FATE-M Statements

Collective work at the 2024 PKU AI for Mathematics Summer School

July 2025

Exercise (1). *Inductively define $G^n = G \times G \times \cdots \times G$, the product of n same groups G. If G is a finite group, prove that this group has order $|G|^n$.*

```
import Mathlib

/--
Inductively define $G^n=G\times G\times\cdots \times G$, the product of $n$
    same groups $G$.
If $G$ is a finite group, prove that this group has order $|G|^n$.
-/
theorem prod_card_eq_card_pow {G : Type*} [Fintype G] [Group G] (n : ℕ) :
    Fintype.card (Π _ : Fin n, G) = (Fintype.card G) ^ n := by
  sorry
```

Exercise (2). *Let G be a cyclic group with generator a, and let G' be a group isomorphic to G. If $\phi : G \to G'$ is an isomorphism, show that, for every $x \in G, \phi(x)$ is completely determined by the value $\phi(a)$. That is, if $\phi : G \to G'$ and $\psi : G \to G'$ are two isomophisms such that $\phi(a) = \psi(a)$, then $\phi(x) = \psi(x)$ for all $x \in G$.*

```
import Mathlib

/--
Let $G$ be a cyclic group with generator $a$, and let $G^{\prime}$ be a group
    isomorphic to $G$.
If $\phi: G \rightarrow G^{\prime}$ is an isomorphism, show that, for every $x
    \in G, \phi(x)$ is
completely determined by the value $\phi(a)$. That is, if $\phi: G \rightarrow
    G^{\prime}$ and
```

```
$\psi: G \rightarrow G^{\prime}$ are two isomophisms such that $
    \phi(a)=\psi(a)$,
then $\phi(x)=\psi(x)$ for all $x \in G$.
-/
theorem monoidHom_eq_of_isCyclic {G G' : Type*} [Group G] [Group G'] (a : G)
    (h : ∀ g : G, ∃ n, g = a ^ n) (f1 f2 : G →* G') (heq : f1 a = f2 a) :
    ∀ g : G, f1 g = f2 g := by
  sorry
```

Exercise (3). *If $f : G \to H$ and $g : H \to K$ are surjective homomorphisms of groups, then the composition $g \circ f : G \to K$ is also a surjective homomorphism.*

```
import Mathlib

/--
If $f:G\to H$ and $g:H\to K$ are surjective homomorphisms of groups, then the
    composition
$g\circ f:G\to K$ is also a surjective homomorphism.
-/
theorem comp_surjective_of_surjective {G H K : Type*} [Group G] [Group H]
    [Group K]
    (f : G →* H) (g : H →* K) (hf : Function.Surjective f) (hg :
    Function.Surjective g) :
    Function.Surjective (g.comp f) := by
  sorry
```

Exercise (4). *Let $\phi : G \to G'$ be a group homomorphism. Show that $ab \in \operatorname{Ker}\phi$ if and only if $ba \in \operatorname{Ker}\phi$.*

```
import Mathlib

/--
Let $\phi: G \rightarrow G^{\prime}$ be a group homomorphism. Show that $ab\in
    \operatorname{Ker}\phi$ if and only if $ba\in \operatorname{Ker}\phi$.
-/
theorem mul_mem_ker_comm {G G' : Type*} [Group G] [Group G'] (f : G →* G') {a
    b : G} :
    (a * b ∈ f.ker) ↔ (b * a ∈ f.ker) := by
  sorry
```

Exercise (5). *Prove that a homomorphism $\phi : G \to G'$ is an isomorphism(There exists a two-sided inverse map $\phi^{-1} : G' \to G$) if and only if it is injective and surjective.*

```
import Mathlib

/--
Prove that a homomorphism $\phi: G \rightarrow G^{\prime}$ is an isomorphism
(There exists a two-sided inverse map $\phi^{-1}:G'\to G$)
if and only if it is injective and surjective.
-/
theorem has_inverse_iff_isomorphism {G G' : Type*} [Group G] [Group G'] (φ : G
    →* G') :
    (∃ φ₁ : G' → G, Function.LeftInverse φ₁ φ ∧ Function.RightInverse φ₁ φ) ↔
    (Function.Injective φ ∧ Function.Surjective φ) := by
  sorry
```

Exercise (6). *Prove that a if G and H are finite groups and their orders are coprime, then any homomorphism $f : G \to H$ is trivial, i.e. $f(G) = \{1_H\}$.*

```
import Mathlib

/--
Prove that a if $G$ and $H$ are finite groups and their orders are coprime,
then any homomorphism $f: G \rightarrow H$ is trivial, i.e. $f(G) = \{ 1_H \}$.
-/
theorem MonoidHom.eq_id_of_card_gcd_eq_one {G H: Type*} [Finite H] [Finite
    G][Group G] [Group H]
    (h : (Nat.card H).gcd (Nat.card G) = 1) (f : G →* H) : ∀ p : G , f p = 1 :=
     by
  sorry
```

Exercise (7). *Let $\phi : G \to G'$ be a group homomorphism. Show that $\phi(G)$ is Abelian if and only if $xyx^{-1}y^{-1} \in \mathrm{Ker}(\phi)$ for all $x, y \in G$.*

```
import Mathlib

/--
Let $\phi: G \rightarrow G^{\prime}$ be a group homomorphism. Show that $
    \phi(G)$ is Abelian
```

```
if and only if $x y x^{-1} y^{-1} \in \operatorname{Ker}(\phi)$ for all $x, y
    \in G$.
-/
theorem commutative_iff_commutator_mem_ker  {G H : Type} [Group G] [Group H]
    (f : G →* H) :
    (∀ x y : H, x ∈ f.range ∧ y ∈ f.range → x * y = y * x)
    ↔ ∀ x y : G, x * y * x⁻¹ * y⁻¹ ∈ f.ker := by
  sorry
```

Exercise (8). *Let G be a group, for $g \in G$, we set $f_g(x) := gxg^{-1}$ to be an isomorphism in* $\operatorname{Aut}(G)$*, prove that the kernel of the homomorphism map $\phi : G \to \operatorname{Aut}(G),\ g \mapsto f_g$ is the center of G, that is $\operatorname{Ker}\phi = Z(G)$.*

```
import Mathlib

/--
Let $G$ be a group, for $g\in G$, we set $f_g(x):=gxg^{-1}$ to be an
    isomorphism in
$\operatorname{Aut}(G)$, prove that the kernel of the homomorphism map
$\phi:G\to\operatorname{Aut}(G),\ g\mapsto f_g$ is the center of $G$, that is
$\operatorname{Ker}\phi=Z(G)$.
-/
theorem conj_ker_eq_center (G : Type*) [Group G] :
    MonoidHom.ker (@MulAut.conj G _) = Subgroup.center G := by
  sorry
```

Exercise (9). *Set $f : G \to H$ is a homomorphism between two groups. If $f(a)$ is not of finite order, then a is also not of finite order.*

```
import Mathlib

/--
Set $f:G\to H$ is a homomorphism between two groups.
If $f(a)$ is not of finite order, then $a$ is also not of finite order.
-/
theorem orderOf_eq_zero_of_monoidHom {G H : Type*} [Group G] [Group H] {f : G
    →* H} {a : G}
    (h : orderOf (f a) = 0) : orderOf a = 0 := by
  sorry
```

Exercise (10). *Set $f : G \to H$ is a homomorphism between two groups. If the range of f has n elements, then $x^n \in \operatorname{Ker} f$ for every $x \in G$.*

```
import Mathlib

/--
Set $f:G\to H$ is a homomorphism between two groups.
If the range of $f$ has $n$ elements, then $x^{n} \in \operatorname{Ker} f$
    for every $x \in G$.
-/
theorem pow_mem_ker_of_card_eq {G H : Type*} [Group G] [Group H] (f : G →* H)
    (n : ℕ)
    (h : Nat.card f.range = n) : ∀ g : G, (g ^ n) ∈ f.ker := by
  sorry
```

Exercise (11). *In any ring R and $a, b, c \in R$, $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$.*

```
import Mathlib

/--
In any ring $R$ and $a,b,c\in R$, $a(b-c)=a b-a c$ and $(b-c) a=b a-c a$.
-/
theorem mul_sub_and_sub_mul {R : Type*} [Ring R] (a b c : R) :
    a * (b - c) = a * b - a * c ∧ (b - c) * a = b * a - c * a := by
  sorry
```

Exercise (12). *Let R be a ring with unit. Then there is a unique homomorphism $f : \mathbb{Z} \to R$ such that $1 \mapsto 1_R$.*

```
import Mathlib

/--
Let $R$ be a ring with unit. Then there is a unique homomorphism
$f:\mathbb Z\to R$ such that $1\mapsto 1_R$.
-/
theorem existUnique_ringHom_int {R : Type*} [Ring R] : ∃! f : ℤ →+* R, True :=
    by
  sorry
```

Exercise (13). *Let R be a ring, and suppose that $a^3 = a, \forall a \in R$. Prove that R is commutative.*

```
import Mathlib

/--
Let $R$ be a ring, and suppose that $a^3=a, \forall a\in R$. Prove that $R$ is
    commutative.
-/
theorem commutative_of_relations {R : Type*} [Ring R] : (∀ a : R, a ^ 3 = a) →
    ∀ (a b : R), a * b = b * a := by
  sorry
```

Exercise (14). *In an integral domain R, if $a \in R$ and natural number $n \in \mathbb{N}$ satisfy $a^n = 0$, then $a = 0$.*

```
import Mathlib

/--
In an integral domain $R$, if $a\in R$ and natural number $n\in\mathbb N$
    satisfy $a^n=0$,
then $a=0$.
-/
theorem zero_of_pow_eq_zero {R : Type*} [Ring R] [IsDomain R] (a : R) (n : ℕ)
    (eq : a ^ n = 0) : a = 0 := by
  sorry
```

Exercise (15). *Let R be a ring with identity 1 and x be an element not equal to zero. If there exists $y \in R$ s.t. $xy = 1$ and $z \in R$ s.t. $zx = 1$, then $y = z$.*

```
import Mathlib

/--
Let $R$ be a ring with identity $1$ and $x$ be an element not equal to zero.
    If there exists
$y \in R$ s.t. $xy = 1$ and $z \in R$ s.t. $zx = 1$, then $y=z$.
-/
theorem left_right_inverse_eq {R : Type*} [Ring R] {x : R} (hx : x ≠ 0) :
    ∃ y, x * y = 1 → ∃ z, z * x = 1 → y = z := by
  sorry
```

Exercise (16). *Suppose R is an integral domain, show that for two element $r_1, r_2 \in R$, the principal ideals $r_1R = r_2R$ iff there exists $u \in R^\times$ s.t. $r_1 = ur_2$.*

```
import Mathlib

/--
Suppose $R$ is an integral domain, show that for two element $r_1,r_2\in R$,
    the principal ideals $r_1R=r_2R$ iff there exists $u\in R^\times$ s.t. $
    r_1=ur_2$.
-/
theorem Ideal.span_eq_iff_associated {R : Type*} [CommRing R] [IsDomain R] (r₁
    r₂ : R) :
     Ideal.span {r₁} = Ideal.span {r₂} ↔ ∃ u : R, IsUnit u ∧ r₁ = u * r₂ := by
  sorry
```

Exercise (17). *Suppose that R is a commutative ring with identity. For a subset S of R, let* $\operatorname{Span}(S)$ *be the minimal ideal containing elements in S. Prove that*

$\operatorname{Span}(S) = \left\{\sum_{s\in S'} r_s s | S' \text{ is a finite subset of } S, r_s \in R\ \forall s \in S'\right\}.$

In other words, prove that the latter one is an ideal and any ideal containing S also contains the right-hand-side.

```
import Mathlib

/--
Suppose that $R$ is a commutative ring with identity. For a subset $S$ of $R$,
let $\operatorname{Span}(S)$ be the minimal ideal containing elements in $S$.
    Prove that
$\operatorname{Span}(S)=\left\{\sum_{s\in S'}r_ss|S'\text{ is a finite subset
    of }S,r_s\in R\ \forall s\in S'\right\}.$
In other words, prove that the latter one is an ideal and any ideal containing
    $S$
also contains the right-hand-side.
-/
theorem ideal_span_eq_diagonal_map_sum {R : Type*} [CommRing R] (S : Set R) :
     (Ideal.span S) = {x : R | ∃ T : Multiset (R × S),
       x = Multiset.sum (Multiset.map (fun (x : R × S) ↦ (x.1 : R) * (x.2 :
    R)) T)} := by
  sorry
```

Exercise (18). *Let R be a commutative ring with identity and I_1 and I_2 be two ideals of R. Assume that I is an ideal containing I_1 and I_2, prove that I contains $I_1 + I_2$.*

```
import Mathlib

/--
Let $R$ be a commutative ring with identity and $I_1$ and $I_2$ be two ideals
    of $R$.
Assume that $I$ is an ideal containing $I_1$ and $I_2$, prove that $I$
    contains $I_1+I_2$.
-/
theorem Ideal.add_le_of_le {R : Type*} [CommRing R] (I : Ideal R) (J : Ideal
    R) (K : Ideal R)
    (h₁ : I ≤ K) (h₂ : J ≤ K) : I + J ≤ K := by
  sorry
```

Exercise (19). *For positive integer $n \geq 2$, show that the ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.*

```
import Mathlib

/--
For positive integer $n\ge 2$, show that the ring $\mathbb Z/n\mathbb Z$ is a
    field if and only if
$n$ is a prime number.
-/
theorem ZMod.isField_iff_prime (n : ℕ) : IsField (ZMod n) ↔ Nat.Prime n := by
  sorry
```

Exercise (20). *In a field F, as a ring, it has only ideals $(0) = \{0\}, (1) = F$.*

```
import Mathlib

/--
In a field $F$, as a ring, it has only ideals $(0)=\{0\},(1)=F$.
-/
theorem Field.ideal_eq_bot_or_top {F : Type*} [Field F] (I : Ideal F) : I = 0 ∨
    I = ⊤ := by
  sorry
```

Exercise (21)**.** *In a field F, for $a \in F^\times, b \in F$, the equation $ax + b = 0$ has a unique solution.*

```
import Mathlib

/--
In a field $F$, for $a\in F^\times, b\in F$, the equation $ax+b=0$ has a
    unique solution.
-/
theorem existUnique_linear_solution {F : Type*} [Field F] {a : Fˣ} {b : F} :
    ∃! x, a * x + b = 0 := by
  sorry
```

Exercise (22)**.** *Prove that an algebraically closed field must be an infinite field.*

```
import Mathlib

/--
Prove that an algebraically closed field must be an infinite field.
-/
theorem infinite_of_isAlgClosed {F : Type*} [Field F] [IsAlgClosed F] :
    Infinite F := by
  sorry
```

Exercise (23)**.** *Let R be a finite commutative ring with identity. Then every prime ideal I of R is maximal.*

```
import Mathlib

/-
Let $R$ be a finite commutative ring with identity. Then every prime ideal $I$
    of $R$ is maximal.
-/
theorem isMaximal_of_isPrime_of_fintype {R : Type*} [CommRing R] [Fintype R]
     (I : Ideal R) (hI : I.IsPrime) : I.IsMaximal := by
  sorry
```

Exercise (24)**.** *Let R be an integral domain. An element $p \in R$ is a prime element if and only if the principal ideal $\langle p \rangle$ is a nonzero prime ideal of R.*

```
import Mathlib

/--
Let $R$ be an integral domain. An element $p \in R$ is a prime element if and
    only if the principal
ideal $\langle p \rangle$ is a nonzero prime ideal of $R$.
-/
theorem isPrime_singleton {R : Type*} [CommRing R] [IsDomain R] {p : R} (hp :
    p ≠ 0) :
    Ideal.IsPrime (Ideal.span {p}) ↔ Prime p:= by
  sorry
```

Exercise (25). *Let R be a commutative ring with identity, and let $P_1, \ldots, P_m$ be prime ideals of R. If A is an ideal of R such that*

$$A \subseteq P_1 \cup \cdots \cup P_m,$$

then there exists some i $(1 \leq i \leq m)$ for which $A \subseteq P_i$.

```
import Mathlib

/--
Let $R$ be a commutative ring with identity, and let $P_1, \dots, P_m$ be
    prime ideals of $R$.
If $A$ is an ideal of $R$ such that
\[ A \subseteq P_1 \cup \cdots \cup P_m, \]
then there exists some $i$ ($1 \leq i \leq m$) for which $A \subseteq P_i$.
-/
theorem primeAvoidance {R : Type} [CommRing R] (A : Ideal R) (m : ℕ)
    (P : Fin (m + 1) → Ideal R)
    (pp : ∀ i : Fin (m + 1), (P i).IsPrime)
    (hA : A.carrier ⊆ ⋃ (i : Fin (m + 1)), P i) :
    ∃ i : Fin (m + 1), A.carrier ⊆ P i := by
  sorry
```

Exercise (26). *Let D be an integral domain, and let m, n be coprime positive integers. If $a, b \in D$ satisfy $a^m = b^m$ and $a^n = b^n$, then $a = b$.*

```
import Mathlib
```

```
/--
Suppose $D$ is integral domain, $m$ and $n$ are coprime positive integers.
Prove that for any $a, b \in D$, if $a^{m}=b^{m}$ and $a^{n}=b^{n}$, we have $
    a=b$
-/
theorem eq_of_pow_eq_of_coPrime {R : Type*} [Ring R] [IsDomain R] (a b : R) (m
    n : ℕ) (hm : m > 0)
     (hn : n > 0) (hmn : m.Coprime n) (h₁ : a ^ m = b ^ m) (h₂ : a ^ n = b ^ n)
    : a = b := by
  sorry
```

Exercise (27). *If D is an integral domain but not a field, then the polynomial ring $D[x]$ is not a principal ideal domain (PID).*

```
import Mathlib

open Polynomial

/--
If $D$ is an integral domain but not a field, then the polynomial ring $D[x]$
    is not a principal
ideal domain (PID).
-/
theorem Polynomial.not_isPrincipalIdealRing {D : Type*} [CommRing D] [IsDomain
    D] (not_field : ¬ IsField D) : ¬ (IsPrincipalIdealRing D[X]) := by
  sorry
```

Exercise (28). *Let E/F and K/F be normal extensions. Then the composite extension EK/F is also normal.*

```
import Mathlib

/-
Suppose $E / F$ and $K / F$ are normal extension. Prove that $E K / F$ is
    normal extension too.
-/
theorem IntermediateField.normal_of_normal_normal
```

```
    {F F₀ : Type*} [Field F] [Field F₀] [Algebra F F₀]
    (E K : IntermediateField F F₀) [Normal F E] [Normal F K]
    [Normal F E] [Normal F K] :
  Normal F (E ⊔ K : IntermediateField F F₀) := by
  sorry
```

Exercise (29)**.** *Let $A \leq G$ be a subgroup of G. Then $C_G(C_G(C_G(A))) = C_G(A)$.*

```
import Mathlib

/--
Let $A \leq G$ be a subgroup of $G$. Then $C_G(C_G(C_G(A))) = C_G(A)$.
-/
theorem Subgroup.centralizer_centralizer_centralizer {G : Type*} [Group G]
    (A A₁ A₂ A₃: Subgroup G) (h₁ : A₁= Subgroup.centralizer A)
    (h₂ : A₂ = Subgroup.centralizer A₁) (h₃ : A₃ = Subgroup.centralizer A₂) :
   A₁ = A₃ := by
  sorry
```

Exercise (30)**.** *The order of a permutation is equal to the least common multiple of the lengths of its disjoint cycles in the cycle decomposition.*

```
import Mathlib

open Classical

/--
The order of a permutation is equal to the least common multiple of the
    lengths of its disjoint cycles
in the cycle decomposition.
-/
theorem lcm_eq_orderOf {α : Type*} [Fintype α] [DecidableEq α] (σ : Equiv.Perm
    α) :
    σ.cycleType.lcm = orderOf σ := by
  sorry
```

Exercise (31)**.** *Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.*

```
import Mathlib

/--
Show that $G L_{n}(F)$ is non-abelian for any $n \geq 2$ and any $F$.
-/
theorem GL_not_commutative {F : Type*} [Field F] {n : ℕ} (h : n ≥ 2) :
    ∃ a b : (GL (Fin n) F) , a * b ≠ b * a := by
  sorry
```

Exercise (32). *Let G be a finite group which possesses an automorphism σ (cf. Exercise 20) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called fixed point free of order 2).*

```
import Mathlib

/--
Let $G$ be a finite group which possesses an automorphism $\sigma$ such that $
    \sigma(g)=g$
if and only if $g=1$. If $\sigma^{2}$ is the identity map from $G$ to $G$,
    prove that $G$ is
abelian (such an automorphism $\sigma$ is called fixed point free of order 2).
-/
theorem commutative_of_idempotent_mulEquiv {G : Type*} [Group G] [Finite G] (σ
    : MulEquiv G G)
    (h : ∀ g, σ g = g ↔ g = 1) (ids : σ ∘ σ = id) : ∀ a b : G, a * b = b * a :=
     by
  sorry
```

Exercise (33). *Prove that in a Boolean ring, every prime ideal is a maximal ideal.*

```
import Mathlib

/--
Prove that in a Boolean ring, every prime ideal is a maximal ideal.
-/
theorem BooleanRing.isMaximal_of_isPrime {R : Type*} [BooleanRing R] {I :
    Ideal R}
    (hi : I.IsPrime) : I.IsMaximal := by
```

```
  sorry
```

Exercise (34). *Prove that* $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

```
import Mathlib

/--
Prove that $C_{G}(A)=\left\{g \in G \mid g^{-1} a g=a\right.$ for all $\left.a
    \in A\right\}$.
-/
theorem Subgroup.centralizer_eq {G : Type*} {A : Set G} [Group G] :
    Subgroup.centralizer A = {g : G | ∀ a ∈ A, g⁻¹ * a * g = a} := by
  sorry
```

Exercise (35). *Prove that the set of complex numbers fixed conjugation is the set of real numbers*

```
import Mathlib

open ComplexConjugate

/--
Prove that the set of complex numbers fixed conjugation is the set of real
    numbers
-/
theorem conj_fixedPoint_eq : {z : ℂ | conj z = z} = {z : ℂ | ∃ (x : ℝ), z = x}
    := by
  sorry
```

Exercise (36). *Assume* R *is commutative. Prove that if* P *is a prime ideal of* R *and* P *contains no zero divisors then* R *is an integral domain.*

```
import Mathlib

/--
Assume $R$ is commutative. Prove that if $P$ is a prime ideal of $R$ and $P$
    contains no zero
divisors then $R$ is an integral domain.
-/
```

```
theorem isDomain_of_ideal_isPrime_noZeroDivisors {R : Type*} [CommRing R]
    {P : Ideal R} [Nontrivial P] (_ : P.IsPrime)
    (hz : ∀ a : P, ∀ b : R, a * b = 0 → a = 0 ∨ b = 0) : IsDomain R := by
  sorry
```

Exercise (37). *Prove that R is a P.I.D. if and only if R is a U.F.D. that is also a Bezout Domain.*

```
import Mathlib

/-
Prove that $R$ is a P.I.D. if and only if $R$ is a U.F.D. that is also a
    Bezout Domain.
-/
theorem isPrincipalIdealRing_iff_uniqueFactorizationMonoid_and_isBezout
    {R : Type*} [CommRing R] [IsDomain R] :
    IsPrincipalIdealRing R ↔ UniqueFactorizationMonoid R ∧ IsBezout R := by
  sorry
```

Exercise (38). *Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals some left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.*

```
import Mathlib

open Pointwise

/--
Let $H \leq G$ and let $g \in G$. Prove that if the right coset $H g$ equals
    some left coset of
$H$ in $G$ then it equals the left coset $g H$ and $g$ must be in $N_{G}(H)$.
-/
theorem coset_eq_and_mem_normalizer {G : Type*} [Group G] (H : Subgroup G) {g
    : G}
    (h : ∃ g' : G, MulOpposite.op g • H = g' • H.carrier) :
    MulOpposite.op g • H = g • H.carrier ∧ g ∈ Subgroup.normalizer H := by
  sorry
```

Exercise (39). *Let G be a group, and $a, b \in G$. For any positive integer n we define a^n by $a^n = \underbrace{aaa \cdots a}_{n \text{ factors}}$*

If there is an element $x \in G$ such that $a = x^2$, we say that a has a square root in G. Similarly, if $a = y^3$ for some $y \in G$, we say a has a cube root in G. In general, a has an nth root in G if $a = z^n$ for some $z \in G$. Prove $1\left(bab^{-1}\right)^n = ba^n b^{-1}$, *for every positive integer Prove by induction.*

```
import Mathlib

/--
Let $G$ be a group, and $a, b \in G$. For any positive integer $n$ we define $
    a^{n}$ by
$a^{n}=\underbrace{a a a \cdots a}_{n \text { factors }}$
In general, $a$ has an $n$th root in $G$ if $a=z^{n}$ for some $z \in G$. Prove
$1\left(b a b^{-1}\right)^{n}=b a^{n} b^{-1}$, for every positive integer.
-/
theorem conj_pow_eq_pow_conj {G : Type} [Group G] (a b : G) (n : ℕ) :
    (b * a * b⁻¹) ^ n = b * a ^ n * b⁻¹ := by
  sorry
```

Exercise (40)**.** *Show that every integer z is generated by 5 and 7.*

```
import Mathlib

/--
Show that every integer $z$ is generated by 5 and 7.
-/
theorem int_eq_five_seven_span : ∀ z : ℤ, ∃ a b : ℤ, z = a * 5 + b * 7 := by
  sorry
```

Exercise (41)**.** *Suppose $g = (a, b) \in G \times H$, where a has order m and b has order n. Prove that* $\operatorname{ord}(g) = \operatorname{LCM}(m, n)$.

```
import Mathlib

/--
Suppose $g=(a, b) \in G \times H$, where $a$ has order $m$ and $b$ has order $
    n$.
Prove that $\operatorname{ord}(g)=\operatorname{LCM}(m,n)$.
-/
theorem orderOf_prod {G H : Type*} [Group G] [Group H] {a : G} {b : H} :
```

```
    orderOf (a, b) = Nat.lcm (orderOf a) (orderOf b) := by
  sorry
```

Exercise (42)**.** *Suppose $(c, d) \in G \times H$, where c has order m and d has order n. Prove: If m and n are not relatively prime (hence have a common factor $q > 1$), then the order of (c, d) is less than mn.*

```
import Mathlib

/--
Suppose $(c, d) \in G \times H$, where $c$ has order $m$ and $d$ has order $n$.
Prove: If $m$ and $n$ are not relatively prime (hence have a common factor $
    q>1$ ),
then the order of $(c, d)$ is less than $m n$.
-/
theorem orderOf_prod_lt_orderOf_mul (G H : Type*) [Group G] [Group H] (c : G)
    (d : H)
    (h : (orderOf c).gcd (orderOf d) > 1) :
    orderOf (c, d) < (orderOf c) * (orderOf d) := by
  sorry
```

Exercise (43)**.** *In a ring with unity, prove that if a is nilpotent, then $a + 1$ and $a - 1$ are both invertible.*

```
import Mathlib

/--
In a ring with unity, prove that if $a$ is nilpotent, then $a+1$ and $a-1$ are
    both invertible.
-/
theorem invertible_of_nilpotent {R : Type*} [Ring  R] (a : R) (h : IsNilpotent
    a) :
    IsUnit (1 + a) ∧ IsUnit (1 - a) := by
  sorry
```

Exercise (44)**.** *Let A be an integral domain. Let $a \in A$. If A has characteristic* p*, and* $\mathrm{n} \cdot a = 0$ *where* n *is not a multiple of* p*, then $a = 0$.*

```
import Mathlib

/--
Let $A$ be an integral domain. Let $a \in A$. If $A$ has characteristic $
    \mathrm{p}$, and
$\mathrm{n} \cdot a=0$ where $\mathrm{n}$ is not a multiple of $\mathrm{p}$,
    then $a=0$.
-/
theorem zero_of_smul_eq_zero {A : Type*} [CommRing A] [IsDomain A] {p : ℕ} {a
    : A}
    [Fact p.Prime] [CharP A p] (hn : n • a = 0) (hnp : ¬ p ∣ n) : a = 0 := by
  sorry
```

Exercise (45)**.** *Let $A \subseteq B$ where A and B are integral domains. Prove: A has characteristic* p *iff B has characteristic* p*.*

```
import Mathlib

/--
Let $A \subseteq B$ where $A$ and $B$ are integral domains. Prove: $A$ has
    characteristic
$\mathrm{p}$ iff $B$ has characteristic $\mathrm{p}$.
-/
theorem ringChar_eq_prime_iff [CommRing B] [IsDomain B] (A : Subring B) :
    (ringChar B = p) ↔ (ringChar A = p) := by
  sorry
```

Exercise (46)**.** *Suppose $a(x)$ and $b(x)$ have degree $< n$. If $a(c) = b(c)$ for n values of c, prove that $a(x) = b(x)$.*

```
import Mathlib

open Polynomial

/--
Suppose $a(x)$ and $b(x)$ have degree $ < n$. If $a(c)=b(c)$ for $n$ values of
    $c$,
prove that $a(x)=b(x)$.
```

```
-/
theorem Polynomial.eq_of_roots_eq {R : Type*} [CommRing R] [IsDomain R] {n : ℕ
    } (a b : R[X])
    (ha : degree a < n) (hb : degree b < n) (hc : Multiset.card (roots (a -
    b)) = n) : a = b := by

  by_contra t
  --We prove this problem by using the reductio ad absurdum.
  have h : a - b ≠ 0 := by exact sub_ne_zero_of_ne t
  --First of all,   if $a \neq b$, then  $a-b \neq 0$.
  have h1 : Multiset.card (roots (a - b)) ≤ (a - b).degree := by exact
    card_roots h
  --By using a corollary of the fundamental theorem of algebra, we immediately
    know that the number of the roots of $a-b$ less than or equal to the
    degree of it.
  have h2 : (a + (-b)).degree ≤  max a.degree (-b).degree := by
  sorry
```

Exercise (47)**.** *Let U and V have the same dimension n. Prove that h is injective iff h is surjective.*

```
import Mathlib

/--
Let $U$ and $V$ have the same dimension $n$. Prove that $h$ is injective iff $
    h$ is surjective.
-/
theorem LinearMap.injective_iff_surjective_of_finiteDimentional
    {K : Type} [Field K] {U V : Type} [AddCommGroup U] [Module K U]
    [AddCommGroup V]
    [Module K V] [FiniteDimensional K U] [FiniteDimensional K V]
    (h : Module.finrank K U = Module.finrank K V) (f : U →ₗ[K] V) :
    Function.Injective f ↔ Function.Surjective f := by
  sorry
```

Exercise (48)**.** *Suppose that G is a group and $a, b \in G$ satisfy $a * b = b * a'$ where as usual, a' is the inverse for a. Prove that $b * a = a' * b$.*

```
import Mathlib
```

```
/--
Suppose that $G$ is a group and $a, b \in G$ satisfy $a * b=b * a^{\prime}$
    where as usual,
$a^{\prime}$ is the inverse for $a$. Prove that $b * a=a^{\prime} * b$.
-/
theorem relations_of_relations {G : Type*} [Group G] (a b : G) (h : a * b = b *
     a⁻¹) :
    b * a = a⁻¹ * b := by
  sorry
```

Exercise (49). *Suppose that* G *is a group and* a *and* b *are elements of* G *that satisfy* $a * b = b * a^3$. *Then the element* $(a * b)^2$ *can be written in the form* $b^k a^r$.

```
import Mathlib

/--
Suppose that $G$ is a group and $a$ and $b$ are elements of $G$ that satisfy $
    a * b=b * a^{3}$.
Then the element $(a * b)^{2}$ can be written in the form $b^{k} a^{r}$.
-/
theorem mul_pow_two_eq_of_relation {G : Type*} [Group G] (a b : G) (h : a * b =
     b * (a ^ 3)) :
    ∃ k r : ℕ, (a * b) ^ 2 = b ^ k * a ^ r := by
  sorry
```

Exercise (50). *Let* G *be a group with a finite number of elements. Show that for any* $a \in G$, *there exists an* $n \in \mathbb{Z}^{+}$*such that* $a^n = e$.

```
import Mathlib

/--
Let $G$ be a group with a finite number of elements. Show that for any $a \in
    G$,
there exists an $n \in \mathbb{Z}^{+}$such that $a^{n}=e$.
-/
theorem exist_pow_eq_one {G : Type*} [Group G] [Fintype G] :
    ∀ a : G, ∃ n : ℕ, n ≠ 0 ∧ a ^ n = 1 := by
  sorry
```

Exercise (51). *Show that if* $(a * b)^2 = a^2 * b^2$ *for* a *and* b *in a group* G*, then* $a * b = b * a$.

```
import Mathlib

/--
Show that if $(a * b)^{2}=a^{2} * b^{2}$ for $a$ and $b$ in a group $G$, then $
    a * b=b * a$.
-/
theorem mul_comm_of_relation {G : Type*} [Group G] (a b : G) (h : (a * b) ^ 2 =
     a ^ 2 * b ^ 2) :
    a * b = b * a := by
  sorry
```

Exercise (52). *Let* G *be a group and suppose that* $a * b * c = e$ *for* $a, b, c \in G$*. Show that* $b * c * a = e$ *also.*

```
import Mathlib

/--
Let $G$ be a group and suppose that $a * b * c=e$ for $a, b, c \in G$. Show
    that $b * c * a=e$ also.
-/
theorem mul_mul_eq_one {G : Type*} [Group G] (a b c : G) (h : a * b * c = 1) :
    b * c * a = 1 := by
  sorry
```

Exercise (53). *Prove that for any integer* $n \geq 3, S_n$ *has a subgroup isomorphic with* D_n.

```
import Mathlib

/--
Prove that for any integer $n \geq 3, S_{n}$ has a subgroup isomorphic with $
    D_{n}$.
-/
theorem DihedralGroup.mulEquiv_equiv_perm_subgroup(n : ℕ) (h : n ≥ 3) :
    ∃ (D : Subgroup (Equiv.Perm (Fin n))), Nonempty (DihedralGroup n ≃* D) :=
    by
  sorry
```

Exercise (54). *Prove that if G is a cyclic group and $|G| \geq 3$, then G has at least 2 generators.*

```
import Mathlib

/--
Prove that if $G$ is a cyclic group and $|G| \geq 3$, then $G$ has at least 2
    generators.
-/
theorem exist_two_generators {G : Type*} [Group G] [Fintype G] [hc : IsCyclic
    G]
     (h : Fintype.card G ≥ 3) :
    ∃ g₁ g₂ : G, g₁ ≠ g₂ ∧ Subgroup.zpowers g₁ = ⊤ ∧ Subgroup.zpowers g₂ = ⊤ :=
    by
  sorry
```

Exercise (55). *Show that a group with no proper nontrivial subgroups is cyclic.*

```
import Mathlib

/--
Show that a group with no proper nontrivial subgroups is cyclic.
-/
theorem isCyclic_of_subgroup_eq_bot_or_top {G : Type*} [Group G]
     (h : ∀ H : Subgroup G, H = ⊥ ∨ H = ⊤) : IsCyclic G := by
  sorry
```

Exercise (56). *Show that $\mathbb{Z}_p$ has no proper nontrivial subgroups if p is a prime number.*

```
import Mathlib

/--
Show that $\mathbb{Z}_{p}$ has no proper nontrivial subgroups if $p$ is a
    prime number.
-/
theorem ZMod.subgroup_eq_bot_or_top_of_prime {G : Type} [Group G] [Fintype G]
    (H : Subgroup G)
     (p : ℕ) [Fact p.Prime] (hGp : Fintype.card G = p) : H = ⊥ ∨ H = ⊤ := by
  sorry
```

Exercise (57)**.** *Consider S_n for a fixed $n \geq 2$ and let σ be a fixed odd permutation. Show that every odd permutation in S_n is a product of σ and some permutation in A_n.*

```
import Mathlib

/--
Consider $S_{n}$ for a fixed $n \geq 2$ and let $\sigma$ be a fixed odd
    permutation.
Show that every odd permutation in $S_{n}$ is a product of $\sigma$ and some
    permutation in $A_{n}$.
-/
theorem odd_eq_alternatingGroup_mul (n : ℕ) (σ : Equiv.Perm (Fin n))
    (odd : Equiv.Perm.sign σ = -1) : ∀ τ : Equiv.Perm (Fin n), Equiv.Perm.sign
    τ = -1 →
    ∃ (π : Equiv.Perm (Fin n)), π ∈ alternatingGroup (Fin n) ∧ τ = σ * π := by
  sorry
```

Exercise (58)**.** *Show that if σ is a cycle of odd length, then σ^2 is a cycle.*

```
import Mathlib

/--
Show that if $\sigma$ is a cycle of odd length, then $\sigma^{2}$ is a cycle.
-/
theorem Equiv.Perm.pow_two_isCycle_of_odd (n : ℕ) (f : Equiv.Perm (Fin n))
    (cyc : Equiv.Perm.IsCycle f) (oddcyc : Odd (orderOf f)) :
    Equiv.Perm.IsCycle (f ^ 2) := by
  sorry
```

Exercise (59)**.** *Prove that if a finite abelian group has order a power of a prime p, then the order of every element in the group is a power of p.*

```
import Mathlib

/--
Prove that if a finite abelian group has order a power of a prime $p$,
then the order of every element in the group is a power of $p$.
-/
```

```
theorem orderOf_eq_pow_of_card_pow {G : Type*} [CommGroup G] [Fintype G] (hp :
    p.Prime)
    (order : Fintype.card G = p ^ n) :
    ∀ (g : G), ∃ k ≤ n, orderOf g = p ^ k := by
  sorry
```

Exercise (60). *Let H be a subgroup of a group G such that $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. Show that every left coset gH is the same as the right coset* Hg.

```
import Mathlib

open scoped Pointwise

open MulOpposite

/--
Let $H$ be a subgroup of a group $G$ such that $g^{-1} h g \in H$ for all $g
    \in G$ and all
$h \in H$. Show that every left coset $g H$ is the same as the right coset $
    \mathrm{Hg}$.
-/
theorem leftCoset_eq_rightCoset_of_cong_mem {G : Type*} [Group G] (H :
    Subgroup G)
    (h : ∀ (h : H), ∀ (g : G), g * h * g⁻¹ ∈ H) :
    ∀ (g : G),  g • (H : Set G) = op g • (H : Set G) := by
  sorry
```

Exercise (61). *Show that an intersection of normal subgroups of a group G is again a normal subgroup of G.*

```
import Mathlib

/--
Show that an intersection of normal subgroups of a group $G$ is again a normal
    subgroup of $G$.
-/
theorem Subgroup.inf_normal_of_normal {G : Type*} [Group G]
    (M : Subgroup G) [hM : M.Normal] (N : Subgroup G) [hN: N.Normal] :
```

```
    (M ⊓ N).Normal := by
  sorry
```

Exercise (62). *Show that if H and K are normal subgroups of a group G such that $H \cap K = \{e\}$, then $hk = kh$ for all $h \in H$ and $k \in K$. [Hint: Consider the commutator $hkh^{-1}k^{-1} = \left(hkh^{-1}\right)k^{-1} = h\left(kh^{-1}k^{-1}\right)$.]*

```
import Mathlib

open Pointwise

/--
Show that if $H$ and $K$ are normal subgroups of a group $G$ such that $H \cap
    K=\{e\}$, then
$h k=k h$ for all $h \in H$ and $k \in K$.
-/
theorem mul_comm_of_normal_inf_eq_bot {G : Type*} [Group G] (N K : Subgroup G)
    [nN : N.Normal] [nK : K.Normal] (h1 : N ⊓ K = ⊥)
    {n k : G} (nin : n ∈ N) (kin : k ∈ K) : n * k = k * n := by
  sorry
```

Exercise (63). *Show that* $\operatorname{Aut}(\mathbb{Q})$ *is a group with only a single element.*

```
import Mathlib

/--
Show that $\operatorname{Aut}(\mathbb{Q})$ is a group with only a single
    element.
-/
theorem ringAut_rat_card_eq_one : Nat.card (RingAut ℚ) = 1 := by
  sorry
```

Exercise (64). *Suppose that G is a group and $g, h \in G$. Prove that $gx = h$ has a unique solution; likewise, prove that $xg = h$ has a unique solution.*

```
import Mathlib

/--
```

```
Suppose that $G$ is a group and $g, h \in G$. Prove that $g x=h$ has a unique
    solution;
likewise, prove that $x g=h$ has a unique solution.
-/
theorem existUnique_inverse {G : Type*} [Group G] (g h : G) :
    ∃! x, g * x = h ∧ ∃! x, x * g = h := by
  sorry
```

Exercise (65). *Prove that in a group, every element has exactly one inverse.*

```
import Mathlib

/--
Prove that in a group, every element has exactly one inverse.
-/
theorem existUnique_inverse {G : Type*} [Group G] {g : G} : ∃! (h : G), g * h =
     1 ∧ h * g = 1 := by
  sorry
```

Exercise (66). *Let G be a group, and $a, b, c \in G$. Prove that the equation $axc = b$ has a unique solution in G.*

```
import Mathlib

/--
Let $G$ be a group, and $a, b, c \in G$.
Prove that the equation $a x c=b$ has a unique solution in $G$.
-/
theorem existUnique_mul_eq {G : Type*} [Group G] (a b c : G) : ∃! x : G, a * x
    * b = c := by
  sorry
```

Exercise (67). *Suppose that G and H are groups with operations $\circ$ and $*$ and suppose $g, k \in G$ are inverses; that is, $g \circ k = e_G$. If $\varphi : G \to H$ is a group isomorphism, prove that $\varphi(g)$ and $\varphi(k)$ are inverses in H.*

```
import Mathlib
```

```
/--
Suppose that $G$ and $H$ are groups with operations $\circ$ and $*$ and suppose
$g, k \in G$ are inverses; that is, $g \circ k=e_{G}$. If $\varphi: G
    \rightarrow H$ is a group
isomorphism, prove that $\varphi(g)$ and $\varphi(k)$ are inverses in $H$.
-/
theorem MonoidHom.map_inv_eq_inv_map {G H : Type*} [Group G] [Group H] (φ : G
    →* H)
     (g k : G) (hgk : g = k⁻¹) : φ g = (φ k)⁻¹ := by
  sorry
```

Exercise (68)**.** *Explain why the order of* g^{-1} *is the same as* g*.*

```
import Mathlib

/--
Show that the order of $g^{-1}$ is the same as $g$.
-/
theorem orderOf_inv_eq_orderOf {G : Type*} [Group G] (a : G) : orderOf a =
    orderOf (a⁻¹) := by
  sorry
```

Exercise (69)**.** *A finite group cannot be isomorphic to a proper subgroup of itself.*

```
import Mathlib

/--
A finite group cannot be isomorphic to a proper subgroup of itself.
-/
theorem not_mulEquiv_subgroup_of_finite {G : Type} [Fintype G][Group G] (H :
    Subgroup G)
     (h1 : H < ⊤) : Nonempty (G ≃* H) → False:= by
  sorry
```

Exercise (70)**.** *Let* R *be a finite ring, and consider its additive group and its group of units. Show that these two groups cannot be isomorphic.*

```
import Mathlib

open Classical

/--
Let $R$ be a finite ring, and consider its additive group and its group of
    units.
Show that these two groups cannot be isomorphic.
-/
theorem not_mulEquiv_units {R : Type} [Fintype R] [Ring R] (h1 : Nontrivial R)
    :
    (Multiplicative R ≃* Rˣ) → False := by
  sorry
```

Exercise (71). *Prove that every subgroup of a cyclic group is cyclic.*

```
import Mathlib

/--
Prove that every subgroup of a cyclic group is cyclic.
-/
theorem subgroup_isCyclic_of_isCyclic {G : Type*} [Group G] {H : Subgroup G}
    (h : IsCyclic G) :
    IsCyclic H := by
  sorry
```

Exercise (72). *Prove that if G is a finite cyclic group with more than two elements, then G has more than one element whose order equals to $|G|$.*

```
import Mathlib

/--
Prove that if $G$ is a finite cyclic group with more than two elements,
then $G$ has more than one element whose order equals to $|G|$.
-/
theorem exists_elements_with_max_order {G : Type*} [Group G] [IsCyclic G]
    [Fintype G]
    (hG_card : Fintype.card G > 2) :
```

```
    ∃ a b : G, a ≠ b ∧ orderOf a = Fintype.card G ∧ orderOf b = Fintype.card G
    := by
  sorry
```

Exercise (73)**.** *If G is a finite group where every non-identity element is a generator of G, show that the order of G is prime or 1.*

```
import Mathlib

/--
If $G$ is a finite group where every non-identity element is a generator of $
    G$,
show that the order of $G$ is prime or $1$.
-/
theorem card_prime_or_one_of_generator {G : Type*} [Group G] [Fintype G]
     (h : ∀ x : G, x ≠ 1 → Subgroup.zpowers x = ⊤) :
     (Fintype.card G).Prime ∨ Fintype.card G = 1 := by
  sorry
```

Exercise (74)**.** *Show that if G is a group and H_1, H_2 are proper subgroups, then it is impossible that $G = H_1 \cup H_2$.*

```
import Mathlib

/--
Show that if $G$ is a group and $H_{1}, H_{2}$ are proper subgroups, then it
    is impossible that $G=H_{1} \cup H_{2}$.
-/
theorem Subgroup.union_neq_top {G : Type*} [Group G] (H₁ H₂ : Subgroup G) (p₁ :
    H₁ ≠ ⊤) (p₂ : H₂ ≠ ⊤) :
    ¬ (H₁.carrier ∪ H₂.carrier = ⊤) := by
  sorry
```

Exercise (75)**.** *Suppose that G is a group for which every element has order a power p^n of a fixed prime p. Let $\varphi : G \to H$ be a surjective homomorphism. Prove that H is a p-group too.*

```
import Mathlib

```

```
/--
Suppose that $G$ is a group for which every element has order a power $p^{n}$
    of a fixed prime $p$.
Let $\varphi: G \rightarrow H$ be a surjective homomorphism. Prove that $H$ is
    a $p$-group too.
-/
theorem IsPGroup_of_surjective {G H : Type*} {p : ℕ} [Group G] [Group H] [Fact
    p.Prime]
     (gp : IsPGroup p G) (f : G →* H) (sf : Function.Surjective f) : IsPGroup p
    H := by
  sorry
```

Exercise (76)**.** *If H is a subgroup of G and two cosets of H share an element, then these two cosets are equal.*

```
import Mathlib

open Pointwise

/--
If $H$ is a subgroup of $G$ and two cosets of $H$ share an element, then these
    two cosets are equal.
-/
theorem cosets_eq_of_inter_ne_empty {G : Type*} [Group G] (H : Subgroup G) (a
    b : G) :
     (a • (H : Set G)) ∩ (b • (H : Set G)) ≠ ∅ →
     QuotientGroup.mk (s := H) a = QuotientGroup.mk (s := H) b  := by
  sorry
```

Exercise (77)**.** *Suppose that G is an infinite group, and H is a subgroup of G with finitely many elements. Then there are infinitly many distinct cosets of H.*

```
import Mathlib

/--
Suppose that $G$ is an infinite group, and $H$ is a subgroup of $G$ with
    finitely many elements.
Then there are infinitly many distinct cosets of $H$.
```

```
-/
theorem quotient_infinite {G : Type*} [Group G] (H : Subgroup G)
    (hH : Finite H) (hG : Infinite G) : Infinite (G / H) := by
  sorry
```

Exercise (78). *Let G be a group of order p^2, where p is prime. Show that every proper subgroup of G is cyclic.*

```
import Mathlib

/--
Let $G$ be a group of order $p^{2}$, where $p$ is prime.
Show that every proper subgroup of $G$ is cyclic.
-/
theorem Subgroup.isCyclic_of_card_eq_primt_pow_two {G : Type*} [Group G]
    [Fintype G] (p : ℕ)
    (hp : Nat.Prime p) (h : Fintype.card G = p ^ 2) : ∀ H : Subgroup G, H < ⊤
    → IsCyclic H := by
  sorry
```

Exercise (79). *In the proof of Lemma 38.1 we needed to show that $x^3 - 2$ has only one real root; we did this using algebra. Prove this result using calculus.*

```
import Mathlib

/--
Show that $x^{3}-2$ has only one real root.
-/
theorem Real.existUnique_pow_three_eq_two : ∃! x : ℝ, x ^ 3 = 2 := by
  sorry
```

Exercise (80). *Show that an r-cycle is an even permutation if and only if r is odd.*

```
import Mathlib

/--
Show that an $r$-cycle is an even permutation if and only if $r$ is odd.
-/
```

```
theorem isCycle_sign_one_iff_odd {α : Type*} [Fintype α] [DecidableEq α] (r : ℕ
    ) {σ : Equiv.Perm α}
    (h1 : σ.IsCycle) (h2 : σ.support.card = r) : Equiv.Perm.sign σ = 1 ↔ Odd
    (r) := by
  sorry
```

Exercise (81). *Prove, for all i, that $\alpha \in S_n$ moves i if and only if α^{-1} moves i.*

```
import Mathlib

/--
Prove, for all $i$, that $\alpha \in S_{n}$ moves $i$ if and only if $
    \alpha^{-1}$ moves $i$.
-/
theorem Equiv.Perm.fix_iff_inv_fix {u : Type*} (α : Equiv.Perm u) (i : u) :
    α i ≠ i ↔ α⁻¹ i ≠ i := by
  sorry
```

Exercise (82). *Give an example of $\alpha, \beta, \gamma \in S_5$, none of which is the identity (1), with $\alpha\beta = \beta\alpha$ and $\alpha\gamma = \gamma\alpha$, but with $\beta\gamma \neq \gamma\beta$.*

```
import Mathlib

/--
Give an example of $\alpha, \beta, \gamma \in S_{5}$, none of which is the
    identity (1),
with $\alpha \beta=\beta \alpha$ and $\alpha \gamma=\gamma \alpha$,
but with $\beta \gamma \neq \gamma \beta$.
-/
theorem equiv_not_commutative : ∃ α β γ : Equiv.Perm (Fin 5), α ≠ 1 ∧ β ≠ 1 ∧
    γ ≠ 1 ∧
    α * β = β * α ∧ α * γ = γ * α ∧ β * γ ≠ γ * β := by
  sorry
```

Exercise (83). *Let G be a group and let $a \in G$ have order pk for some prime p, where $k \geq 1$. Prove that if there is $x \in G$ with $x^p = a$, then the order of x is p^2k, and hence x has larger order than a.*

```
import Mathlib

/--
Let $G$ be a group and let $a \in G$ have order $p k$ for some prime $p$,
    where $k \geq 1$.
Prove that if there is $x \in G$ with $x^{p}=a$, then the order of $x$ is $
    p^{2} k$, and hence
$x$ has larger order than $a$.
-/
theorem orderOf_eq_pow_two_mul {G : Type*} [Group G] (a : G) (x : G) (k : ℕ)
    [Fact p.Prime]
    (h₀ : k ≥ 1) (h :orderOf a = p * k) (hp: x ^ p = a) :
    orderOf x = (p ^ 2) * k := by
  sorry
```

Exercise (84). *Prove that every element in a dihedral group D_{2n} has a unique factorization of the form $a^i b^j$, where $0 \leq i < n$ and $j = 0$ or 1 .*

```
import Mathlib

/--
Prove that every element in a dihedral group $D_{2 n}$ has a unique
    factorization of the
form $a^{i} b^{j}$, where $0 \leq i < a$ and $j=0$ or 1.
-/
theorem DihedralGroup.eq_r_or_sr (g : DihedralGroup n) :
    ∃ (t : ZMod n) , g = (DihedralGroup.r t) ∨ g = (DihedralGroup.sr t) := by
  sorry
```

Exercise (85). *If H and K are subgroups of a group G and if $|H|$ and $|K|$ are relatively prime, prove that $H \cap K = \{1\}$.*

```
import Mathlib

open Classical

/--
```

```
If $H$ and $K$ are subgroups of a group $G$ and if $|H|$ and $|K|$ are
    relatively prime,
prove that $H \cap K=\{1\}$.
-/
theorem inf_eq_bot_of_card_coprime {G : Type*} [Group G] [Fintype G] (H :
    Subgroup G) (K : Subgroup G)
    (h : Nat.Coprime (Fintype.card H) (Fintype.card K)) : H ⊓ K = ⊥ := by
  sorry
```

Exercise (86). *Let G be a group of order 4. Prove that either G is cyclic or $x^2 = 1$ for every $x \in G$. Conclude that G must be abelian.*

```
import Mathlib

/--
Let $G$ be a group of order 4. Prove that $G$ must be abelian.
-/
theorem commutative_of_card_eq_four {G : Type*} [Group G] [Fintype G] (h :
    Fintype.card G = 4) :
    ∀ a b : G, a * b = b * a := by
  sorry
```

Exercise (87). *If $f : G \to H$ is a homomorphism and if $(|G|, |H|) = 1$, prove that $f(x) = 1$ for all $x \in G$*

```
import Mathlib

/--
If $f: G \rightarrow H$ is a homomorphism and if $(|G|,|H|)=1$, prove that $
    f(x)=1$ for all $x \in G$.
-/
theorem forall_coe_one_of_card_coprime {G H : Type*} [Group G] [Group H] (f :
    G →* H) [Fintype G] [Fintype H]
    (h : (Fintype.card G).Coprime (Fintype.card H)) : ∀ x : G, f x = 1 := by
  sorry
```

Exercise (88). *Let G be a finite group written multiplicatively. Prove that if $|G|$ is odd, then every $x \in G$ has a unique square root; that is, there exists exactly one $g \in G$ with $g^2 = x$.*

```
import Mathlib

/--
Let $G$ be a finite group written multiplicatively. Prove that if $|G|$ is
    odd, then every
$x \in G$ has a unique square root; that is, there exists exactly one $g \in
    G$ with $g^{2}=x$.
-/
theorem existUnique_square_root_of_odd_card {G : Type u} [Fintype G] [Group G]
    (hg : Odd (Fintype.card G)) : ∀ (x : G), ∃! (y : G), y ^ 2 = x := by
  sorry
```

Exercise (89)**.** *Prove that* $|\operatorname{Aut}(Z/pZ)| = p - 1$.

```
import Mathlib

/--
Prove that $|\operatorname{Aut}(Z/pZ)|=p-1$.
-/
theorem ZMod.addAut_card_eq_prime_sub_one {p : ℕ} [Fact p.Prime] :
    Nat.card (AddAut (ZMod p)) = p - 1 := by
  sorry
```

Exercise (90)**.** *If* G *is a group and* $G/Z(G)$ *is cyclic, where* $Z(G)$ *denotes the center of* G*, prove that* G *is abelian; that is,* $G = Z(G)$.

```
import Mathlib

/--
If $G$ is a group and $G / Z(G)$ is cyclic, where $Z(G)$ denotes the center of
    $G$,
prove that $G$ is abelian; that is, $G=Z(G)$.
-/
theorem comm_of_isCyclic_center_quotient {G : Type} [Group G]
    (h : IsCyclic (G / (Subgroup.center G))) : ∀ a b : G, a * b = b * a := by
  sorry
```

Exercise (91). *Let R be a ring, and suppose there exists a positive even integer n such that $x^n = x$ for all $x \in R$. Prove that $-x = x$ for all $x \in R$.*

```
import Mathlib

/--
Let $R$ be a ring, and suppose there exists a positive even integer $n$ such
    that $x^{n}=x$ for all
$x \in R$. Prove that $-x=x$ for all $x \in R$.
-/
theorem neg_eq_self_of_even_pow_eq_self {R : Type*} [Ring R] [Nontrivial R] {n
    : ℕ} [NeZero n]
    (h : ∀ x : R, x ^ (2 * n) = x) : ∀ x : R, x = -x := by
  sorry
```

Exercise (92). *Let R be a commutative ring, and let $p(x), f(x)$, and $g(x)$ be polynomials in $R[x]$. Prove that if $p(x)$ divides both $f(x)$ and $g(x)$ in $R[x]$, then for any polynomials $u(x)$ and $v(x)$ in $R[x]$, $p(x)$ divides $f(x)u(x) + g(x)v(x)$.*

```
import Mathlib

open Polynomial

/--
Let $R$ be a commutative ring, and let $p(x), f(x)$, and $g(x)$ be polynomials
    in $R[x]$.
Prove that if $p(x)$ divides both $f(x)$ and $g(x)$ in $R[x]$,
then for any polynomials $u(x)$ and $v(x)$ in $R[x]$, $p(x)$ divides $f(x)
    u(x)+g(x) v(x)$.
-/
theorem combination_dvd {R : Type*} [CommRing R] (p f g : R[X]) (pdvd : p ∣ f ∧
     p ∣ g) :
    ∀ u v : R[X], p ∣ f * u + g * v := by
  sorry
```

Exercise (93). *Let S be a set having an operation $*$ which assigns an element $a * b$ of S for any $a, b \in S$. Let us assume that the following two rules hold:*

1. *If a, b are any objects in S, then $a * b = a$.*

2. *If a, b are any objects in S, then $a * b = b * a$.*

Show that S can have at most one object.

```
import Mathlib

/--
Let $S$ be a set having an operation $*$ which assigns an element $a * b$ of $
    S$ for any
$a, b \in S$. Let us assume that the following two rules hold:

1. If $a, b$ are any objects in $S$, then $a * b=a$.

2. If $a, b$ are any objects in $S$, then $a * b=b * a$.

Show that $S$ can have at most one object.
-/
theorem cardinal_le_one_of_relations {S : Type*} [Mul S] (h₁ : ∀ (a b : S), a *
     b = a)
    (h₂ : ∀ (a b : S),a * b = b * a) : Subsingleton S := by
  sorry
```

Exercise (94)**.** *Show that $a \in Z(G)$ if and only if $C(a) = G$.*

```
import Mathlib

/--
Show that $a \in Z(G)$ if and only if $C(a)=G$.
-/
theorem mem_center_iff_centralizer_eq_top {G : Type*} [Group G] (a : G) :
    a ∈ Subgroup.center G ↔ Subgroup.centralizer {a} = ⊤ := by
  sorry
```

Exercise (95)**.** *If M is a subgroup of G such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that actually $x^{-1}Mx = M$.*

```
import Mathlib

open MulOpposite Pointwise
```

```
/--
If $M$ is a subgroup of $G$ such that $x^{-1} M x \subset M$ for all $x \in
    G$, prove that actually $x^{-1} M x=M$.
-/
theorem leftCoset_eq_self_of_subset {G : Type*} [Group G] (M:Subgroup G)
    (sub : ∀ (x : G), op x • (x⁻¹ • (M : Set G)) ⊆ (M : Set G)) :
    (∀ (x : G),(op x) • (x⁻¹ • (M : Set G)) = (M : Set G)):= by
  sorry
```

Exercise (96)**.** *If p is a prime, show that the only solutions of $x^2 \equiv 1 \bmod p$ are $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.*

```
import Mathlib

/--
If $p$ is a prime, show that the only solutions of $x^{2} \equiv 1 \bmod p$
    are $x \equiv$
$1 \bmod p$ or $x \equiv-1 \bmod p$.
-/
theorem pow_two_mod_prime_one {p : ℕ} [Fact p.Prime] (x : ℕ) :
    x ^ 2 ≡ 1 [MOD p] → x - 1 ≡ 0 [MOD p] ∨ x + 1 ≡ 0 [MOD p] := by
  sorry
```

Exercise (97)**.** *Let G be a group such that all subgroups of G are normal in G. If $a, b \in G$, prove that $ba = a^j b$ for some j.*

```
import Mathlib

/--
Let $G$ be a group such that all subgroups of $G$ are normal in $G$. If $a, b
    \in G$,
prove that $b a=a^{j} b$ for some $j$.
-/
theorem mul_eq_pow_mul_of_normal (G : Type*) [Group G] (h : ∀ N : Subgroup G,
    N.Normal) :
    ∀ a b : G, ∃ j : ℤ, b * a = a ^ j * b := by
  sorry
```

Exercise (98). *Prove that a group of order p^2, p a prime, has a normal subgroup of order p.*

```
import Mathlib

open Classical

/--
Prove that a group of order $p^{2}, p$ a prime, has a normal subgroup of order
    $p$.
-/
theorem exist_subgroup_normal_of_card_prime_pow_two {G : Type*} {p : ℕ} [Group
    G] [Fintype G]
     (pp : p.Prime) (ord : Fintype.card G = p ^ 2) :
    ∃ P : Subgroup G, (P.Normal) ∧ (Fintype.card P = p) := by
  sorry
```

Exercise (99). *If G is a group and $N \triangleleft G$ is such that G/N is abelian, prove that $aba^{-1}b^{-1} \in N$ for all $a, b \in G$*

```
import Mathlib

/--
If $G$ is a group and $N \triangleleft G$ is such that $G / N$ is abelian,
prove that $a b a^{-1} b^{-1} \in N$ for all $a, b \in G$
-/
theorem commutator_mem_of_quotient_commutative {G : Type*} [Group G] (N :
    Subgroup G) [N.Normal]
     (hc : ∀ a b : (G / N), a * b = b * a) : ∀ a b : G, a * b * a⁻¹ * b⁻¹ ∈ N :=
     by
  sorry
```

Exercise (100). *If G is a group and $H \triangleleft G$, show that if $a \in G$ has finite order $o(a)$, then Ha in G/H has finite order m, where $m \mid o(a)$.*

```
import Mathlib

/--
If $G$ is a group and $H \triangleleft G$, show that if $a \in G$ has finite
    order $o(a)$,
```

```
then $H a$ in $G / H$ has finite order $m$, where $m \mid o(a)$.
-/
theorem QuotientGroup.orderOf_dvd {G : Type*} [Group G] (H : Subgroup G)
    [H.Normal] (a : G)
    (h : 0 < orderOf a) : (orderOf <| QuotientGroup.mk (s := H) a) ∣ orderOf a
    := by
  sorry
```

Exercise (101). *Let A be a normal subgroup of a group G, and suppose that $b \in G$ is an element of prime order p, and that $b \notin A$. Show that $A \cap (b) = (e)$.*

```
import Mathlib

/--
Let $A$ be a normal subgroup of a group $G$, and suppose that $b \in G$ is an
    element of
prime order $p$, and that $b \notin A$. Show that $A \cap(b)=(e)$.
-/
theorem inf_zpowers_eq_bot_of_orderOr_prime {G : Type*} [Group G] (A :
    Subgroup G) [A.Normal]
    (b : G) (hb : (orderOf b).Prime) (h4 : b ∉ A) : A ⊓ (Subgroup.zpowers b) =
    ⊥ := by
  sorry
```

Exercise (102). *If $|G| = p^3$ and $|Z(G)| \geq p^2$, prove that G is abelian.*

```
import Mathlib

open Classical

/--
If $|G|=p^{3}$ and $|Z(G)| \geq p^{2}$, prove that $G$ is abelian.
-/
theorem commutative_of_center_card_eq_prime_pow_three {G : Type*} {p : ℕ}
    [Group G] [Fintype G]
    (pp : p.Prime) (p3 : Fintype.card G = p ^ 3) (p2 : Fintype.card
    (Subgroup.center G) ≥ p ^ 2) :
    ∀ a b : G, a * b = b * a := by
  sorry
```

Exercise (103). *If $P \triangleleft G$, P a p-Sylow subgroup of G, prove that $\varphi(P) = P$ for every automorphism φ of G.*

```
import Mathlib

/--
If $P \triangleleft G, P$ a $p$-Sylow subgroup of $G$,
prove that $\varphi(P)=P$ for every automorphism $\varphi$ of $G$.
-/
theorem sylow_fixedBy_mulEquiv {G : Type*} {p : ℕ} [Group G] [Fintype G] [Fact
    p.Prime] (P : Sylow p G) [pn : P.Normal]
     (φ : G ≃* G) : φ '' P = P := by
  sorry
```

Exercise (104). *If $N \triangleleft G$, let $B(N) = \{x \in G \mid xa = ax \text{ for all } a \in N\}$. Prove that $B(N) \triangleleft G$.*

```
import Mathlib

/--
If $N \triangleleft G$, let $B(N)=\{x \in G \mid x a=a x$ for all $a \in N\}$.
Prove that $B(N) \triangleleft G$.
-/
theorem centralizer_normal (G : Type) [Group G] (N : Subgroup G) [nh :
    N.Normal] :
     (Subgroup.centralizer (N : Set G)).Normal := by
  sorry
```

Exercise (105). *If P is a p-Sylow subgroup of G, show that $N(N(P)) = N(P)$.*

```
import Mathlib

/--
If $P$ is a $p$-Sylow subgroup of $G$, show that $N(N(P))=N(P)$.
-/
theorem Sylow.normalizer_normalizer_eq_normalizer {G : Type*} [Group G] {p : ℕ
    } [Fact (Nat.Prime p)]
     [Finite (Sylow p G)] (P : Sylow p G) : P.normalizer.normalizer =
    P.normalizer := by
  sorry
```

Exercise (106). *If* $|G| = p^n$, *show that* G *has a subgroup of order* p^m *for all* $1 \leq m \leq n$.

```
import Mathlib

open Classical

/--
If $|G|=p^{n}$, show that $G$ has a subgroup of order $p^{m}$ for all $1 \leq
    m \leq n$.
-/
theorem exists_subgroup_card_prime_pow_of_card_prime_pow {G : Type} [Group G]
    [Fintype G] (p n : ℕ)
    [Fact p.Prime] (hG : Fintype.card G = p ^ n) :
    ∀ (m : ℕ), 1 ≤ m ∧ m ≤ n → ∃ N : Subgroup G, Fintype.card N = p ^ m := by
  sorry
```

Exercise (107). *Prove that for any permutation* $\sigma, \sigma\tau\sigma^{-1}$ *is a transposition if* τ *is a transposition.*

```
import Mathlib

/--
Prove that for any permutation $\sigma, \sigma \tau \sigma^{-1}$ is a
    transposition if $\tau$ is a transposition.
-/
theorem cong_isSwap_of_Swap {α : Type*} [Fintype α] [DecidableEq α] (f :
    Equiv.Perm α) (g : Equiv.Perm α)
    (hg : Equiv.Perm.IsSwap g) : Equiv.Perm.IsSwap (f * g * f⁻¹) := by
  sorry
```

Exercise (108). *Prove that if* τ_1, τ_2, *and* τ_3 *are transpositions, then* $\tau_1\tau_2\tau_3 \neq e$, *the identity element of* S_n.

```
import Mathlib

open Equiv Equiv.Perm

/--
Prove that if $\tau_{1}, \tau_{2}$, and $\tau_{3}$ are transpositions, then
$\tau_{1} \tau_{2} \tau_{3} \neq e$, the identity element of $S_{n}$.
```

```
-/
theorem IsSwap.mul_mul_mul_ne_one (n : ℕ)
    (τ₁ : Perm (Fin n)) (τ₂ : Perm (Fin n)) (τ₃ : Perm (Fin n))
    (h₁ : IsSwap τ₁) (h₂ : IsSwap τ₂) (h₃ : IsSwap τ₃) : τ₁ * τ₂ * τ₃ ≠ 1 := by
  sorry
```

Exercise (109). *If R is an integral domain and $ab = ac$ for $a \neq 0, b, c \in R$, show that $b = c$.*

```
import Mathlib

/--
If $R$ is an integral domain and $a b=a c$ for $a \neq 0, b, c \in R$, show
    that $b=c$.
-/
theorem mul_left_cancel_of_NoZeroDivisors {R :Type*} [Ring R] [NoZeroDivisors
    R]
    (a b c : R) (h₁ : ¬ a = 0 ∧ a * b = a * c) : b = c := by
  sorry
```

Exercise (110). *If R is a ring and $e \in R$ is such that $e^2 = e$, show that $(xe - exe)^2 = 0$ for every $x \in R$.*

```
import Mathlib

/--
If $R$ is a ring and $e \in R$ is such that $e^{2}=e$, show that $(x e-e x
    e)^{2}=0$ for every $x \in R$.
-/
theorem pow_two_zero_of_relations {R : Type*} [Ring R] (e : R) (h : e * e = e)
    :
    ∀ x : R, (x * e - e * x * e) ^ 2 = 0 := by
  sorry
```

Exercise (111). *If $a^2 = 0$ in R, show that $ax + xa$ commutes with a.*

```
import Mathlib

/--
```

```
If $a^{2}=0$ in $R$, show that $a x+x a$ commutes with $a$.
-/
theorem commute_of_pow_two_zero (R : Type) [Ring R] (a : R) (h : a ^ 2 = 0) :
    ∀ x : R, Commute (a * x + x * a) a := by
  sorry
```

Exercise (112). *Let R be a ring with 1 . An element $a \in R$ is said to have a left inverse if $ba = 1$ for some $b \in R$. Show that if the left inverse b of a is unique, then $ab = 1$ (so b is also a right inverse of a).*

```
import Mathlib

/--
Let $R$ be a ring with 1 . An element $a \in R$ is said to have a left inverse
    if $b a=1$ for
some $b \in R$. Show that if the left inverse $b$ of $a$ is unique, then $a
    b=1$
(so $b$ is also a right inverse of $a$).
-/
theorem right_inverse_of_unique_left_inverse {R : Type*} [Ring R] {a b : R}
    (h₁ : b * a = 1)
    (h₂ : ∀ c : R, c * a = 1 → c = b) : a * b = 1 := by
  sorry
```

Exercise (113). *Show that for every positive integer n, $X^n - 2$ is an irreducible polynomial over the integers.*

```
import Mathlib

open Polynomial

/--
Show that for every positive integer $n$, $X^n -2$ is an irreducible
    polynomial over the integers.
-/
theorem irreducible_X_pow_n_minus_two (n : ℕ) (npos : 1 ≤ n) : Irreducible (X
    ^ n - 2 : ℤ[X]) := by
  sorry
```

Exercise (114)**.** *If H and K are subgroups of a group G, then $H \cup K$ cannot be a subgroup unless $H \subseteq K$ or $K \subseteq H$.*

```
import Mathlib

/--
If $H$ and $K$ are subgroups of a group $G$, then $H \cup K$ cannot be a
    subgroup
unless $H \subseteq K$ or $K \subseteq H$.
-/
theorem union_subgroup_iff_le {G : Type*} [Group G] {A B : Subgroup G} :
    (∃ C : Subgroup G , C = (A ∪ B : Set G)) ↔ A ≤ B ∨ B ≤ A := by
  sorry
```

Exercise (115)**.** *R is a relation on set A, $R^{-1} := \{(x, y) \mid (y, x) \in R\}$, prove that R is transitive if and only if R^{-1} is transitive.*

```
import Mathlib



/--
$R$ is a relation on set $A$, $R^{-1} := \{ (x,y) ~|~ (y,x) \in R\}$,
prove that $R$ is transitive if and only if $R^{-1}$ is transitive.
-/
theorem transitive_iff {A : Type} (R : A → A → Prop) :
  (Transitive R) ↔ (Transitive (fun x y => R y x)) := by
  sorry
```

Exercise (116)**.** *In any ring R and $a, b \in R$, if $ab = -ba$, then $(a + b)^2 = (a - b)^2 = a^2 + b^2$.*

```
import Mathlib

/--
In any ring $R$ and $a,b\in R$, if $a b=-b a$, then $
    (a+b)^{2}=(a-b)^{2}=a^{2}+b^{2}$.
-/
theorem pow_add_pow_eq {R : Type*} (a b : R) [Ring R]
    (h : a * b = - (b * a)) :
```

```
    (a + b) ^ 2 = a ^ 2 + b ^ 2 ∧ (a - b) ^ 2 = a ^ 2 + b ^ 2  := by
  sorry
```

Exercise (117)**.** *Let R be a commutative ring, and suppose $a^2 = b^3 = 0$ for some $a, b \in R$. Show that $(a+b)^4 = 0$.*

```
import Mathlib

/--
   Let $R$ be a commutative ring, and suppose $a^2=b^3=0$ for some $a, b \in
    R$. Show that $(a+b)^4 = 0$.
-/
theorem add_pow_four_eq_zero {R : Type*} [CommRing R] (a b : R)
    (h1 : a ^ 2 = 0) (h2 : b ^ 3 = 0) : (a + b) ^ 4 = 0 := by
  sorry
```

Exercise (118)**.** *Let R be a commutative ring. $a, b \in R$ are nilpotent. Prove that $a+b$ is also nilpotent.*

```
import Mathlib

/--
Let $R$ be a commutative ring. $a,b\in R$ are nilpotent. Prove that $a+b$ is
    also nilpotent.
-/
theorem isNilpotent_add_of_isNilpotent {R : Type*} [CommRing  R] (a b : R)
    {h₁ : IsNilpotent a} {h₂ : IsNilpotent b}: IsNilpotent (a + b) := by
  sorry
```

Exercise (119)**.** *Let R_1 be a commutative ring with identity* 1 *and R_2 be an integral domain. Let $f : R_1 \to R_2$ be a ring homomorphism, prove that* $\mathrm{Ker}(f)$ *is a prime ideal in R_1.*

```
import Mathlib

/--
Let $R_1$ be a commutative ring with identity $1$ and $R_2$ be an integral
    domain.
Let $f: R_1 \rightarrow R_2$ be a ring homomorphism, prove that $
    \operatorname{Ker}(f)$ is a
```

```
prime ideal in $R_1$.
-/
theorem ker_isPrime_of_isDomain {R R' F: Type*} [CommRing R] [CommRing R']
    [IsDomain R']
    (f : R →+* R') : Ideal.IsPrime (RingHom.ker f) := by
  sorry
```

Exercise (120)**.** *Let a, b be any two elements of a group G. If a, b commute with their commutator $[a, b]$, then for all integers m and n,*

$$[a^m, b^n] = [a, b]^{mn}.$$

```
import Mathlib

/--
Let $a, b$ be any two elements of a group $G$. If $a$, $b$ commute with their
    commutator $[a, b]$,
then for all integers $m$ and $n$,
\[
[a^m, b^n] = [a, b]^{mn}.
\]
-/
theorem pow_commutator_eq_commutator_pow_mul {G : Type*} [Group G] (a b : G)
    (ha : Commute a ⁅a, b⁆) (hb : Commute b ⁅a, b⁆) :
    ∀ m n : ℕ, ⁅a ^ m, b ^ n⁆ = ⁅a, b⁆ ^ (m * n) := by
  sorry
```

Exercise (121)**.** *Let α be an automorphism of a group G such that $g^{-1}\alpha(g) \in Z(G)$ for all $g \in G$. Then α acts trivially on the derived subgroup G', i.e., $\alpha(a) = a$ for all $a \in G'$.*

```
import Mathlib

/--
Suppose $G$ is a group and $\alpha$ is an automorphism of G. Prove that if for
    any $g \in G, g^{-1} \alpha(g) \in Z(G)$, then for any $a $ in $
    G^{\prime}$, we have $\alpha(a)=a$.
-/
theorem fixedBy_commutator_of_conj_mem_center {G : Type*} [Group G] (α : G ≃*
    G)
```

```
    (h : ∀ g, g⁻¹ * α g ∈ Subgroup.center G) : ∀ a ∈ commutator G, α a = a :=
    by
  sorry
```

Exercise (122). *Let A and B be two non-empty subsets of a finite group G. If $|A| + |B| > |G|$, then $G = AB$.*

```
import Mathlib

/--
Let $A$ and $B$ be two non-empty subsets of a finite group $G$. If $|A| + |B|
    > |G|$, then $G = AB$.
-/
theorem sum_eq_top_of_card_add_gt {G : Type*} [Group G] [Finite G] (A B : Set
    G) [ha : Nonempty A] [hb : Nonempty B]
    (h : A.ncard + B.ncard > (T : Set G).ncard) :
    (T : Set G) = {g | ∃ a ∈ A, ∃ b ∈ B, g = a * b} := by
  sorry
```

Exercise (123). *The additive group of rational numbers $\mathbb{Q}$ is not a cyclic group.*

```
import Mathlib

/--
Addictive group of $\mathbb{Q}$ is not cyclic.
-/
theorem Rat.not_isAddCyclic : ¬ (IsAddCyclic ℚ) := by
  sorry
```

Exercise (124). *Let $G = G_1 \times G_2$, and let $H \triangleleft G$ be a normal subgroup such that $H \cap G_i = \{1\}$ for $i = 1, 2$. Prove that $H \leq Z(G)$.*

```
import Mathlib

/--
Let $G = G_{1} \times G_{2}$, and let $H \triangleleft G$ be a normal subgroup
    such that
$H \cap G_{i} = \{1\}$ for $i = 1, 2$. Prove that $H \leq Z(G)$.
```

```
-/
theorem mem_center_of_inter_eq_bot {G₁ G₂ : Type*} [Group G₁] [Group G₂]
    (H : Subgroup (G₁ × G₂)) (H_Normal : H.Normal)
    (h₁ : H ⊓ (Subgroup.prod ⊤ ⊥) = ⊥) (h₂ : H ⊓ (Subgroup.prod ⊥ ⊤) = ⊥) :
    H ≤ Subgroup.center (G₁ × G₂) := by
  sorry
```

Exercise (125). *Let G act on a set S. For any $a, b \in S$, if there exists $g \in G$ such that $ga = b$, then $G_a = g^{-1}G_b g$. In other words, the stabilizers of elements in the same orbit are conjugate to each other.*

```
import Mathlib

/--
Let $G$ act on a set $S$. For any $a, b \in S$, if there exists $g \in G$ such
    that $g a = b$,
then $G_{a} = g^{-1} G_{b} g$. In other words, the stabilizers of elements in
    the same orbit are
conjugate to each other.
-/
theorem conj_stabilizer_eq {G : Type*} [Group G] (S : Type*) [MulAction G S]
    (a b : S) (g : G) (h : g • a = b) : (MulAction.stabilizer G a) =
    Subgroup.map (MulAut.conj (G := G) g⁻¹) (MulAction.stabilizer G b) := by
  sorry
```

Exercise (126). *Let N be a normal subgroup of G such that $N \cap [G, G] = \{1\}$. Then N is contained in the center of G, i.e., $N \leq Z(G)$.*

```
import Mathlib

/--
Suppose $N \triangleleft G, N \cap[G, G]=\{1\}$. Then $N \leqslant Z(G)$.
-/
theorem le_center_of_inf_commutator_eq_bot {G : Type*} [Group G] (N : Subgroup
    G) [hN : N.Normal]
    (h : N ⊓ (commutator G) = ⊥) : N ≤ Subgroup.center G := by
  sorry
```

Exercise (127)**.** *Let G be a monoid with identity. An element $b \in G$ is the inverse of $a \in G$ if and only if the following relations hold:*

$$aba = a \quad \text{and} \quad ab^2 a = 1.$$

```
import Mathlib

/--
Let $G$ be a monoid with identity. An element $b \in G$ is the inverse of $a
    \in G$ if and only if
the following relations hold:
\[ a b a = a \quad \text{and} \quad a b^2 a = 1. \]
-/
theorem inverse_iff_relations {G : Type*} [Monoid G] (a b : G) :
    (b * a = 1 ∧ a * b = 1) ↔ (a * b * a = a ∧ a * b ^ 2 * a = 1) := by
  sorry
```

Exercise (128)**.** *Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following: $Z\left(D_{2n}\right) = 1$ if n is odd.*

```
import Mathlib

/--
Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following: $Z\left(D_{2
    n}\right)=1$
if $n$ is odd.
-/
theorem DihedralGroup.center_eq_bot_of_odd (n : ℕ) [NeZero n] (ge : n ≥ 2) (h
    : Odd n) :
    (Subgroup.center (DihedralGroup n) = ⊥) := by
  sorry
```

Exercise (129)**.** *Prove that if H is a subgroup of G then $\langle H \rangle = H$.*

```
import Mathlib

/--
Prove that if $H$ is a subgroup of $G$ then $\langle H\rangle=H$.
-/
theorem Subgroup.closure_eq_self {G : Type*} [Group G] (H : Subgroup G) :
```

```
    Subgroup.closure H.carrier = H := by
  sorry
```

Exercise (130)**.** *Prove that* $Z(G) \leq N_G(A)$ *for any subset* A *of* G*.*

```
import Mathlib

/--
Let $G$ be a group, and $A$ is a subgroup of $G$. Show that $Z(G) \leq
    N_{G}(A)$.
-/
theorem subgroup_center_le_normalizer {G : Type*} [Group G] (A : Subgroup G) :
    (Subgroup.center G) ≤ (Subgroup.normalizer A) := by
  sorry
```

Exercise (131)**.** *Let* H *be a subgroup of order 2 in* G*. Show that* $N_G(H) = C_G(H)$*.*

```
import Mathlib

/--
Let $H$ be a subgroup of order 2 in $G$. Show that $N_{G}(H)=C_{G}(H)$.
-/
theorem normalizer_eq_centralizer_of_subgroup_orderOf_two
    {G : Type*} [Group G] (H : Subgroup G) (h : Nat.card H = 2) :
    (Subgroup.center G) = (Subgroup.normalizer H) := by
  sorry
```

Exercise (132)**.** *Show that a ring* R *has no nonzero nilpotent element if and only if 0 is the only solution of* $x^2 = 0$ *in* R*.*

```
import Mathlib

/--
Show that a ring $R$ has no nonzero nilpotent element if and only if 0 is the
    only solution
of $x^{2}=0$ in $R$.
-/
theorem has_no_nilpotent_iff_zero_of_pow_two_zero {R : Type*} [Ring R] :
```

```
    (∀ x : R, ∀ k : ℕ, x ≠ 0 → x ^ k ≠ 0) ↔ (∀ x : R, x ^ 2 = 0 → x = 0) := by
  sorry
```

Exercise (133)**.** *$\mathbb{Q}[x] / \left\langle x^{2}-5 x+6\right\rangle$ is not a field.*

```
import Mathlib

open Polynomial

/--
$\mathbb{Q}[x] /\left\langle x^{2}-5 x+6\right\rangle$ is not a field.
-/
theorem not_isField_quotient_ideal_span : ¬ IsField (ℚ[X] / Ideal.span {(X ^ 2
    - 5 * X + 6 : ℚ[X])}) := by
  sorry
```

Exercise (134)**.** *Show that if H is a normal subgroup of G and H is a p-group, then H is contained in every Sylow p-subgroup of G.*

```
import Mathlib

variable [Group G] [Finite G]

-- Every Sylow $p$ group of $G$ is finite.
instance : Finite (Sylow p G) := by
  sorry
```

Exercise (135)**.** *Prove that $1^{3}+2^{3}+\cdots+n^{3}=\frac{1}{4} n^{4}+\frac{1}{2} n^{3}+\frac{1}{4} n^{2}$.*

```
import Mathlib

open BigOperators

/--
Prove that $1^{3}+2^{3}+\cdots+n^{3}=\frac{1}{4} n^{4}+\frac{1}{2}
    n^{3}+\frac{1}{4} n^{2}$.
-/
theorem Finset.sum_cubic (n : ℕ) :
```

```
    ((∑ i ∈ Finset.range (n + 1), i ^ 3) : ℚ) =
    ((n : ℚ) ^ 4 / 4) + ((n : ℚ) ^ 3 / 2) + ((n : ℚ) ^ 2 / 4) := by
  sorry
```

Exercise (136). *If a and b are positive integers with $(a, b) = 1$, and if ab is a square, prove that both a and b are squares.*

```
import Mathlib

/--
If $a$ and $b$ are positive integers with $(a, b)=1$, and if $a b$ is a square,
prove that both $a$ and $b$ are squares.
-/
theorem isSquare_of_mul_isSquare_of_isCoprime {a b : ℤ} (hab : IsCoprime a b)
    (pos : a > 0 ∧ b > 0) (hn : IsSquare (a * b)) : IsSquare a ∧ IsSquare b :=
    by
  sorry
```

Exercise (137). *Let G be a group and regard $G \times G$ as the direct product of G with itself. If the multiplication $\mu : G \times G \to G$ is a group homomorphism, prove that G must be abelian.*

```
import Mathlib

/--
Let $G$ be a group and regard $G \times G$ as the direct product of $G$ with
    itself.
If the multiplication $\mu: G \times G \rightarrow G$ is a group homomorphism,
prove that $G$ must be abelian.
-/
theorem comm_of_diagonal_hom {G : Type*} [Group G] (f : G × G →* G)
    (h : ∀ x : (G × G), f x = x.1 * x.2) : ∀ a b : G, a * b = b * a := by
  sorry
```

Exercise (138). *Prove that a finite p-group G is simple if and only if $|G| = p$.*

```
import Mathlib

/--
```

```
Prove that a finite $p$-group $G$ is simple if and only if $|G|=p$.
-/
theorem IsPGroup.isSimpleGroup_iff_card_eq_prime {G : Type*} [Group G]
    [Fintype G] {p : ℕ}
    [Fact (Nat.Prime p)] (h : IsPGroup p G) : IsSimpleGroup G ↔ Fintype.card
    G = p := by
  sorry
```

Exercise (139). *Prove that if G is a group and has exactly one subgroup H of order n, then H is a normal subgroup of G.*

```
import Mathlib

/--
Prove that if $G$ is a group and has exactly one subgroup $H$ of order $n$,
then $H$ is a normal subgroup of $G$.s
-/
theorem normal_of_card_eq_unique {G : Type*} [Group G] {H : Subgroup G}
    (hH : ∀ K : Subgroup G, (Nat.card K = Nat.card H) → (K = H)) : H.Normal :=
    by
  sorry
```

Exercise (140). *In a group G, show that the intersection of a left coset of $H \leqq G$ and a left coset of $K \leqq G$ is either empty or a left coset of $H \cap K$.*

```
import Mathlib

open Pointwise

/--
In a group $G$, show that the intersection of a left coset of $H \leqq G$ and
    a left coset of
$K \leqq G$ is either empty or a left coset of $H \cap K$.
-/
theorem leftCoset_inter_eq_bot_or_eq_leftCoset {G : Type*} [Group G] (H K :
    Subgroup G) (a b : G) :
    (a • H.carrier) ∩ (b • K) = ⊥ ∨ ∃ c : G,  (a • H.carrier) ∩ (b • K) = c •
    (H ⊓ K) := by
  sorry
```

Exercise (141). *Prove that every subgroup of a solvable group is solvable.*

```
import Mathlib

/--
Prove that every subgroup of a solvable group is solvable.
-/
theorem Subgroup.solvable_of_solvable {G : Type*} [Group G] [IsSolvable G] (H
    : Subgroup G) :
    IsSolvable H := by
  sorry
```

Exercise (142). *Let $f : R \rightarrow S$ be a ring homomorphism,with R and S commutative. If P is a prime ideal of S, show that the preimage $f^{-1}(P)$ is a prime ideal of R.*

```
import Mathlib

/--
Let $f: R \rightarrow S$ be a ring homomorphism,with $R$ and $S$ commutative.
If $P$ is a prime ideal of $S$, show that the preimage $f^{-1}(P)$ is a prime
    ideal of $R$.
-/
theorem comap_isPrime_of_isPrime {R S : Type*} [CommRing R] [CommRing S] (f :
    R →+* S) (P : Ideal S)
    (HP : Ideal.IsPrime P) : Ideal.IsPrime (Ideal.comap f P) := by
  sorry
```

Exercise (143). *Let G be a group, and $a, b \in G$. For any positive integer n we define a has an nth root in G if $a = z^n$ for some $z \in G$. Prove the following: If $a^3 = e$, then a has a square root.*

```
import Mathlib

/--
Let $G$ be a group, and $a, b \in G$. For any positive integer $n$ we define $
    a$ has an
$n$th root in $G$ if $a=z^{n}$ for some $z \in G$.
Prove the following: If $a^{3}=e$, then $a$ has a square root.
-/
```

```
theorem isSquare_of_pow_three_eq_one {G : Type} [Group G] (a : G) (h : a ^ 3 =
    1) :
    ∃ x : G, x ^ 2 = a := by
  sorry
```

Exercise (144)**.** *Let G be a finite group, and let H and K be subgroups of G. Prove the following: Suppose H and K are not equal, and both have order the same prime number p. Then $H \cap K = \{e\}$.*

```
import Mathlib

open Classical

/--
Let $G$ be a finite group, and let $H$ and $K$ be subgroups of $G$. Prove the
    following:
Suppose $H$ and $K$ are not equal, and both have order the same prime number $
    p$.
Then $H \cap K=\{e\}$.
-/
theorem inf_eq_bot_of_card_prime {G : Type} [Group G] [Fintype G] (p : ℕ) (H K
    : Subgroup G) [Fact p.Prime]
    (hH : Fintype.card H = p) (hK : Fintype.card K = p) (h : H ≠ K) :
    H ⊓ K = (⊥ : Subgroup G) := by
  sorry
```

Exercise (145)**.** *Prove that the order of any p-group is a power of p.*

```
import Mathlib

/--
Prove that the order of any $p$-group is a power of $p$.
-/
theorem IsPGroup.card_eq_pow {p : ℕ} {G : Type*} [h₁ : Group G] [Fact
    (Nat.Prime p)]
    [h₂ : Fintype G] (h : IsPGroup p G) : ∃ n : ℕ, Fintype.card G = p ^ n := by
  sorry
```

Exercise (146)**.** *Let R be a commutative ring and $f(x) \in R[x]$ a polynomial. Then if $f(x)$ is a zero divisor in $R[x]$, there exists a non-zero $a \in R$ such that $af(x) = 0$.*

```
import Mathlib

open Polynomial

/--
Suppose $R$ is a commutative ring. Prove that if $f(x)\in R[x]$ is a zero
    divisor, then exist $a\in R^*$ such that $af(x)=0$.
-/
theorem exists_nonzero_scalar_mul_zero_of_zeroDivisor {R : Type*} [CommRing R]
    (f : R[X]) (_ : f ≠ 0)
    (h : ∃ g : R[X], g ≠ 0 ∧ g * f = 0) : ∃ a : R, a ≠ 0 ∧ C a * f = 0 := by
  sorry
```

Exercise (147). *Let G be a finite group of order p^2q, where p and q are primes with $p > q$. Then the Sylow p-subgroup of G is normal.*

```
import Mathlib

/--
Suppose $|G|=p^2q$ where $p>q$ are primes. Let $P$ be a Sylow $p$-subgroup of $
    G$, then $P\lhd G$.
-/
theorem Sylow.normal_of_card_eq_p_pow_two_q {G : Type} [Group G] [Fintype G]
    {p q : ℕ} (pp : Nat.Prime p) (pq : Nat.Prime q)
    (h₁ : Fintype.card G = p ^ 2 * q) (h₂ : q < p) (P : Sylow p G): P.Normal :=
    by
  sorry
```

Exercise (148). *Let R be a commutative ring and $a \in R$ a non-unit element. Then there exists a maximal ideal M of R containing a.*

```
import Mathlib

/--
Let $R$ be a commutative ring and $a \in R$ a non-unit element.
Then there exists a maximal ideal $M$ of $R$ containing $a$.
-/
```

```
theorem mem_max_ideal_of_not_isUnit {R : Type*} [CommRing R] (a : R) {h₁ :
    ¬IsUnit a} :
    ∃ (I : Ideal R), a ∈ I ∧ Ideal.IsMaximal I := by
  sorry
```

Exercise (149). *If H is a subgroup of G and if $x \in H$, prove that*

$$C_H(x) = H \cap C_G(x).$$

```
import Mathlib

/--
If $H$ is a subgroup of $G$ and if $x \in H$, prove that $$C_{H}(x)=H \cap
    C_{G}(x).$$
-/
theorem Subgroup.centralizer_eq_self_inf_centralizer
    {G : Type*} [Group G] (H : Subgroup G) (x : H) :
    Subgroup.map H.subtype (Subgroup.centralizer {x}) = H ⊓
    Subgroup.centralizer {x.1} := by
  sorry
```

Exercise (150). *Show that $m\mathbb{Z}$ is a subgroup of $n\mathbb{Z}$ if and only if n divides m. (See Example 7.7.)*

```
import Mathlib

/--
Show that $m \mathbb{Z}$ is a subgroup of $n \mathbb{Z}$ if and only if $n$
    divides $m$.
-/
theorem zmultiples_le_iff_dvd (m n : ℤ) :
    (AddSubgroup.zmultiples m : Set ℤ) ≤ AddSubgroup.zmultiples n ↔ n ∣ m :=
    by
  sorry
```