2n + 1$ if $n \le k$ else $a_n = n + k + 1$, for some $k \in \mathbb{N} \cup \{+\infty\}$.*

```
import Mathlib

namespace Problem92

/--
\(a_n = 2n+1\) if \(n \le k\) else \(a_n = n + k + 1\), for some \(k \in \mathbb{N} \{+\infty\}\).
-/
def a (k : ℕ∞) (n : ℕ) :=
  if h : n ≤ k then 2 * n + 1
  else n + WithTop.untop k (by rintro rfl; exact h le_top) + 1

/--
Let $A$ be a commutative ring with identity, $\dim A = 1$.
Then all possible sequences for \(a_n = dim A[x_1, \ldots, x_n] ( n \in \mathbb{N})\) are exactly
the sequences of the form: \(a_n = 2n+1\) if \(n \le k\) else \(a_n = n + k + 1\), for some
\(k \in \mathbb{N} \cup \{+\infty\}\).
-/
theorem dimension_sequences_of_one_dimensional_rings :
    (∀ (A : Type) [CommRing A] (h : ringKrullDim A = 1),
      ∃ (k : ℕ∞), (∀ (n : ℕ), ringKrullDim (MvPolynomial (Fin n) A) = a k n)) ∧
    (∀ (k : ℕ), ∃ (A : Type) (_ : CommRing A) (h : ringKrullDim A = 1),
      (∀ (n : ℕ), ringKrullDim (MvPolynomial (Fin n) A) = a k n)):= by
  sorry

end Problem92
```

Exercise (93). *There exists a field k and a (not necessarily commutative) ring A such that A is integral and finitely generated over k but $\dim_k A$ is not finite.*

```
import Mathlib

namespace Problem93

/--
There exists a field $k$ and a (not necessarily commutative) ring $A$
such that $A$ is integral and finitely generated over $k$ but $\dim_k A$ is not finite.
```

```
-/
theorem exists_integral_finiteType_not_finiteDimensional : ∃ (k A : Type) (_ : Field k)
    (_ : Ring A) (_ : Algebra k A),
    Algebra.IsIntegral k A ∧ Algebra.FiniteType k A ∧ ¬ FiniteDimensional k A := by
  sorry

end Problem93
```

Exercise (94). *Let k be field,* $\mathrm{char}\ k = 0$*, A be a finite-type k-algebra, $f : A \to A$ be an étale endomorphsim, $\varphi : A \to k$, $I \subset A$ be a ideal. If A is a domain, then*

$$\{n \in \mathbb{N} \mid \left.\varphi \circ f^n\right|_I = 0\}$$

is either finite or contains an arithmetic progression with a positive common difference.

```
import Mathlib

namespace Problem94

variable {k A : Type} [Field k] [CharZero k] [CommRing A] [IsDomain A] [Algebra k A]
  [Algebra.FiniteType k A] (f : A →ₐ[k] A) (φ : A →ₐ[k] k) (I : Ideal A)

/--
The set $\{ n \in \mathbb{N} \mid \left. \varphi \circ f^n \right|_I = 0 \right\rbrace \}$.
-/
def zeroSet : Set ℕ := {n | ∀ x : I, (φ.comp (f ^ n)) (x : A) = 0}

/--
Let $k$ be field, $\mathrm{char}\ k=0$, $ A $ be a finite-type $k$-algebra, $f: A \to A$ be an
\'etale endomorphsim, $\varphi: A \to k$, $I \subset A$ be a ideal. If $A$ is a domain,
then $$\left\lbrace  n \in \mathbb{N} \mid \left. \varphi \circ f^n \right|_I = 0 \right\rbrace $$
is either finite or contains an arithmetic progression with a positive common difference.
-/
theorem zeroSet_finite_or_contain_arithmetic_progression (hf : f.FormallyEtale) :
    (zeroSet f φ I).Finite ∨ ∃ (d : ℕ+) (a : ℕ), ∀ n : ℕ, a + d * n ∈ zeroSet f φ I := by
  sorry

end Problem94
```

Exercise (95). *Let $f : \mathbb{C}[x, y] \to \mathbb{C}[x, y]$, $x \mapsto p(x) + ay, y \mapsto x$, where $a \in \mathbb{C}$, $a \neq 0$, $p(x) \in \mathbb{C}[x]$ have degree > 1, $\mathfrak{p} \subset \mathbb{C}[x, y]$ be a prime ideal. If* height $\mathfrak{p} = 1$*, then $f(\mathfrak{p}) \neq \mathfrak{p}$.*

```
import Mathlib

namespace Problem95

open Polynomial Bivariate

/--
```

```
Let $f : \mathbb{C}[x, y] \to \mathbb{C}[x, y]$, $x \mapsto p(x) + ay, y \mapsto x$,
where $a \in \mathbb{C}$, $p(x) \in \mathbb{C}[x]$.
-/
noncomputable
def f (a : ℂ) (p : ℂ[X]): ℂ[X][Y] →+* ℂ[X][Y] :=
  eval₂RingHom (aeval (a • Y + C p)).toRingHom (C X)

/--
Let $f : \mathbb{C}[x, y] \to \mathbb{C}[x, y]$, $x \mapsto p(x) + ay, y \mapsto x$,
where $a \in \mathbb{C}$, $a \ne 0$, $p(x) \in \mathbb{C}[x]$ have degree $>1$, $\mathfrak{p}
\subset \mathbb{C}[x, y]$ be a prime ideal. If $\mathrm{height}\ \mathfrak{p} = 1 $, then
$f(\mathfrak{p}) \ne \mathfrak{p}$.
-/
theorem p_map_ne_p (p : ℂ[X]) (h : p.natDegree > 1) {a : ℂ} (ha : a ≠ 0)
    (𝔭 : Ideal ℂ[X][Y]) (h𝔭 : 𝔭.IsPrime) (h : 𝔭.height = 1) :
    𝔭.map (f a p) ≠ 𝔭 := by
  sorry

end Problem95
```

Exercise (96). *Let $f(x) \in \mathbb{Q}(x)$ be a rational function of degree at least 2, $\alpha \in \mathbb{Q}$. If the orbit $\mathscr{O}_f(\alpha)$ contains infinitely many integers, then $f^2(x)$ is a polynomial.*

```
import Mathlib

namespace Problem96

open RatFunc

/--
Let $f(x) \in \mathbb{Q}(x)$ be a rational function of degree at least 2, $\alpha \in \mathbb{Q}$.
If the orbit $\mathcal{O}_f(\alpha)$ contains infinitely many integers, then $f^2(x)$ is
a polynomial.
-/
theorem ratFunc_square_is_poly_of_orbit_contain_infinite_integer
    {f : RatFunc ℚ} (hf : f.num.natDegree ≥ 2 ∨ f.denom.natDegree ≥ 2) {a : ℚ}
    (h : ∀ n : ℕ, (f.eval (RingHom.id ℚ))^[n] a ≠ 0) -- exclude the case that the `denom` is zero
    (ha : {m : ℤ | ∃ n : ℕ, m = (f.eval (RingHom.id ℚ))^[n] a}.Infinite) :
    ∃ g : Polynomial ℚ, g = f.eval C f := by
  sorry

end Problem96
```

Exercise (97). *If k is a field of characteristic zero, $n \in \mathbb{N}$, $n \neq 0$, and $\phi\colon k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ is given by $(x_1, \ldots, x_n) \mapsto (f_1(x_1), \ldots, f_n(x_n))$, where $f_i(x_i) \in k[x_i]$ having degree at least two, then there is a point $a \in k^n$ such that for any non-zero polyminal $p \in k[x_1, \ldots, x_n]$, there exists $m \in \mathbb{N}$ such that $p(\phi^m(a)) \neq 0$.*

```
import Mathlib

namespace Problem97

open scoped Polynomial

/--
If $k$ is a field of characteristic zero, $n \in \mathbb{N}$, $n \ne 0$,
and $\phi \colon k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]$ is given by $(x_1, \dots, x_n) \mapsto
(f_1(x_1), \dots, f_n(x_n))$, where $f_i(x_i) \in k[x_i]$ having degree at least two, then there
is a point $a \in k^n$ such that for any non-zero polyminal $p \in k[x_1, \dots, x_n]$,
there exists $m \in \mathbb{N}$ such that $p(\phi^m(a)) \ne 0$.
-/
theorem exists_point_not_in_zero_set {τ k : Type} [Finite τ] [Nonempty τ] [Field k] [CharZero k]
    {f : τ → k[X]} (hfd : ∀ i : τ, (f i).natDegree ≥ 2): ∃ a : τ → k,
    ∀ p : MvPolynomial τ k, p ≠ 0 →
    ∃ m : ℕ, (((MvPolynomial.aeval (fun i ↦ (f i).toMvPolynomial i)) ^ m) p).aeval a ≠ 0 := by
  sorry

end Problem97
```

Exercise (98)**.** *If K be a number field, A be a finite-type K-algebra, $f : A \to A$ be an endomorphism. If A is a domain and f is not of finite order, then there exists a maximal ideal $m \subset A$ such that for all $n \in \mathbb{N}_+$, $f^{-n}(m) \neq m$.*

```
import Mathlib

namespace Problem98

/--
If $K$ be a number field, $A$ be a finite-type $K$-algebra, $f : A \to A$ be an endomorphism.
If $A$ is a domain and $f$ is not of finite order, then there exists a maximal ideal $m \subset A$
such that for all $n \in \mathbb{N}_+$, $f^{-n}(m) \ne m$.
-/
theorem exists_maximal_ideal_not_in_finite_order {K A : Type} [Field K] [NumberField K] [CommRing A]
    [IsDomain A] [Algebra K A] [Algebra.FiniteType K A] {f : A →ₐ[K] A} (hf : ∀ n > 0, f ^ n ≠ 1) :
    ∃ m : Ideal A, m.IsMaximal ∧ ∀ n > 0, m.comap (f ^ n) ≠ m := by
  sorry

end Problem98
```

Exercise (99)**.** *Let A be a finite-type $\mathbb{C}$-algebra, $n \in \mathbb{N}$, $n \geq 1$. If A is a domain, and $\mathrm{Aut}_{\mathbb{C}}\ A$ is isomorphic to $\mathrm{Aut}_{\mathbb{C}}\ \mathbb{C}[x_1, \dots, x_n]$, then A is isomorphic to $\mathbb{C}[x_1, \dots, x_n]$ as $\mathbb{C}$-algebras.*

```
import Mathlib

namespace Problem99
```

```
/--
Let $A$ be a finite-type $\mathbb{C}$-algebra, $n \in \mathbb{N}$, $n \ge 1$. If $A$ is a domain,
and $\mathrm{Aut}_\mathbb{C}\ A$ is isomorphic to $\mathrm{Aut}_\mathbb{C}\
\mathbb{C}[x_1, \dots, x_n]$, then $A$ is isomorphic to $\mathbb{C}[x_1, \dots, x_n]$ as
$\mathbb{C}$-algebras.
-/
theorem equiv_of_aut_equiv {A : Type} [CommRing A] [IsDomain A] [Algebra ℂ A]
    [Algebra.FiniteType ℂ A] {n : ℕ} (hn : n ≥ 1)
    (e : (A ≃ₐ[ℂ] A) ≃* (MvPolynomial (Fin n) ℂ ≃ₐ[ℂ] MvPolynomial (Fin n) ℂ)) :
    Nonempty (A ≃ₐ[ℂ] MvPolynomial (Fin n) ℂ) := by
  sorry

end Problem99
```

Exercise (100). *Let R be a Noetherian ring, P be a countably generated projective R-module such that $P_{\mathfrak{m}}$ has infinite rank for all maximal ideals $\mathfrak{m}$ of R. Then P is free.*

```
import Mathlib

namespace Problem100

open Module

/--
Let $R$ be a Noetherian ring, $P$ be a countably generated projective $R$-module
such that $P_{\mathfrak{m}}$ has infinite rank for all maximal ideals $\mathfrak{m}$ of $R$.
Then $P$ is free.
-/
theorem free_of_countably_generated_projective_of_local_infinite_rank {R : Type} [CommRing R]
    [IsNoetherianRing R] (P : Type) [AddCommGroup P] [Module R P] [Projective R P]
    (hcg : ∃ s : Set P, s.Countable ∧ Submodule.span R s = ⊤)
    (hm : ∀ m : Ideal R, (_ : m.IsMaximal) →
      ¬ Module.Finite (Localization.AtPrime m) (LocalizedModule.AtPrime m P)) : Free R P := by
  sorry

end Problem100
```