Problems in Group Theory

Determine the Number of Elements of Order 3 in a Non-Cyclic Group of Order 57

Problem 628

Let G be a group of order 57. Assume that G is not a cyclic group.
Then determine the number of elements in G of order 3.

Proof.

Observe the prime factorization $57 = 3 \cdot 19$.
Let n_{19} be the number of Sylow 19-subgroups of G.
By Sylow's theorem, we know that

$$n_{19} \equiv 1 \pmod{19} \text{ and } n_{19} \mid 3.$$

It follows that $n_{19} = 1$.

Now, observe that if $g \in G$, then the order of g is 1, 3, or 19. Note that since G is not a cyclic group, the order of g cannot be 57.
As there is exactly one Sylow 19-subgroup P, any element that is not in P must have order 3.

Therefore, the number of elements of order 3 is $57 - 19 = 38$.

Remark.

Note that there are 16 elements of order 19 and the identity element is the only element of order 1.

If There are 28 Elements of Order 5, How Many Subgroups of Order 5?

Problem 626

Let G be a group. Suppose that the number of elements in G of order 5 is 28.
Determine the number of distinct subgroups of G of order 5.

Solution.

Let g be an element in G of order 5.
Then the subgroup $\langle g \rangle$ generated by g is a cyclic group of order 5.
That is, $\langle g \rangle = \{e, g, g^2, g^3, g^4\}$, where e is the identity element in G.
Note that the order of each non-identity element in $\langle g \rangle$ is 5.

Also, if h is another element in G of order 5, then we have either $\langle g \rangle = \langle h \rangle$ or $\langle g \rangle \cap \langle h \rangle = \{e\}$.
This follows from the fact that the intersection $\langle g \rangle \cap \langle h \rangle$ is a subgroup of the order 5 group $\langle g \rangle$, and thus the order of $\langle g \rangle \cap \langle h \rangle$

is either 5 or 1.

On the other hand, if H is a subgroup of G of order 5, then every non-identity element in H has order 5.

These observations imply that each subgroup of order 5 contains exactly 4 elements of order 5 and each element of order 5 appears in exactly one of such subgroups.
As there are 28 elements of order 5, there are $28/4 = 7$ subgroups of order 5.

Union of Two Subgroups is Not a Group

Problem 625

Let G be a group and let H_1, H_2 be subgroups of G such that $H_1 \not\subset H_2$ and $H_2 \not\subset H_1$.
(a) Prove that the union $H_1 \cup H_2$ is never a subgroup in G.
(b) Prove that a group cannot be written as the union of two proper subgroups.

Proof.

Prove that the union $H_1 \cup H_2$ is never a subgroup in G.

Seeking a contradiction, let us assume that the union $H_1 \cup H_2$ is a subgroup of G.
Since $H_1 \not\subset H_2$, there exists an element $a \in H_1$ such that $a \notin H_2$.
Similarly, as $H_2 \not\subset H_1$, there exists an element $b \in H_2$ such that $b \notin H_1$.
As we are assuming $H_1 \cup H_2$ is a group, we have $ab \in H_1 \cup H_2$.
It follows that either $ab \in H_1$ or $ab \in H_2$.

If $ab \in H_1$, then we have

$$b = a^{-1}(ab) \in H_1$$

as both a^{-1} and ab are elements in the subgroup H_1.
This contradicts our choice of the element b.

Similarly, if $ab \in H_2$, we have

$$a = (ab)b^{-1} \in H_2,$$

which contradicts the choice of a.
In either case, we reached a contradiction.
Thus, we conclude that the union $H_1 \cup H_2$ is not a subgroup of G.

(b) Prove that a group cannot be written as the union of two proper subgroups.

This is a special case of part (a).
If a group G is a union of two proper subgroup H_1 and H_2, then we must have $H_1 \not\subset H_2$ and $H_2 \not\subset H_1$, otherwise $G = H_1$ or $G = H_2$ and this is impossible as H_1, H_2 are proper subgroups.
Then $G = H_1 \cup H_2$ is a subgroup of G, which is prohibited by part (a).

Thus, any group cannot be a union of proper subgroups.

Normal Subgroup Whose Order is Relatively Prime to Its Index

Problem 621

Let G be a finite group and let N be a normal subgroup of G.
Suppose that the order n of N is relatively prime to the index $|G:N|=m$.
(a) Prove that $N=\{a\in G \mid a^n=e\}$.
(b) Prove that $N=\{b^m \mid b\in G\}$.

Proof.

Note that as n and m are relatively prime integers, there exits $s,t\in\mathbb{Z}$ such that

$$sn+tm=1. \tag{*}$$

Also, note that as the order of the group G/N is $|G/N|=|G:N|=m$, we have

$$g^mN=(gN)^m=N$$

for any $g\in G$ by Lagrange' theorem, and thus

$$g^m\in N. \tag{**}$$

(a) Prove that $N=\{a\in G \mid a^n=e\}$.

Suppose $a\in\{a\in G \mid a^n=e\}$. Then we have $a^n=e$.
It follows that

$$a\overset{(*)}{=}a^{sn+tm}=a^{sn}a^{tm}=a^{tm}=(a^t)^m\in N$$

by (**).
This proves that $\{a\in G \mid a^n=e\}\subset N$.

On the other hand, if $a\in N$, then we have $a^n=e$ as n is the order of the group N.
Hence $N\subset\{a\in G \mid a^n=e\}$.
Putting together these inclusions yields that $N=\{a\in G \mid a^n=e\}$ as required.

(b) Prove that $N=\{b^m \mid b\in G\}$.

Let $b^m\in\{b^m \mid b\in G\}$. Then by (**), we know that $b^m\in N$.
Thus, we have $\{b^m \mid b\in G\}\subset N$.

On the other hand, let $a\in N$. Then we have $a^n=e$ as $n=|N|$.
Hence it follows that

$$a\overset{(*)}{=}a^{sn+tm}=a^{sn}a^{tm}=a^{tm}=b^m,$$

where we put $b:=a^t$.
This implies that $a\in\{b^m \mid b\in G\}$, and hence we have $N\subset\{b^m \mid b\in G\}$.
So we see that $N=\{b^m \mid b\in G\}$ by these two inclusions.

Every Cyclic Group is Abelian

Problem 619

Prove that every cyclic group is abelian.

Proof.

Let G be a cyclic group with a generator $g \in G$.

Namely, we have $G = \langle g \rangle$ (every element in G is some power of g.)

Let a and b be arbitrary elements in G.

Then there exists $n, m \in \mathbb{Z}$ such that $a = g^n$ and $b = g^m$.

It follows that

$$ab = g^n g^m = g^{n+m} = g^m g^n = ba.$$

Hence we obtain $ab = ba$ for arbitrary $a, b \in G$.

Thus G is an abelian group.

The Set of Square Elements in the Multiplicative Group $(\mathbb{Z}/p\mathbb{Z})^*$

Problem 616

Suppose that p is a prime number greater than 3.

Consider the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$ of order $p-1$.

(a) Prove that the set of squares $S = \{x^2 \mid x \in G\}$ is a subgroup of the multiplicative group G.

(b) Determine the index $[G : S]$.

(c) Assume that $-1 \notin S$. Then prove that for each $a \in G$ we have either $a \in S$ or $-a \in S$.

Proof.

(a) Prove that $S = \{x^2 \mid x \in G\}$ is a subgroup of G.

Consider the map $\phi : G \to G$ defined by $\phi(x) = x^2$ for $x \in G$.

Then ϕ is a group homomorphism. In fact, for any $x, y \in G$, we have

$$\phi(xy) = (xy)^2 = x^2 y^2 = \phi(x)\phi(y)$$

as G is an abelian group.

By definition of ϕ, the image is $\mathrm{im}(\phi) = S$.

Since the image of a group homomorphism is a group, we conclude that S is a subgroup of G.

(b) Determine the index $[G : S]$.

By the first isomorphism theorem, we have

$$G/\ker(\phi) \cong S.$$

If $x \in \ker(\phi)$, then $x^2 = 1$.

It follows that $(x-1)(x+1) = 0$ in $\mathbb{Z}/p\mathbb{Z}$.

Since $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, it follows that $x = \pm 1$ and $\ker(\phi) = \{\pm 1\}$.

Thus, $|S| = |G/\ker(\phi)| = (p-1)/2$ and hence the index is

$$[G : S] = |G|/|S| = 2.$$

(c) Assume that $-1 \notin S$. Then prove that for each $a \in G$ we have either $a \in S$ or $-a \in S$.

Since $-1 \notin S$ and $[G : S] = 2$, we have the decomposition

$$G = S \sqcup (-S).$$

Suppose that an element a in G is not in S.

Then, we have $a \in -S$.

Thus, there exists $b \in S$ such that $a = -b$.

It follows that $-a = b \in S$. Therefore, we have either $a \in S$ or $-a \in S$.

The Number of Elements Satisfying $g^5 = e$ in a Finite Group is Odd

Problem 614

Let G be a finite group. Let S be the set of elements g such that $g^5 = e$, where e is the identity element in the group G. Prove that the number of elements in S is odd.

Proof.

Let $g \neq e$ be an element in the group G such that $g^5 = e$.

As 5 is a prime number, this yields that the order of g is 5.

Consider the subgroup $\langle g \rangle$ generated by g.

As the order of g is 5, the order of the subgroup $\langle g \rangle$ is 5.

If $h \neq e$ is another element in G such that $h^5 = e$, then we have either $\langle g \rangle = \langle h \rangle$ or $\langle g \rangle \cap \langle h \rangle = \{e\}$ as the intersection of these two subgroups is a subgroup of $\langle g \rangle$.

It follows that S is the union of subgroups of order 5 that intersect only at the identity element e.

Thus the number of elements in S are $4n + 1$ for some nonnegative integer n.

Group Homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ When m Divides n

Problem 613

Let m and n be positive integers such that $m \mid n$.
(a) Prove that the map $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ sending $a + n\mathbb{Z}$ to $a + m\mathbb{Z}$ for any $a \in \mathbb{Z}$ is well-defined.
(b) Prove that ϕ is a group homomorphism.
(c) Prove that ϕ is surjective.
(d) Determine the group structure of the kernel of ϕ.

Proof.

(a) Prove that the map $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ sending $a + n\mathbb{Z}$ to $a + m\mathbb{Z}$ for any $a \in \mathbb{Z}$ is well-defined.

To show that ϕ is well-defined, we need show that the value of ϕ does not depends on the choice of representative a.

So suppose that $a + n\mathbb{Z} = a' + n\mathbb{Z}$ so that a and a' are two representatives for the same element.

This yields that $a - a'$ is divisible by n.

Now, $a + n\mathbb{Z}$ is mapped to $a + m\mathbb{Z}$ by ϕ. On the other hand, $a' + n\mathbb{Z}$ is mapped to $a + m\mathbb{Z}$ by ϕ.

Since $a - a'$ is divisible by n and $m \mid n$, it follows that $a - a'$ is divisible by m.

This implies that $a+m\mathbb{Z}=a'+m\mathbb{Z}$.

This prove that ϕ does not depend on the choice of the representative, and hence ϕ is well-defined.

(b) Prove that ϕ is a group homomorphism.

Let $a+n\mathbb{Z}$, $b+n\mathbb{Z}$ be two elements in $\mathbb{Z}/n\mathbb{Z}$. Then we have

$$\begin{aligned}
&\phi\left((a+n\mathbb{Z})+(b+n\mathbb{Z}) \right) \\
&=\phi\left((a+b)+n\mathbb{Z} \right) && \text{by addition in } \mathbb{Z}/n\mathbb{Z} \\
&=(a+b)+m\mathbb{Z} && \text{by definition of } \phi \\
&=(a+m\mathbb{Z})+(b+m\mathbb{Z}) && \text{by addition in } \mathbb{Z}/m\mathbb{Z} \\
&=\phi(a+n\mathbb{Z})+\phi(b+n\mathbb{Z}) && \text{by definition of } \phi.
\end{aligned}$$

Hence ϕ is a group homomorphism.

(c) Prove that ϕ is surjective.

For any $c+m\mathbb{Z}\in\mathbb{Z}/m\mathbb{Z}$, we pick $c+n\mathbb{Z}\in\mathbb{Z}/n\mathbb{Z}$.

Then as $\phi(c+n\mathbb{Z})=c+m\mathbb{Z}$, we see that ϕ is surjective.

(d) Determine the group structure of the kernel of ϕ.

If $a+n\mathbb{Z}\in\ker(\phi)$, then we have $0+m\mathbb{Z}=\phi(a+n\mathbb{Z})=a+m\mathbb{Z}$.

This implies that $m\mid a$.

On the other hand, if $m\mid a$, then $\phi(a+n\mathbb{Z})=a+m\mathbb{Z}=0+m\mathbb{Z}$ and $a+n\mathbb{Z}\in\ker(\phi)$.

It follows that

$$\ker(\phi)=\{mk+n\mathbb{Z}\mid k=0,1,\dots,l-1\},$$

where l is an integer such that $n=ml$.

Thus, $\ker(\phi)$ is a group of order l.

Since $\ker(\phi)$ is a subgroup of the cyclic group $\mathbb{Z}/n\mathbb{Z}$, we know that $\ker(\phi)$ is also cyclic.

Thus

$$\ker(\phi)\cong\mathbb{Z}/l\mathbb{Z}.$$

Another approach

Here is a more direct proof of this result.

Define a map $\psi:\mathbb{Z}\to\ker(\phi)$ by sending $k\in\mathbb{Z}$ to $mk+n\mathbb{Z}$.

It is straightforward to verify that ψ is a surjective group homomorphism and the kernel of ψ is $\ker(\psi)=l\mathbb{Z}$.

It follows from the first isomorphism theorem that

$$\mathbb{Z}/l\mathbb{Z}=\mathbb{Z}/\ker(\psi)\cong\mathrm{im}(\psi)=\ker(\phi).$$

Example of an Infinite Group Whose Elements Have Finite Orders

Problem 594

Is it possible that each element of an infinite group has a finite order?

If so, give an example. Otherwise, prove the non-existence of such a group.

Solution.

We give an example of a group of infinite order each of whose elements has a finite order.

Consider the group of rational numbers $\mathbb{Q}$ and its subgroup $\mathbb{Z}$.

The quotient group $\mathbb{Q}/\mathbb{Z}$ will serve as an example as we verify below.

Note that each element of $\mathbb{Q}/\mathbb{Z}$ is of the form

$$\frac{m}{n}+\mathbb{Z},$$

where m and n are integers.

This implies that the representatives of $\mathbb{Q}/\mathbb{Z}$ are rational numbers in the interval $[0,1)$.

There are infinitely many rational numbers in $[0,1)$, and hence the order of the group $\mathbb{Q}/\mathbb{Z}$ is infinite.

On the other hand, as each element of $\mathbb{Q}/\mathbb{Z}$ is of the form $\frac{m}{n}+\mathbb{Z}$ for $m,n\in\mathbb{Z}$, we have

$$n\cdot\left(\frac{m}{n}+\mathbb{Z}\right)=m+\mathbb{Z}=0+\mathbb{Z}$$

because $m\in\mathbb{Z}$.

Thus the order of the element $\frac{m}{n}+\mathbb{Z}$ is at most n.

Hence the order of each element of $\mathbb{Q}/\mathbb{Z}$ is finite.

Therefore, $\mathbb{Q}/\mathbb{Z}$ is an infinite group whose elements have finite orders.

If a Half of a Group are Elements of Order 2, then the Rest form an Abelian Normal Subgroup of Odd Order

Problem 575

Let G be a finite group of order $2n$.

Suppose that exactly a half of G consists of elements of order 2 and the rest forms a subgroup.

Namely, suppose that $G=S\sqcup H$, where S is the set of all elements of order in G, and H is a subgroup of G. The cardinalities of S and H are both n.

Then prove that H is an abelian normal subgroup of odd order.

Proof.

The index of the subgroup H in G is 2, hence H is a normal subgroup.

(See the post "Any Subgroup of Index 2 in a Finite Group is Normal".)

Also, the order of H must be odd, otherwise H contains an element of order 2.

So it remains to prove that H is abelian.

Let $a\in S$ be an element of order 2.

As $a\notin H$, the left coset aH is different from H.

Since the index of H is 2, we have $aH=G\setminus H=S$.

So for any $h\in H$, the order of ah is 2.

It follows that we have for any $h\in H$

$$e=(ah)^2=ahah,$$

where e is the identity element in G.

Equivalently, we have

$$aha^{-1} = h^{-1} \tag{*}$$

for any $h \in H$.

(Remark that $a = a^{-1}$ as the order of a is 2.)

Using this relation, for any $h, k \in H$, we have

$$\begin{aligned}(hk)^{-1} &\overset{(*)}{=} a(hk)a^{-1} \\ &= (aha^{-1})(aka^{-1}) \\ &\overset{(*)}{=} h^{-1}k^{-1} = (kh)^{-1}.\end{aligned}$$

As a result, we obtain $hk = kh$ for any h, k.

Hence the subgroup H is abelian.

Every Group of Order 24 Has a Normal Subgroup of Order 4 or 8

Problem 568

Prove that every group of order 24 has a normal subgroup of order 4 or 8.

Proof.

Let G be a group of order 24.

Note that $24 = 2^3 \cdot 3$.

Let P be a Sylow 2-subgroup of G. Then $|P| = 8$.

Consider the action of the group G on the left cosets G/P by left multiplication.

This induces a permutation representation homomorphism

$$\phi : G \to S_{G/P},$$

where $S_{G/P}$ is a group of bijective maps (permutations) on G/P.

This homomorphism is defined by

$$\phi(g)(aP) = gaP$$

for $g \in G$ and $aP \in G/P$.

Then by the first isomorphism theorem, we see that

$$G/\ker(\phi) \cong \mathrm{im}(\phi) < S_{G/P}.$$

This implies that the order of $G/\ker(\phi)$ divides the order of $S_{G/P}$. Note that as $|G/P| = 3$, we have $|S_{G/P}| = |S_3| = 6$. Thus, we must have $4 \mid |\ker\phi|$.

Also note that $\ker(\phi) < P$. To see this let $x \in \ker(\phi)$. Then we have

$$xP = \phi(x)(P) = \mathrm{id}(P) = P.$$

Here id is the identity map from G/P to itself. Hence $x \in P$. It follows that $|\ker(\phi)|$ divides $|P| = 8$.

Combining these restrictions, we see that $|\ker(\phi)| = 4, 8$.

Being the kernel of a homomorphism, $\ker(\phi)$ is a normal subgroup of G.

Hence the group G of order 24 has a normal subgroup of order 4 or 8.

Every Group of Order 12 Has a Normal Subgroup of Order 3 or 4

Problem 566

Let G be a group of order 12. Prove that G has a normal subgroup of order 3 or 4.

Hint.

Use Sylow's theorem.

(See Sylow's Theorem (Summary) for a review of Sylow's theorem.)

Recall that if there is a unique Sylow p-subgroup in a group GH , then it is a normal subgroup in G.

Proof.

Since $12 = 2^2 \cdot 3$, a Sylow 2-subgroup of G has order 4 and a Sylow 3-subgroup of G has order 3.

Let n_p be the number of Sylow p-subgroups in G, where $p = 2, 3$.

Recall that if $n_p = 1$, then the unique Sylow p-subgroup is normal in G.

By Sylow's theorem, we know that $n_2 \mid 3$, hence $n_p = 1, 3$.

Also by Sylow's theorem, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 4$.

It follows that $n_3 = 1, 4$.

If $n_3 = 1$, then the unique Sylow 3-subgroup is a normal subgroup of order 3.

Suppose that $n_3 = 4$. Then there are four Sylow 3-subgroup in G.

The order of each Sylow 3-subgroup is 3, and the intersection of two distinct Sylow 3-subgroups intersect trivially (the intersection consists of the identity element) since every nonidentity element has order 3.

Hence two elements of order 3 in each Sylow 3-subgroup are not included in other Sylow 3-subgroup.

Thus, there are totally $4 \cdot 2 = 8$ elements of order 3 in G.

Since $|G| = 12$, there are $12 - 8 = 4$ elements of order not equal to 3.

Since any Sylow 2-subgroup contains four elements, these elements fill up the remaining elements.

So there is just one Sylow 2-subgroup, and hence it is a normal subgroup of order 4.

In either case, the group G has a normal subgroup of order 3 or 4.

If the Quotient is an Infinite Cyclic Group, then Exists a Normal Subgroup of Index n

Problem 557

Let N be a normal subgroup of a group G.
Suppose that G/N is an infinite cyclic group.
Then prove that for each positive integer n, there exists a normal subgroup H of G of index n.

Hint.

Use the **fourth (or Lattice) isomorphism theorem**.

Proof.

Let n be a positive integer.

Since G/N is a cyclic group, let g be a generator of G/N.

So we have $G/N = \langle g \rangle$.

Then $\langle g^n \rangle$ is a subgroup of G/N of index n.

By the fourth isomorphism theorem, every subgroup of G/N is of the form H/N for some subgroup H of G containing N.

Thus we have $\langle g^n \rangle = H/N$ for some subgroup H in G containing N.

Since G/N is cyclic, it is in particular abelian.

Thus H/N is a normal subgroup of G/N.

The fourth isomorphism theorem also implies that H is a normal subgroup of G, and we have

$$[G : H] = [G/N : H/N] = n.$$

Hence H is a normal subgroup of G of index n.

If Generators x, y Satisfy the Relation $xy^2 = y^3x$, $yx^2 = x^3y$, then the Group is Trivial

Problem 554

Let x, y be generators of a group G with relation

$$xy^2 = y^3x, \tag{1}$$
$$yx^2 = x^3y. \tag{2}$$

Prove that G is the trivial group.

Proof.

From the relation (1), we have

$$xy^2x^{-1} = y^3.$$

Computing the power of n of this equality yields that

$$xy^{2n}x^{-1} = y^{3n} \tag{3}$$

for any $n \in \mathbb{N}$.

In particular, we have

$$xy^4x^{-1} = y^6 \text{ and } xy^6x^{-1} = y^9.$$

Substituting the former into the latter, we obtain

$$x^2y^4x^{-2} = y^9. \tag{4}$$

Cubing both sides gives

$$x^2y^{12}x^{-2} = y^{27}.$$

Using the relation (3) with $n = 4$, we have $xy^8x^{-1} = y^{12}$.
Substituting this into equality (4) yields $x^3y^8x^{-1} = y^{27}$.

Now we have

$$y^{27} = x^3y^8x^{-1} = (x^3y)y^8(y^{-1}x^{-3}) = yx^2y^8x^{-2}y.$$

Squaring the relation (4), we have $x^2y^8x^{-2} = y^{18}$.
Substituting this into the previous, we obtain $y^{27} = y^{18}$, and hence

$$y^9 = e,$$

where e is the identity element of G.

Note that as we have $xy^2x^{-1} = y^3$, the elements y^2, y^3 are conjugate to each other.
Thus, the orders must be the same. This observation together with $y^9 = e$ imply $y = e$.
It follows from the relation (2) that $x = e$ as well.
Therefore, the group G is the trivial group.

The Product of Distinct Sylow p-Subgroups Can Never be a Subgroup

Problem 544

Let G a finite group and let H and K be two distinct Sylow p-group, where p is a prime number dividing the order $|G|$ of G.
Prove that the product HK can never be a subgroup of the group G.

Proof.

Let G be a group of order 24.
Note that $24 = 2^3 \cdot 3$.
Let P be a Sylow 2-subgroup of G. Then $|P| = 8$.

Consider the action of the group G on the left cosets G/P by left multiplication.
This induces a permutation representation homomorphism

$$\phi : G \to S_{G/P},$$

where $S_{G/P}$ is a group of bijective maps (permutations) on G/P.
This homomorphism is defined by

$$\phi(g)(aP) = gaP$$

for $g \in G$ and $aP \in G/P$.

Then by the first isomorphism theorem, we see that

$$G/\ker(\phi) \cong \mathrm{im}(\phi) < S_{G/P}.$$

This implies that the order of $G/\ker(\phi)$ divides the order of $S_{G/P}$. Note that as $|G/P| = 3$, we have $|S_{G/P}| = |S_3| = 6$. Thus, we must have $4 \mid |\ker\phi|$.

Also note that $\ker(\phi) < P$. To see this let $x \in \ker(\phi)$. Then we have

$$xP = \phi(x)(P) = \mathrm{id}(P) = P.$$

Here id is the identity map from G/P to itself. Hence $x \in P$. It follows that $|\ker(\phi)|$ divides $|P| = 8$.

Combining these restrictions, we see that $|\ker(\phi)| = 4, 8$.
Being the kernel of a homomorphism, $\ker(\phi)$ is a normal subgroup of G.
Hence the group G of order 24 has a normal subgroup of order 4 or 8.

The Normalizer of a Proper Subgroup of a Nilpotent Group is Strictly Bigger

Problem 523

Let G be a nilpotent group and let H be a proper subgroup of G.
Then prove that $H \subsetneq N_G(H)$, where $N_G(H)$ is the normalizer of H in G.

Proof.

Note that we always have $H \subset N_G(H)$.
Hence our goal is to find an element in $N_G(H)$ that does not belong to H.

Since G is a nilpotent group, it has a lower central series

$$G = G^0 \triangleright G^1 \triangleright \cdots \triangleright G^n = \{e\},$$

where $G = G^0$ and G^i is defined by

$$G^i = [G^{i-1}, G] = \langle [x, y] = xyx^{-1}y^{-1} \mid x \in G^{i-1}, y \in G \rangle$$

successively, and e is the identity element of G.

Since H is a proper subgroup of G, there is an index k such that

$$G^{k+1} \subset H \text{ but } G^k \not\subseteq H.$$

Take any $x \in G^k \setminus H$.
We claim that $x \in N_G(H)$.

For any $y \in H$, it follows from the definition of G^{k+1} that

$$[x, y] \in G^{k+1} \subset H.$$

Hence $xyx^{-1}y^{-1} \in H$.
Since $y \in H$, we see that $xyx^{-1} \in H$.
As this is true for any $y \in H$, we conclude that $x \in N_G(H)$.
The claim is proved.

Since x does not belong to H, we conclude that $H \subsetneq N_G(H)$.

Elements of Finite Order of an Abelian Group form a Subgroup

Problem 522

Let G be an abelian group and let H be the subset of G consisting of all elements of G of finite order. That is,

$$H = \{a \in G \mid \text{the order of } a \text{ is finite}\}.$$

Prove that H is a subgroup of G.

Proof.

Note that the identity element e of G has order 1, hence $e \in H$ and H is not an empty set.
To show that H is a subgroup of G, we need to show that H is closed under multiplications and inverses.

Let $a, b \in H$.
By definition of H, the orders of a, b are finite.
So let $m, n \in \mathbb{N}$ be the orders of a, b, respectively:
We have

$$a^m = e \text{ and } b^n = e.$$

Then we have

$$\begin{aligned} (ab)^{mn} &= a^{mn}b^{mn} && \text{since } G \text{ is abelian} \\ &= (a^m)^n (b^n)^m \\ &= e^n e^m = e. \end{aligned}$$

This implies that the order of ab is at most mn, hence the order of ab is finite.
Thus $ab \in H$ for any $a, b \in H$.

Next, consider any $a \in H$. We want to show that the inverse a^{-1} also lies in H.
Let $m \in \mathbb{N}$ be the order of a.

Then we have

$$(a^{-1})^m = (a^m)^{-1} = e^{-1} = e.$$

This implies that the order of a^{-1} is also finite, and hence $a^{-1} \in H$.

Therefore we have proved that H is closed under multiplications and inverses.
Hence H is a subgroup of G.

The Additive Group of Rational Numbers and The Multiplicative Group of Positive Rational Numbers are Not Isomorphic

Problem 510

Let $(\mathbb{Q}, +)$ be the additive group of rational numbers and let $(\mathbb{Q}_{>0}, \times)$ be the multiplicative group of positive rational numbers.
Prove that $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{>0}, \times)$ are not isomorphic as groups.

Proof.

Suppose, towards a contradiction, that there is a group isomorphism

$$\phi : (\mathbb{Q}, +) \to (\mathbb{Q}_{>0}, \times).$$

Then since ϕ is in particular surjective, there exists $r \in \mathbb{Q}$ such that $\phi(r) = 2$.
As r is a rational number, so is $r/2$.
It follows that we have

$$\begin{aligned} 2 = \phi(r) &= \phi\left(\frac{r}{2} + \frac{r}{2}\right) \\ &= \phi\left(\frac{r}{2}\right) \cdot \phi\left(\frac{r}{2}\right) && \text{because } \phi \text{ is a homomorphism} \\ &= \phi\left(\frac{r}{2}\right)^2. \end{aligned}$$

It yields that

$$\phi\left(\frac{r}{2}\right) = \pm\sqrt{2}.$$

However, this is a contradiction since $\phi\left(\frac{r}{2}\right)$ must be a positive rational number, yet $\sqrt{2}$ is not a rational number.
We conclude that there is no such group isomorphism, and hence the groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{>0} \times)$ are not isomorphic as groups.

The Existence of an Element in an Abelian Group of Order the Least Common Multiple of Two Elements

Problem 497

Let G be an abelian group.
Let a and b be elements in G of order m and n, respectively.
Prove that there exists an element c in G such that the order of c is the least common multiple of m and n.
Also determine whether the statement is true if G is a non-abelian group.

Hint.

First, consider the case when m and n are relatively prime.

Proof.

When m and n are relatively prime

Recall that if the orders m, n of elements a, b of an abelian group are relatively prime, then the order of the product ab is mn.

(For a proof, see the post "Order of the Product of Two Elements in an Abelian Group".)

So if m, n are relatively prime, then we can take $c = ab \in G$ and c has order mn, which is the least common multiple.

The general Case

Now we consider the general case.

Let p_i be the prime factors of either m or n.

Then write prime factorizations of m and n as

$$m = \prod_i p_i^{\alpha_i} \text{ and } n = \prod_i p_i^{\beta_i}.$$

Here α_i and β_i are nonzero integers (could be zero).

Define

$$m' = \prod_{i:\alpha_i \geq \beta_i} p_i^{\alpha_i} \text{ and } n' = \prod_{i:\beta_i > \alpha_i} p_i^{\beta_i}.$$

(For example, if $m = 2^3 \cdot 3^2 \cdot 5$ and $n = 3^2 \cdot 7$ then $m' = 2^3 \cdot 3^2 \cdot 5$ and $n' = 7$.)

Note that $m' \mid m$ and $n' \mid n$, and also m' and n' are relatively prime. The least common multiple l of m and n is given by

$$l = m'n'$$

Consider the element $a' := a^{m/m'}$. We claim that the order of a' is m'.

Let k be the order of the element a'. Then we have

$$e = (a')^k = (a^{\frac{m}{m'}})^k = a^{mk/m'},$$

where e is the identity element in the group G.

This yields that m divides mk/m' since m is the order of a.

It follows that m' divides k.

On the other hand, we have

$$(a^{m/m'})^{m'} = a^m = e,$$

and hence k divides m' since k is the order of the element $a^{m/m'}$.

As a result, we have $k = m'$.
So the order of a' is m'.

Similarly, the order of $b' := b^{n/n'}$ is n'.
The orders of elements a' and b are m' and n', and they are relatively prime.
Hence we can apply the first case and we conclude that the element $a'b'$ has order

$$m'n' = l.$$

Thus, we can take $c = a'b'$.

The Case When G is a Non-Abelian Group

Next, we show that if G is a non-abelian group then the statement does not hold.
For example, consider the symmetric group S_3 with three letters.
Let

$$a = (1\,2\,3) \text{ and } b = (1\,2).$$

Then the order of a is 3 and the order of b is 2.
The least common multiple of 2 and 3 is 6.
However, the symmetric group S_3 have no elements of order 6.
Hence the statement of the problem does not hold for non-abelian groups.

Related Question.

Problem. Let G be a group. Let a and b be elements of G.
If the order of a, b are m, n respectively, then is it true that the order of the product ab divides mn? If so give a proof. If not, give a counterexample.

For a solution of this problem, see the post "Order of Product of Two Elements in a Group".

Every Finite Group Having More than Two Elements Has a Nontrivial Automorphism

Problem 495

Prove that every finite group having more than two elements has a nontrivial automorphism.
(*Michigan State University, Abstract Algebra Qualifying Exam*)

Proof.

Let G be a finite group and $|G| > 2$.

Case When G is a Non-Abelian Group

Let us first consider the case when G is a non-abelian group.
Then there exist elements $g, h \in G$ such that $gh \neq hg$.
Consider the map $\phi : G \to G$ defined by sending $x \in G$ to gxg^{-1}.
Then it is straightforward to check that ϕ is a group homomorphism and its inverse is given by the conjugation by g^{-1}.
Hence ϕ is an automorphism.

If $\phi = 1$, then we have $h = \phi(h) = ghg^{-1}$, and this implies that $gh = hg$.
This contradicts our choice of g and h.
Hence ϕ is a non-trivial automorphism of G.

Case When G is an Abelian Group

Next consider the case when G is a finite abelian group of order greater than 2.
Since G is an abelian group the map $\psi : G \to G$ given by $x \mapsto x^{-1}$ is an isomorphism, hence an automorphism.
If ψ is a trivial automorphism, then we have $x = \psi(x) = x^{-1}$.
Thus, $x^2 = e$, where e is the identity element of G.

Sub-Case When G has an Element of Order ≥ 3.

Therefore, if G has at least one element of order greater than 2, then ψ is a non-trivial automorphism.

Sub-Case When Elements of G has order ≤ 2.

It remains to consider the case when G is a finite abelian group such that $x^2 = e$ for all elements $x \in G$.
In this case, the group G is isomorphic to

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^n.$$

Since $|G| > 2$, we have $n > 1$.
Then the map $(\mathbb{Z}/2\mathbb{Z})^n \to (\mathbb{Z}/2\mathbb{Z})^n$ defined by exchanging the first two entries

$$(x_1, x_2, x_3, \dots, x_n) \mapsto (x_2, x_1, x_3, \dots, x_n)$$

is an example of nontrivial automorphism of G.
Therefore, in any case, the group G has a nontrivial automorphism.

If Two Subsets A, B of a Finite Group G are Large Enough, then $G = AB$

Problem 493

Let G be a finite group and let A, B be subsets of G satisfying

$$|A| + |B| > |G|.$$

Here $|X|$ denotes the cardinality (the number of elements) of the set X.
Then prove that $G = AB$, where

$$AB = \{ab \mid a \in A, b \in B\}.$$

Proof.

Since A, B are subsets of the group G, we have $AB \subset G$.
Thus, it remains to show that $G \subset AB$, that is any element $g \in G$ is of the form ab for some $a \in A$ and $b \in B$.
This is equivalent to finding $a \in A$ and $b \in B$ such that $gb^{-1} = a$.
Consider the subset

$$B^{-1} := \{b^{-1} \mid b \in B\}.$$

Since taking the inverse gives the bijective map $B \to B^{-1}, b \mapsto b^{-1}$, we have $|B| = |B^{-1}|$.

Also consider the subset

$$gB^{-1} = \{gb^{-1} \mid b \in B\}.$$

Note that multiplying by g and by its inverse g^{-1} give the bijective maps

$$B^{-1} \to gB^{-1}, b^{-1} \mapsto gb^{-1} \text{ and } gB^{-1} \to B^{-1}, gb^{-1} \mapsto b^{-1}.$$

Hence we have

$$|B| = |B^{-1}| = |gB^{-1}|.$$

Since A and gB^{-1} are both subsets in G and we have by assumption that

$$|A| + |gB^{-1}| = |A| + |B| > |G|,$$

the intersection $A \cap gB^{-1}$ cannot be empty.
Therefore, there exists $a \in A \cap gB^{-1}$, and thus $a \in A$ and $a = gb^{-1}$ for some $b \in B$.
As a result we obtain $g = ab$.
It yields that $G \subset AB$, and we have $G = AB$ as a consequence.

Related Question.

As an application, or use the similar technique, try the following

Problem.
Every element in a finite field F is the sum of two squares in F.

See the post↴
Each Element in a Finite Field is the Sum of Two Squares
for a proof of this problem.

A Group Homomorphism that Factors though Another Group

Problem 490

Let G, H, K be groups. Let $f : G \to K$ be a group homomorphism and let $\pi : G \to H$ be a surjective group homomorphism such that the kernel of π is included in the kernel of f: $\ker(\pi) \subset \ker(f)$.
Define a map $\bar{f} : H \to K$ as follows.
For each $h \in H$, there exists $g \in G$ such that $\pi(g) = h$ since $\pi : G \to H$ is surjective.
Define $\bar{f} : H \to K$ by $\bar{f}(h) = f(g)$.
(a) Prove that the map $\bar{f} : H \to K$ is well-defined.
(b) Prove that $\bar{f} : H \to K$ is a group homomorphism.

Proof.

(a) Prove that the map $\bar{f} : H \to K$ is well-defined.

Let $h \in H$. Suppose that there are two elements $g, g' \in G$ such that $\pi(g) = h, \pi(g') = h$.
Then we have

$$\pi(gg'^{-1}) = \pi(g)\pi(g')^{-1} = hh^{-1} = 1$$

since π is a homomorphism.

Thus,

$$gg'^{-1} \in \ker(\pi) \subset \ker(f).$$

It yields that $f(gg'^{-1}) = 1$.
It follows that

$$1 = f(gg'^{-1}) = f(g)f(g')^{-1},$$

and hence we have

$$f(g) = f(g').$$

Therefore, the definition of $\bar{f}$ does not depend on the choice of elements $g \in G$ such that $\pi(g) = h$, hence it is well-defined.

(b) Prove that $\bar{f} : H \to K$ is a group homomorphism.

Our goal is to show that for any elements $h, h' \in H$, we have

$$\bar{f}(hh') = \bar{f}(h)\bar{f}(h').$$

Let g, g' be elements in G such that

$$\pi(g) = h \text{ and } \pi(g') = h'.$$

Then by definition of $\bar{f}$, we have

$$\bar{f}(h) = f(g) \text{ and } \bar{f}(h') = f(g'). \tag{*}$$

Since π is a homomorphism, we have

$$hh' = \pi(g)\pi(g') = \pi(gg').$$

By definition of $\bar{f}$, we have

$$\bar{f}(hh') = f(gg').$$

Since f is a homomorphism, we obtain

$$\begin{aligned} \bar{f}(hh') &= f(gg') \\ &= f(g)f(g') \\ &\overset{(*)}{=} \bar{f}(h)\bar{f}(h'). \end{aligned}$$

This proves that $\bar{f}$ is a group homomorphism.

If a Finite Group Acts on a Set Freely and Transitively, then the Numbers of Elements are the Same

Problem 488

Let G be a finite group and let S be a non-empty set.
Suppose that G acts on S freely and transitively.
Prove that $|G| = |S|$. That is, the number of elements in G and S are the same.

Definition (Free and Transitive Group Action)

- A group action of a group G on a set S is called **free** if whenever we have

$$gs = hs$$

for some $g, h \in G$ and $s \in S$, this implies $g = h$.

- A group action of a group G on a set S is called **transitive** if for each pair $s, t \in S$ there exists an element $g \in G$ such that

$$gs = t.$$

Proof.

We simply denote by gs the action of $g \in G$ on $s \in S$.

Since S is non-empty, we fix an element $s_0 \in S$. Define a map

$$\phi : G \to S$$

by sending $g \in G$ to $gs_0 \in S$.

We prove that the map ϕ is bijective.

Suppose that we have $\phi(g) = \phi(h)$ for some $g, h \in G$.

Then it gives $gs_0 = hs_0$, and since the action is free this implies that $g = h$.

Thus ϕ is injective.

To show that ϕ is surjective, let s be an arbitrary element in S.

Since the action is transitive, there exists $g \in G$ such that $gs_0 = s$.

Hence we have $\phi(g) = s$, and ϕ is surjective.

Therefore the map $\phi : G \to S$ is bijective, and we conclude that $|G| = |S|$.

Every Group of Order 72 is Not a Simple Group

Problem 474

Prove that every finite group of order 72 is not a simple group.

Definition.

A group G is said to be **simple** if the only normal subgroups of G are the trivial group $\{e\}$ or G itself.

Hint.

Let G be a group of order 72.

Use the Sylow's theorem and determine the number of Sylow 3-subgroups of G.

If there is only one Sylow 3-subgroup, then it is a normal subgroup, hence G is not simple.

If there are more than one, consider the action of G on those Sylow 3-subgroups given by conjugation.

Then consider the induced permutation representation.

For a review of the Sylow's theorem, check out the post "Sylow's Theorem (summary)".

Proof.

Observe the prime factorization $72 = 2^3 \cdot 3^2$.

Let G be a group of order 72.

Let n_3 be the number of Sylow 3-subgroups in G.

By Sylow's theorem, we know that n_3 satisfies

$$n_3 \equiv 1 \pmod 3 \text{ and}$$
$$n_3 \text{ divides } 8.$$

The first condition gives n_3 could be $1, 4, 7, \dots$.

Only $n_3 = 1, 4$ satisfy the second condition.

Now if $n_3 = 1$, then there is a unique Sylow 3-subgroup and it is a normal subgroup of order 9.

Hence, in this case, the group G is not simple.

It remains to consider the case when $n_3 = 4$.

So there are four Sylow 3-subgroups of G.

Note that these subgroups are not normal by Sylow's theorem.

The group G acts on the set of these four Sylow 3-subgroups by conjugation.

Hence it affords a permutation representation homomorphism

$$f : G \to S_4,$$

where S_4 is the symmetric group of degree 4.

By the first isomorphism theorem, we have

$$G/\ker f < S_4.$$

Thus, the order of $G/\ker f$ divides the order of S_4.

Since $|S_4| = 4! = 2^3 \cdot 3$, the order $|\ker f|$ must be divisible by 3 (otherwise $|G/\ker f| does not divide |S_4|$), hence \ker f$ is not the trivial group.

We claim that $\ker f \neq G$.

If $\ker f = G$, then it means that the action given by the conjugation by any element $g \in G$ is trivial.

That is, $gPg^{-1} = P$ for any $g \in G$ and for any Sylow 3-subgroup P.

Since those Sylow 3-subgroups are not normal, this is a contradiction.

Thus, $\ker f \neq G$.

Since a kernel of a homomorphism is a normal subgroup, this yields that $\ker f$ is a nontrivial proper normal subgroup of G, hence G is not a simple group.

A Subgroup of Index a Prime p of a Group of Order p^n is Normal

Problem 470

Let G be a finite group of order p^n, where p is a prime number and n is a positive integer.

Suppose that H is a subgroup of G with index $[G : P] = p$.

Then prove that H is a normal subgroup of G.

(*Michigan State University, Abstract Algebra Qualifying Exam*)

Proof.

Let G/H be the set of left cosets of H.

Then the group G acts on G/H by the left multiplication.

This action induces the permutation representation homomorphism

$$\phi: G \to S_{G/H},$$

where $S_{G/H}$ is the symmetric group on G/H.

For each $g \in G$, the map $\phi(g): G/H \to G/H$ is given by $x \mapsto gx$.

By the first isomorphism theorem, we have

$$G/\ker(\phi) \cong \mathrm{im}(\phi) < S_{G/H}.$$

This implies the order $|G/\ker(\phi)|$ divides the order $|S_{G/H}| = p!$.

Since

$$|G/\ker(\phi)| = \frac{|G|}{|\ker(\phi)|} = \frac{p^n}{|\ker(\phi)|}$$

and $p!$ contains only one factor of p, we must have either $|\ker(\phi)| = p^n$ or $|\ker(\phi)| = p^{n-1}$.

Note that if $g \in \ker(\phi)$, then $\phi(g) = \mathrm{id}: G/H \to G/H$.

This yields that $gH = H$, and hence $g \in H$.

As a result, we have $\ker(\phi) \subset H$.

Since the index of H is p, the order of H is p^{n-1}.

Thus we conclude that $|\ker(\phi)| = p^{n-1}$ and

$$\ker(\phi) = H.$$

Since every kernel of a group homomorphism is a normal subgroup, the subgroup $H = \ker(\phi)$ is a normal subgroup of G.

If Squares of Elements in a Group Lie in a Subgroup, then It is a Normal Subgroup

Problem 469

Let H be a subgroup of a group G.

Suppose that for each element $x \in G$, we have $x^2 \in H$.

Then prove that H is a normal subgroup of G.

(*Purdue University, Abstract Algebra Qualifying Exam*)

Proof.

To show that H is a normal subgroup of G, we prove that

$$ghg^{-1} \in H$$

for any $g \in G$ and $h \in H$.

For any $g \in G$ and $h \in H$ we have

$$\begin{aligned} &ghg^{-1} \\ &= g^2g^{-1}hg^{-1} && \text{since } g = g^2g^{-1} \\ &= g^2g^{-1}hg^{-1}hh^{-1} && \text{since } e = hh^{-1} \\ &= g^2(g^{-1}h)^2h^{-1}. && (*) \end{aligned}$$

It follows from the assumption that the elements g^2 and $(g^{-1}h)^2$ are in H.

Since $h \in H$, the inverse h^{-1} is also in H.

Thus the expression in (*) is the product of elements in H, hence it is in H.

Thus, we have proved that $ghg^{-1} \in H$ for all $g \in G, h \in H$.

Therefore, the subgroup H is a normal subgroup in G.

Example of Two Groups and a Subgroup of the Direct Product that is Not of the Form of Direct Product

Problem 467

Give an example of two groups G and H and a subgroup K of the direct product $G \times H$ such that K cannot be written as $K = G_1 \times H_1$, where G_1 and H_1 are subgroups of G and H, respectively.

Solution.

Let G be any nontrivial group, and let $G = H$.

(For example, you may take $G = H = \mathbb{Z}/2\mathbb{Z}$.)

Then consider the subset K in the direct product given by

$$K := \{(g, g) \mid g \in G\} \subset G \times G.$$

We claim that K is a subgroup of $G \times G$.

In fact, we have

$$\begin{aligned}(g,g)(h,h) = (gh, gh) \in K \text{ and} \\ (g,g)^{-1} = (g^{-1}, g^{-1}) \in K\end{aligned}$$

for any $g, h \in G$.

Thus, K is closed under multiplications and inverses, and hence K is a subgroup of $G \times G$.

Now we show that K is not of the form $G_1 \times H_1$ for some subgroups G_1, H_1 of G.

Assume on the contrary $K = G_1 \times H_1$ for some subgroups G_1, H_1 of G.

Since G is a nontrivial group, there is a nonidentity element $x \in G$.

So $(x, x) \in K$ and K is not the trivial group.

Thus, both G_1 and H_1 cannot be the trivial group.

Without loss of generality, assume that G_1 is nontrivial.

Then G_1 contains a nonidentity element y.

Since the identity element e is contained in all subgroups, we have

$$(y, e) \in G_1 \times H_1.$$

However, this element cannot be in K since $y \neq e$, a contradiction.

Hence K is not of the form $G_1 \times H_1$.

The Symmetric Group is a Semi-Direct Product of the Alternating Group and a Subgroup $\langle (1,2) \rangle$

Problem 465

Prove that the symmetric group S_n, $n \geq 3$ is a semi-direct product of the alternating group A_n and the subgroup $\langle (1,2) \rangle$ generated by the element $(1,2)$.

Definition (Semi-Direct Product).

Internal Semi-Direct-Product

Recall that a group G is said to be an **(internal) semi-direct product** of subgroups H and K if the following conditions hold.

1. H is a normal subgroup of G.
2. $H \cap K = \{e\}$, where e is the identity element in G.
3. $G = HK$.

In this case, we denote the group by $G = H \rtimes K$.

External Semi-Direct Product

If G is an internal semi-direct product of H and K, it is an **external semi-direct product** defined by the homomorphism $\phi : K \to \mathrm{Aut}(H)$ given by mapping $k \in K$ to the automorphism of left conjugation by k on H.

That is, $G \cong H \rtimes_\phi K$.

Proof.

Recall that each element of the symmetric group S_n can be written as a product of transpositions (permutations which exchanges only two elements).

This defines a group homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$ that maps each element of S_n that is a product of even number of transpositions to 1, and maps each element of S_n that is a product of odd number of transpositions to -1.

The alternating group A_n is defined to be the kernel of the homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$:

$$A_n := \ker(\mathrm{sgn}).$$

As it is the kernel, the alternating group A_n is a normal subgroup of S_n.

Also by first isomorphism theorem, we have

$$S_n / A_n \cong \{\pm 1\},$$

and it yields that

$$|A_n| = \frac{|S_n|}{|\{\pm 1\}|} = \frac{n!}{2}.$$

Since $\mathrm{sgn}(\,(1,2)\,) = -1$, the intersection of A_n and $\langle (1,2) \rangle$ is trivial:

$$A_n \cap \langle (1,2) \rangle = \{e\}.$$

Let $H = A_n$ and $K = \langle (1,2) \rangle$.

Then we have

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = \frac{n!}{2} \cdot 2 = n!.$$

Since $HK < S_n$ and both groups have order $n!$, we have $S_n = HK$.

In summary we have observed that $H = A_n$ and $K = \langle (1,2) \rangle$ satisfies the conditions for a semi-direct product of $G = S_n$.

Hence

$$S_n = A_n \rtimes \langle (1,2) \rangle.$$

As an external semi-direct product, it is given by

$$S_n \cong A_n \rtimes_\phi \langle (1,2) \rangle,$$

where $\phi : \langle (1,2) \rangle \to \mathrm{Aut}(A_n)$ is given by

$$\phi\left((1,2) \right)(x) = (1,2)x(1,2)^{-1}.$$

Every Sylow 11-Subgroup of a Group of Order 231 is Contained in the Center $Z(G)$

Problem 464

Let G be a finite group of order $231 = 3 \cdot 7 \cdot 11$.

Prove that every Sylow 11-subgroup of G is contained in the center $Z(G)$.

Hint.

Prove that there is a unique Sylow 11-subgroup of G, and consider the action of G on the Sylow 11-subgroup by conjugation.

Check out the post "Sylow's Theorem (summary)" for a review of Sylow's theorem.

Proof.

We first claim that there is a unique Sylow 11-subgroup of G.

Let n_{11} be the number of Sylow 11-subgroups in G.

By Sylow's theorem, we know that

$$\begin{aligned} &n_{11} \equiv 1 \pmod{11} \\ &n_{11} | 21. \end{aligned}$$

By the first condition, $n_{11} = 1, 12, 23 \cdots$ and only $n_{11} = 1$ divides 21.

Thus, we have $n_{11} = 1$ and there is only one Sylow 11-subgroup P_{11} in G, and hence it is normal in G.

Now we consider the action of G on the normal subgroup P_{11} given by conjugation.

The action induces the permutation representation homomorphism

$$\psi : G \to \mathrm{Aut}(P_{11}),$$

where $\mathrm{Aut}(P_{11})$ is the automorphism group of P_{11}.

Note that P_{11} is a group of order 11, hence it is isomorphic to the cyclic group $\mathbb{Z}/11\mathbb{Z}$.

Recall that

$$\mathrm{Aut}(\mathbb{Z}/11\mathbb{Z}) \cong (\mathbb{Z}/11\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z}.$$

The first isomorphism theorem gives

$$G/\ker(\psi) \cong \mathrm{im}(\psi) < \mathrm{Aut}(P_{11}) \cong \mathbb{Z}/10\mathbb{Z}.$$

Hence the order of $G/\ker(\psi)$ must be a divisor of 10.

Since $|G| = 231 = 3 \cdot 7 \cdot 11$, the only possible way for this is $|G/\ker(\psi)| = 1$ and thus $\ker(\psi) = G$.

This implies that for any $g \in G$, the automorphism $\psi(g) : P_{11} \to P_{11}$ given by $h \mapsto ghg^{-1}$ is the identity map.

Thus, we have $ghg^{-1} = h$ for all $g \in G$ and $h \in H$.

It yields that P_{11} is in the center $Z(G)$ of G.

Every Group of Order 20449 is an Abelian Group

Problem 462

Prove that every group of order 20449 is an abelian group.

Outline of the Proof

Note that $20449 = 11^2 \cdot 13^2$.

Let G be a group of order 20449.

We prove by Sylow's theorem that there are a unique Sylow 11-subgroup and a unique Sylow 13-subgroup of G.

Hence G is the direct product of these Sylow subgroups.

Since these Sylow subgroups are of order 11^2 and 13^2, respectively, they are abelian.

Since the direct product of abelian groups is abelian, the group G is abelian.

Proof.

Observe that $20449 = 11^2 \cdot 13^2$.

Let G be a group of order 20449.

Let n_{11} be the number of Sylow 11-subgroups of G.

By Sylow's theorem, n_{11} satisfies

$$\begin{aligned} &n_{11} \equiv 1 \pmod{11} \text{ and} \\ &n_{11} \text{ divides } 13^2. \end{aligned}$$

The second condition yields that n_{11} could be $1, 13, 13^2$.

Among these numbers, only $n_{11} = 1$ satisfies the first condition.

So there is a unique Sylow 11-subgroup P_{11} of G, hence P_{11} is a normal subgroup of G.

Similarly, let n_{13} be the number of Sylow 13-subgroups of G.

Sylow's theorem yields that n_{13} satisfies:

$$\begin{aligned} &n_{13} \equiv 1 \pmod{13} \text{ and} \\ &n_{13} \text{ divides } 11^2. \end{aligned}$$

From the second condition, we see that n_{13} could be $1, 11, 13$.

Among these numbers, only $n_{13} = 1$ satisfies the first condition.

So there is a unique Sylow 13-subgroup P_{13} of G, hence P_{13} is a normal subgroup of G.

Note that the orders of P_{11} and P_{13} are 11^2 and 13^2, respectively.

The intersection of P_{11} and P_{13} is the trivial group.

Thus, we have

$$|G| = \frac{|P_{11}P_{13}|}{|P_{11} \cap P_{13}|} = |P_{11}P_{13}|.$$

This yields that $G = P_{11}P_{13}$.

In summary, we have

- Sylow subgroups P_{11} and P_{13} are normal in G.
- $P_{11} \cap P_{13} = \{e\}$.
- $G = P_{11}P_{13}$.

These implies that G is the direct product of P_{11} and P_{13}:

$$G = P_{11} \times P_{13}.$$

Recall that every group of order p^2 for some prime number p is an abelian group.

Thus, P_{11} and P_{13} are both abelian group.

Since the direct product of abelian groups is abelian, we conclude that the group $G = P_{11} \times P_{13}$ is abelian.

The Group of Rational Numbers is Not Finitely Generated

Problem 461

(a) Prove that the additive group $\mathbb{Q} = (\mathbb{Q}, +)$ of rational numbers is not finitely generated.
(b) Prove that the multiplicative group $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \times)$ of nonzero rational numbers is not finitely generated.

Proof.

(a) Prove that the additive group $\mathbb{Q} = (\mathbb{Q}, +)$ is not finitely generated.

Seeking a contradiction assume that the group $\mathbb{Q} = (\mathbb{Q}, +)$ is finitely generated and let $r_1, \dots, r_n$ be nonzero generators of $\mathbb{Q}$.

Express the generators as fractions

$$r_i = \frac{a_i}{b_i},$$

where a_i, b_i are integers.

Then every rational number r can be written as the sum

$$r = c_1 r_1 + \cdots + c_k r_n$$

for some integers $c_1, \dots, c_n$.

Then we have

$$r = \frac{m}{b_1 \cdots b_n},$$

where m is an integer (which you can write down explicitly using a_i, c_i).

Let p be a prime number that does not divide $b_1 \cdots b_n$, and choose $r = 1/p$.

Then we must have

$$\frac{1}{p} = \frac{m}{b_1 \cdots b_n}$$

for some integer m.

Then we have

$$pm = b_1 \cdots b_n$$

and this implies p divides $b_1 \cdots b_n$, which contradicts our choice of the prime number p.

Thus, the group $\mathbb{Q}$ cannot be finitely generated.

(b) Prove that the multiplicative group $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \times)$ of nonzero rational numbers is not finitely generated.

Suppose on the contrary that the group $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \times)$ is finitely generated and let

$$r_i = \frac{a_i}{b_i}$$

be generators for $i = 1, \dots, n$, where a_i, b_i are integers.

Then every nonzero rational number r can be written as

$$r = r_1^{c_1} \cdots r_n^{c_n} = \frac{a_1^{c_1} \cdots a_n^{c_n}}{b_1^{c_1} \cdots b_n^{c_n}}$$

for some integers c_n.

Let p be a prime number that does not divide $b_1 \cdots b_n$, and consider $r = 1/p$.

Then as in part (a), this leads a contradiction.

Hence $\mathbb{Q}^*$ is not finitely generated.

Every Finitely Generated Subgroup of Additive Group $\mathbb{Q}$ of Rational Numbers is Cyclic

Problem 460

Let $\mathbb{Q} = (\mathbb{Q}, +)$ be the additive group of rational numbers.
(a) Prove that every finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic.
(b) Prove that $\mathbb{Q}$ and $\mathbb{Q} \times \mathbb{Q}$ are not isomorphic as groups.

Proof.

(a) Prove that every finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic.

Let G be a finitely generated subgroup of $(\mathbb{Q}, +)$ and let $r_1, \dots, r_n$ be nonzero generators of G.

Let us express

$$r_i = \frac{a_i}{b_i},$$

where a_i, b_i are integers.

Let

$$s := \frac{1}{\prod_{j=1}^{n} b_j} \in \mathbb{Q}.$$

Then we can write each r_i as

$$r_i = \frac{a_i}{b_i} = \left(a_i \prod_{\substack{j=1 \\ j \neq i}}^{n} b_i \right) \cdot \frac{1}{s}.$$

It follows from the last expressions that the elements r_i is contained in the subgroup $\langle s \rangle$ generated by the element s.

Hence G is a subgroup of $\langle s \rangle$.

Since every subgroup of a cyclic group is cyclic, we conclude that G is also cyclic.

(b) Prove that $\mathbb{Q}$ and $\mathbb{Q} \times \mathbb{Q}$ are not isomorphic as groups.

Seeking a contradiction, assume that $\mathbb{Q}$ is isomorphic to the direct product $\mathbb{Q} \times \mathbb{Q}$:

$$\mathbb{Q} \cong \mathbb{Q} \times \mathbb{Q}.$$

Then consider the subgroup $\mathbb{Z} \times \mathbb{Z}$ of $\mathbb{Q} \times \mathbb{Q}$.

We claim that the subgroup $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

If it were cyclic, then there would be a generator $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

However, for example, the element $(b, -a)$ cannot be expressed as an integer multiple of (a, b).

To see this, suppose that

$$n(a, b) = (b, -a)$$

for some integer n.

Then we have $na = b$ and $nb = -a$. Substituting the first equality into the second one, we obtain

$$n^2 a = -a.$$

If $a \neq 0$, then this yields that $n^2 = -1$, which is impossible, and hence $a = 0$.

Then $na = b$ implies $b = 0$ as well.

However, $(a, b) = (0, 0)$ is clearly not a generator of $\mathbb{Z} \times \mathbb{Z}$.

Thus we have reached a contradiction and $\mathbb{Z} \times \mathbb{Z}$ is a non-cyclic subgroup of $\mathbb{Q} \times \mathbb{Q}$.

This implies via the isomorphism $\mathbb{Q} \cong \mathbb{Q} \times \mathbb{Q}$ that $\mathbb{Q}$ has a non-cyclic subgroup.

We saw in part (a) that this is impossible.

Therefore, $\mathbb{Q}$ is not isomorphic to $\mathbb{Q} \times \mathbb{Q}$.

Prove that a Group of Order 217 is Cyclic and Find the Number of Generators

Problem 458

Let G be a finite group of order 217.

(a) Prove that G is a cyclic group.

(b) Determine the number of generators of the group G.

Sylow's Theorem

We will use Sylow's theorem to prove part (a).

For a review of Sylow's theorem, check out the post "Sylow's Theorem (summary)".

Proof.

(a) Prove that G is a cyclic group.

Note the prime factorization $217 = 7 \cdot 31$.

We first determine the number n_p of Sylow p-group for $p = 7, 31$.

Recall from Sylow's theorem that

$$n_p \equiv 1 \pmod{p}$$

$$n_p \text{ divides } n/p.$$

Thus, n_7 could be $1, 8, 15, 22, 29, \ldots$ and n_7 needs to divide $217/7 = 31$.

Hence the only possible value for n_7 is $n_7 = 1$.

So there is a unique Sylow 7-subgroup P_7 of G.

By Sylow's theorem, the unique Sylow 7-subgroup must be a normal subgroup of G.

Similarly, $n_{31} = 1, 32, \ldots$ and n_{31} must divide $217/31 = 7$, and hence we must have $n_{31} = 1$.

Thus G has a unique normal Sylow 31-subgroup P_{31}.

Note that these Sylow subgroup have prime order, and hence they are isomorphic to cyclic groups:

$$P_7 \cong \mathbb{Z}/7\mathbb{Z} \text{ and } P_{31} \cong \mathbb{Z}/31\mathbb{Z}.$$

It is also straightforward to see that $P_7 \cap P_{31} = \{e\}$, where e is the identity element in G.

In summary, we have

1. P_7, P_{31} are normal subgroups of G.
2. $P_7 \cap P_{31} = \{e\}$.
3. $|P_7 P_{31}| = |G|$.

These yields that G is a direct product of P_7 and P_{31}, and we obtain

$$G = P_7 \times P_{31} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z} \cong \mathbb{Z}/217\mathbb{Z}.$$

Hence G is a cyclic group.

(b) Determine the number of generators of the group G.

Recall that the number of generators of a cyclic group of order n is equal to the number of integers between 1 and n that are relatively prime to n.

Namely, the number of generators is equal to $\phi(n)$, where ϕ is the Euler totient function.

By part (a), we know that G is a cyclic group of order 217.

Thus, the number of generators of G is

$$\phi(217) = \phi(7)\phi(31) = 6 \cdot 30 = 180,$$

where the first equality follows since ϕ is multiplicative.

The Order of a Conjugacy Class Divides the Order of the Group

Problem 455

Let G be a finite group.
The **centralizer** of an element a of G is defined to be

$$C_G(a) = \{g \in G \mid ga = ag\}.$$

A **conjugacy class** is a set of the form

$$\mathrm{Cl}(a) = \{bab^{-1} \mid b \in G\}$$

for some $a \in G$.

(a) Prove that the centralizer of an element of a in G is a subgroup of the group G.
(b) Prove that the order (the number of elements) of every conjugacy class in G divides the order of the group G.

Proof.

(a) Prove that the centralizer of a in G is a subgroup of G.

Since the identity element e of G satisfies $ea = a = ae$, it is in the centralizer $C_G(a)$.
Hence $C_G(a)$ is not an empty set. We show that $C_G(a)$ is closed under multiplications and inverses.
Let $g, h \in C_G(a)$. Then we have

$$\begin{aligned}
(gh)a &= g(ha) \\
&= g(ah) && \text{since } h \in C_G(a) \\
&= (ga)h \\
&= (ag)h && \text{since } g \in C_G(a) \\
&= a(gh).
\end{aligned}$$

So gh commutes with a and thus $gh \in C_G(a)$.
Thus $C_G(a)$ is closed under multiplications.
Let $g \in C_G(a)$. This means that we have $ga = ag$.
Multiplying by g^{-1} on the left and on the right, we obtain

$$g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1},$$

and thus we have

$$ag^{-1} = g^{-1}a.$$

This implies that $g^{-1} \in C_G(a)$, hence $C_G(a)$ is closed under inverses.
Therefore, $C_G(a)$ is a subgroup of G.

(b) Prove that the order of every conjugacy class in G divides the order of G.

We give two proofs for part (b).The first one is a more direct proof and the second one uses the orbit-stabilizer theorem.

The First Proof of (b).

By part (a), the centralizer $C_G(a)$ is a subgroup of the finite group G.
Hence the set of left cosets $G/C_G(a)$ is a finite set, and its order divides the order of G by Lagrange's theorem.
We prove that there is a bijective map from $G/C_G(a)$ to $\mathrm{Cl}(a)$.
Define the map $\phi : G/C_G(a) \to \mathrm{Cl}(a)$ by

$$\phi\left(gC_G(a) \right) = gag^{-1}.$$

We must show that it is well-defined.
For this, note that we have

$$\begin{aligned} gC_G(a) = hC_G(a) &\Leftrightarrow h^{-1}g \in C_G(a) \\ &\Leftrightarrow (h^{-1}g)a(h^{-1}g)^{-1} = a \\ &\Leftrightarrow gag^{-1} = hag^{-1}. \end{aligned}$$

This computation shows that the map ϕ is well-defined as well as ϕ is injective.
Since the both sets are finite sets, this implies that ϕ is bijective.
Thus, the order of the two sets is equal.
It yields that the order of $C_G(a)$ divides the order of the finite group G.

The Second Proof of (b). Use the Orbit-Stabilizer Theorem

We now move on to the alternative proof.
Consider the action of the group G on itself by conjugation:

$$\psi : G \times G \to G, \quad (g, h) \mapsto g \cdot h = ghg^{-1}.$$

Then the orbit $\mathcal{O}(a)$ of an element $a \in G$ under this action is

$$\mathcal{O}(a) = \{g \cdot a \mid g \in G\} = \{gag^{-1} \mid g \in G\} = \mathrm{Cl}(a).$$

Let G_a be the stabilizer of a.
Then the **orbit-stabilizer theorem** for finite groups say that we have

$$|\mathrm{Cl}(a)| = |\mathcal{O}(a)| = [G : G_a] = \frac{|G|}{|G_a|}$$

and hence the order of $\mathrm{Cl}(a)$ divides the order of G.
Note that the stabilizer G_a of a is the centralizer $C_G(a)$ of a since

$$G_a = \{g \in G \mid g \cdot a = a\} = \{g \in G \mid ga = ag\} = C_G(a).$$

The Product of a Subgroup and a Normal Subgroup is a Subgroup

Problem 448

Let G be a group. Let H be a subgroup of G and let N be a normal subgroup of G.
The **product** of H and N is defined to be the subset

$$H \cdot N = \{hn \in G \mid h \in H, n \in N\}.$$

Prove that the product $H \cdot N$ is a subgroup of G.

Definition.

A subgroup N of a group G is called a **normal subgroup** if for any $g \in G$ and $n \in N$, we have

$$gng^{-1} \in N.$$

Proof.

We prove that the product $H \cdot N$ is closed under products and inverses.

Let h_1n_1 and h_2n_2 be elements in $H \cdot N$, where $h_1, h_2 \in H$ and $n_1, n_2 \in N$.

Let e be the identity element in G.

We have

$$\begin{aligned}(h_1n_1)(h_2n_2) &= h_1en_1h_2n_2 \\ &= h_1(h_2h_2^{-1})n_1h_2n_2 \qquad \text{since } h_2h_2^{-1} = e \\ &= (h_1h_2)(h_2^{-1}n_1h_2n_2). \qquad (*)\end{aligned}$$

Since H is a subgroup, the element h_1h_2 is in H.

Also, since N is a normal subgroup, we have $h_2^{-1}n_1h_2$ is in N. Hence

$$h_2^{-1}n_1h_2n_2 = (h_2^{-1}n_1h_2)n_2 \in N.$$

It follows from (*) that the product

$$(h_1n_1)(h_2n_2) = (h_1h_2)(h_2^{-1}n_1h_2n_2) \in H \cdot N.$$

Therefore, the product $H \cdot N$ is closed under products.

Next, let hn be any element in $H \cdot N$, where $h \in H$ and $n \in N$.

Then we have

$$\begin{aligned}(hn)^{-1} &= n^{-1}h^{-1} \\ &= en^{-1}h^{-1} \\ &= (h^{-1}h)n^{-1}h^{-1} \qquad \text{since } h^{-1}h = e \\ &= h^{-1}(hn^{-1}h^{-1}).\end{aligned}$$

Since N is a normal subgroup, we have $hn^{-1}h^{-1} \in N$, and hence

$$(hn)^{-1} = h^{-1}(hn^{-1}h^{-1}) \in H \cdot N.$$

Thus, the product $H \cdot N$ is closed under inverses.

This completes the proof that the product $H \cdot N$ is a subgroup of G.

Inverse Map of a Bijective Homomorphism is a Group Homomorphism

Problem 445

Let G and H be groups and let $\phi : G \to H$ be a group homomorphism.

Suppose that $f : G \to H$ is bijective.

Then there exists a map $\psi : H \to G$ such that

$$\psi \circ \phi = \mathrm{id}_G \text{ and } \phi \circ \psi = \mathrm{id}_H.$$

Then prove that $\psi : H \to G$ is also a group homomorphism.

Proof.

Let a, b be arbitrary elements of the group H.

To prove $\psi : H \to G$ is a group homomorphism, we need

$$\psi(ab) = \psi(a)\psi(b).$$

We compute

$$\begin{aligned}
&\phi\left(\psi(a)\psi(b)\right) \\
&= \phi\left(\psi(a)\right)\phi\left(\psi(b)\right) && \text{since } \phi \text{ is a group homomorphism} \\
&= ab && \text{since } \phi \circ \psi = \mathrm{id}_H \\
&= \phi\left(\psi(ab)\right) && \text{since } \phi \circ \psi = \mathrm{id}_H.
\end{aligned}$$

Since ϕ is injective, it yields that

$$\psi(ab) = \psi(a)\psi(b),$$

and thus $\psi : H \to G$ is a group homomorphism.

What's an Isomorphism?

A bijective group homomorphism $\phi : G \to H$ is called **isomorphism**.

The above problem guarantees that the inverse map of an isomorphism is again a homomorphism, and hence isomorphism.

Group Homomorphism Sends the Inverse Element to the Inverse Element

Problem 444

Let G, G' be groups. Let $\phi : G \to G'$ be a group homomorphism.

Then prove that for any element $g \in G$, we have

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

Definition (Group homomorphism).

A map $\phi : G \to G'$ is called a group homomorphism if

$$\phi(ab) = \phi(a)\phi(b)$$

for any elements $a, b \in G$.

Proof.

Let e, e' be the identity elements of G, G', respectively.

First we claim that

$$\phi(e) = e'.$$

In fact, we have

$$\phi(e) = \phi(ee) = \phi(e)\phi(e) \qquad (*)$$

since ϕ is a group homomorphism.

Thus, multiplying by $\phi(e)^{-1}$ on the left, we obtain

$$\begin{aligned} e' &= \phi(e)^{-1}\phi(e) \\ &= \phi(e)^{-1}\phi(e)\phi(e) \qquad \text{by } (*) \\ &= e'\phi(e) = \phi(e). \end{aligned}$$

Hence the claim is proved.

Then we have

$$\begin{aligned} e' &= \phi(e) && \text{by claim} \\ &= \phi(gg^{-1}) \\ &= \phi(g)\phi(g^{-1}) && \text{since } \phi \text{ is a group homomorphism.} \end{aligned}$$

It follows that we have

$$\begin{aligned} \phi(g)^{-1} &= \phi(g)^{-1}e' \\ &= \phi(g)^{-1}\phi(g)\phi(g^{-1}) \\ &= e'\phi(g^{-1}) \\ &= \phi(g^{-1}). \end{aligned}$$

This completes the proof.

Injective Group Homomorphism that does not have Inverse Homomorphism

Problem 443

Let $A = B = \mathbb{Z}$ be the additive group of integers.
Define a map $\phi : A \to B$ by sending n to $2n$ for any integer $n \in A$.
(a) Prove that ϕ is a group homomorphism.
(b) Prove that ϕ is injective.
(c) Prove that there does not exist a group homomorphism $\psi : B \to A$ such that $\psi \circ \phi = \mathrm{id}_A$.

Proof.

(a) Prove that ϕ is a group homomorphism.

For any integers $m, n \in A$, we have

$$\begin{aligned} \phi(m+n) &= 2(m+n) \\ &= 2m + 2n \\ &= \phi(m) + \phi(n). \end{aligned}$$

Thus, the map ϕ is a group homomorphism.

(b) Prove that ϕ is injective.

Suppose that we have

$$\phi(m) = \phi(n)$$

for some integers $m, n \in A$.

This yields that we have $2m = 2n$, and hence $m = n$.

So ϕ is injective.

Since ϕ is a group homomorphism, we can also prove the injectivity by showing that $\ker(\phi) = \{0\}$.

(For this, see the post "A Group Homomorphism is Injective if and only if the Kernel is Trivial".)

Suppose that we have

$$\phi(m) = 0.$$

Then we have $2m = 0$, and hence $m = 0$.

It follows that the group homomorphism ϕ is injective.

(c) Prove that there does not exist a group homomorphism $\psi : B \to A$ such that $\psi \circ \phi = \mathrm{id}_A$.

Seeking a contradiction, assume that there exists a group homomorphism $\psi : B \to A$ such that $\psi \circ \phi = \mathrm{id}_A$.

Then we compute

$$\begin{aligned} 1 &= \mathrm{id}_A(1) = \psi \circ \phi(1) \\ &= \psi(2) = \psi(1+1) \\ &= \psi(1) + \psi(1) \qquad \text{since } \psi \text{ is a group homomorphism} \\ &= 2\psi(1). \end{aligned}$$

It yields that

$$\psi(1) = \frac{1}{2}.$$

However note that $\psi(1)$ is an element in A, thus $\psi(1)$ is an integer.

Hence we got a contradiction, and we conclude that there is no such ψ.

Fundamental Theorem of Finitely Generated Abelian Groups and its application

Problem 420

In this post, we study the **Fundamental Theorem of Finitely Generated Abelian Groups**, and as an application we solve the following problem.

Problem.

Let G be a finite abelian group of order n.

If n is the product of distinct prime numbers, then prove that G is isomorphic to the cyclic group $Z_n = \mathbb{Z}/n\mathbb{Z}$ of order n.

Fundamental Theorem of Finitely Generated Abelian Groups

Before stating the fundamental theorem for finitely generated abelian groups, we define several terminologies and notations.

Definitions / notations

- We say that a group G is finitely generated if there is a finite subset S of G such that G is generated by S, that is, $G = \langle S \rangle$.
- For each positive integer r, let

$$\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ times}}$$

be the direct product of r copies of $\mathbb{Z}$. Here we set $\mathbb{Z}^0 = 1$ to be the trivial group.

- The group $\mathbb{Z}^r$ is called the free abelian group of rank r.
- For each positive integer n, let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n.

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)

Theorem. Let G be a finitely generated abelian group. Then it decomposes as follows:

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}, \tag{*}$$

for some integers $r, n_1, n_2, \ldots, n_s$ satisfying the following conditions:

1. $r \geq 0$ and $n_i \geq 2$ for all i, and
2. $n_{i+1} | n_i$ for $1 \leq i \leq s-1$.

The decomposition of G satisfying these conditions is unique.

- The integer r in the decomposition (*) is called the **free rank** or **Betti number** of G.
- The integers $n_1, n_2, \ldots, n_s$ are called the **invariant factors** of G.
- The decomposition (*) is called the **invariant factor decomposition** of G.

Problem

Let G be a finite abelian group of order n.

If n is the product of distinct prime numbers, then prove that G is isomorphic to the cyclic group $Z_n = \mathbb{Z}/n\mathbb{Z}$ of order n.

Proof.

Since G is a finite abelian group, it is in particular a finitely generated abelian group.

(We can take G itself for a finite set of generators of G.)

Then by the fundamental theorem of finitely generated abelian groups, we have the invariant factor decomposition

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

satisfying

1. $r \geq 0$ and $n_i \geq 2$ for all i, and
2. $n_{i+1} | n_i$ for $1 \leq i \leq s-1$.

Since G is a finite group, the rank r must be 0. Thus we have an isomorphism

$$G \cong Z_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}.$$

Comparing the order, we have

$$n = n_1 n_2 \cdots n_s.$$

Let p be a prime factor of n. Then p divides some n_i.

If $i > 1$, then it follows from condition (2) that p divides n_1 as well.

Thus p^2 divides n. Since n is a square-free integer, this is a contradiction.

It follows that any prime factor of n divides only n_1.

Therefore we obtain $n = n_1$ and $s = 1$. So the invariant factor decomposition of G is

$$G \cong Z_n.$$

Hence G is isomorphic to the cyclic group $\mathbb{Z}_n$ of order n.

Reference

Abstract Algebra by Dummit and Foote (third edition) Section 5.2.

Prove a Group is Abelian if $(ab)^3 = a^3b^3$ and No Elements of Order 3

Problem 402

Let G be a group. Suppose that we have

$$(ab)^3 = a^3b^3$$

for any elements a, b in G. Also suppose that G has no elements of order 3.
Then prove that G is an abelian group.

Proof.

Let a, b be arbitrary elements of the group G. We want to show that $ab = ba$.
By the given relation $(ab)^3 = a^3b^3$, we have

$$ababab = a^3b^3.$$

Multiplying by a^{-1} on the left and b^{-1} on the right, we obtain

$$baba = a^2b^2,$$

or equivalently we have

$$(ba)^2 = a^2b^2 \tag{*}$$

for any $a, b \in G$.

Now we consider $aba^{-1}b^{-1}$ (such an expression is called the commutator of a, b).
We have

$$\begin{aligned}
(aba^{-1}b^{-1})^2 &= (a^{-1}b^{-1})^2(ab)^2 && \text{by (*)} \\
&= b^{-2}a^{-2}b^2a^2 && \text{by (*)} \\
&= b^{-2}(ba^{-1})^2a^2 && \text{by (*)} \\
&= b^{-2}ba^{-1}ba^{-1}a^2 \\
&= b^{-1}a^{-1}ba.
\end{aligned}$$

Hence we have obtained

$$(aba^{-1}b^{-1})^2 = b^{-1}a^{-1}ba \tag{**}$$

for any $a, b \in G$.

Taking the square of (**), we obtain

$$\begin{aligned}(aba^{-1}b^{-1})^4 &= (b^{-1}a^{-1}ba)^2\\ &= aba^{-1}b^{-1}. \qquad \text{by } (**)\end{aligned}$$

It follows that we have

$$(aba^{-1}b^{-1})^3 = e,$$

where e is the identity element of G.

Since the group G does not have an element of order 3, this yields that

$$aba^{-1}b^{-1} = e.$$

(Otherwise, the order of the element $aba^{-1}b^{-1}$ would be 3.)
This is equivalent to

$$ab = ba.$$

Thus, we have obtained $ab = ba$ for any elements a, b in G.
Therefore, the group G is abelian.

Related Question.

I came up with this problem when I solved the previous problem:

Problem. Prove that if a group G satisfies $(ab)^2 = a^2b^2$ for $a, b \in G$, then G is an abelian group.

(For a proof of this problem, see the post "Prove a group is abelian if $(ab)^2 = a^2b^2$".)
I wondered what happens if I change 2 to 3, and that's how I made this problem.

Prove a Group is Abelian if $(ab)^2 = a^2b^2$

Problem 401

Let G be a group. Suppose that

$$(ab)^2 = a^2b^2$$

for any elements a, b in G. Prove that G is an abelian group.

Proof.

To prove that G is an abelian group, we need

$$ab = ba$$

for any elements a, b in G.
By the given relation, we have

$$(ab)^2 = a^2b^2.$$

The left hand side is

$$(ab)^2 = (ab)(ab),$$

and thus the relation becomes

$$(ab)(ab) = a^2b^2.$$

Equivalently, we can express it as

$$abab = aabb.$$

Multiplying by a^{-1} on the left and b^{-1} on the right, we obtain

$$a^{-1}(abab)b^{-1} = a^{-1}(aabb)b^{-1}.$$

Since $a^{-1}a = e, bb^{-1} = e$, where e is the identity element of G, we have

$$ebae = eabe.$$

Since e is the identity element, it yields that

$$ba = ab$$

and this implies that G is an abelian group.

Related Question.

I wondered what happens if I change the number 2 in $(ab)^2 = a^2b^2$ into 3, and created the following problem:

> Problem. If G is a group such that $(ab)^3 = a^3b^3$ and G does not have an element of order 3, then G is an abelian group.

For a proof of this problem, see the post "Prove a group is abelian if $(ab)^3 = a^3b^3$ and no elements of order 3".

p-Group Acting on a Finite Set and the Number of Fixed Points

Problem 359

Let P be a p-group acting on a finite set X.
Let

$$X^P = \{x \in X \mid g \cdot x = x \text{ for all } g \in P\}.$$

The prove that

$$|X^P| \equiv |X| \pmod{p}.$$

Proof.

Let $\mathcal{O}(x)$ denote the orbit of $x \in X$ under the action of the group P.
Let $X^P = \{x_1, x_2, \dots, x_m\}$.
The orbits of an element in X^p under the action of P is the element itself, that is, $\mathcal{O}(x_i) = \{x_i\}$ for $i = 1, \dots, m$. Let $x_{m+1}, x_{m+2}, \dots, x_n$ be representatives of other orbits of X.
Then we have the decomposition of the set X into a disjoint union of orbits

$$X = \mathcal{O}(x_1) \sqcup \cdots \sqcup \mathcal{O}(x_m) \sqcup \mathcal{O}(x_{m+1}) \sqcup \cdots \sqcup \mathcal{O}(x_n).$$

For $j = m+1, \dots, n$, the orbit-stabilizer theorem gives

$$|\mathcal{O}(x_j)| = [P : \mathrm{Stab}_P(x_j)] = p^{\alpha_j}$$

for some positive integer α_j. Here $\alpha_j \neq 0$ otherwise $x_j \in X^P$.

Therefore we have

$$\begin{aligned} |X| &= \sum_{i=1}^{m} |\mathcal{O}(x_i)| + \sum_{j=m+1}^{n} |\mathcal{O}(x_j)| \\ &= \sum_{i=1}^{m} 1 + \sum_{j=m+1}^{n} p^{\alpha_j} \\ &= |X^P| + \sum_{j=m+1}^{n} p^{\alpha_j} \\ &\equiv |X^P| \pmod{p}. \end{aligned}$$

This completes the proof.

Order of Product of Two Elements in a Group

Problem 354

Let G be a group. Let a and b be elements of G.

If the order of a, b are m, n respectively, then is it true that the order of the product ab divides mn? If so give a proof. If not, give a counterexample.

Proof.

Let r be the order of the element ab.

Since we have

$$\begin{aligned} (ab)^{mn} &= a^{mn}b^{mn} \quad (\text{since } G \text{ is an abelian group}) \\ &= (a^m)^n (b^n)^m \\ &= 1 \end{aligned}$$

since $a^m = 1$ and $b^n = 1$.

This implies that the order r of ab divides mn, that is, we have

$$r | mn. \tag{*}$$

Now, since r is the order of ab we have

$$1 = (ab)^r = a^r b^r.$$

Then we have

$$1 = 1^n = a^{rn} b^{rn} = a^{rn}$$

since $b^n = 1$. This yields that the order m of the element a divides rn.

Since m and n are relatively prime, this implies that we have

$$m | r.$$

Similarly (switch the role of n and m), we obtain

$$n|r.$$

Thus we have

$$mn|r \qquad (**)$$

since m and n are relatively prime.

From (*) and (**), we have $r = mn$, and hence the order of the element ab is mn.

Related Question.

As a generalization of this problem, try the following problem.

Problem.Let G be an abelian group.

Let a and b be elements in G of order m and n, respectively.

Prove that there exists an element c in G such that the order of c is the least common multiple of m and n.

A proof of this problem is given in the post "The Existence of an Element in an Abelian Group of Order the Least Common Multiple of Two Elements".

Also See the post "Order of product of two elements in a group" for a similar problem about the order of elements in a non-abelian group.

Group Homomorphisms From Group of Order 21 to Group of Order 49

Problem 346

Let G be a finite group of order 21 and let K be a finite group of order 49.

Suppose that G does not have a normal subgroup of order 3.

Then determine all group homomorphisms from G to K.

Proof.

Let e be the identity element of the group K.

We claim that every group homomorphism from G to K is trivial.

Namely, if $\phi : G \to K$ is a group homomorphism, then we have $\phi(g) = e$ for every $g \in G$.

The first isomorphism theorem gives the isomorphism

$$G/\ker(\phi) \cong \mathrm{im}(\phi) < K.$$

It follows that the order $|\mathrm{im}(\phi)|$ of the image $\mathrm{im}(\phi)$ is a divisor of the order of G and that of K. Hence the order $|\mathrm{im}(\phi)|$ divides the greatest common divisor of $|G| = 3 \cdot 7$ and $|K| = 7^2$, which is 7. So, the possibilities are $|\mathrm{im}(\phi)| = 1, 7$. If $|\mathrm{im}(\phi)| = 7$, then we have

$$\frac{|G|}{|\ker(\phi)|} = |\mathrm{im}(\phi)| = 7,$$

and we obtain $|\ker(\phi)| = 3$. Since the kernel of a group homomorphism is a normal subgroup, this contradicts the assumption that G does not have a normal subgroup of order 3. Therefore, we must have $|\mathrm{im}(\phi)| = 1$, and this implies that ϕ is a trivial homomorphism. Thus we conclude that every group homomorphism from G to K is trivial.

Number Theoretical Problem Proved by Group Theory. $a^{2^n}+b^{2^n}\equiv 0 \pmod p$ Implies $2^{n+1}|p-1$.

Problem 344

Let a, b be relatively prime integers and let p be a prime number.
Suppose that we have

$$a^{2^n}+b^{2^n}\equiv 0 \pmod p$$

for some positive integer n.
Then prove that 2^{n+1} divides $p-1$.

Proof.

Since a and b are relatively prime, at least one of them is relatively prime to p.

Without loss of generality let us assume that b and p are relatively prime.

Then the given equality becomes

$$\begin{aligned} a^{2^n} &\equiv -b^{2^n} \pmod p \\ \iff \left(\frac{a}{b}\right)^{2^n} &\equiv -1 \pmod p. \end{aligned}$$

Taking square of both sides we obtain

$$\left(\frac{a}{b}\right)^{2^{n+1}} \equiv 1 \pmod p.$$

Now, we can think of these congruences as equalities of elements in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $p-1$:

$$\left(\frac{a}{b}\right)^{2^n} = -1 \text{ and } \left(\frac{a}{b}\right)^{2^{n+1}} = 1 \text{ in } (\mathbb{Z}/p\mathbb{Z})^\times.$$

Note that the second equality yields that the order of the element a/b divides 2^{n+1}.

On the other hand, the first equality implies that any smaller power of 2 is not the order of a/b.

Thus, the order of the element a/b is exactly 2^{n+1}.

In general, the order of each element divides the order of the group.

(This is a consequence of Lagrange's theorem.)

Since the order of the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p-1$, it follows that 2^{n+1} divides $p-1$.

This completes the proof.

Abelian Normal subgroup, Quotient Group, and Automorphism Group

Problem 343

Let G be a finite group and let N be a normal abelian subgroup of G.
Let $\mathrm{Aut}(N)$ be the group of automorphisms of G.
Suppose that the orders of groups G/N and $\mathrm{Aut}(N)$ are relatively prime.
Then prove that N is contained in the center of G.

Outline of the proof

Here is the outline of the proof.

1. Define a group homomorphism $\psi : G \to \mathrm{Aut}(N)$ by $\psi(g)(n) = gng^{-1}$ for all $g \in G$ and $n \in N$.
   We need to check:
   - The map $\psi(g)$ is an automorphism of N for each $g \in G$.
   - The map ψ is in fact a group homomorphism from G to $\mathrm{Aut}(N)$.
2. The assumption that the orders of groups G/N and $\mathrm{Aut}(N)$ are relatively prime implies that $G = \ker(\psi)$.
3. This implies that N is in the center of G.

Proof.

We define a group homomorphism $\psi : G \to \mathrm{Aut}(N)$ as follows.
For each $g \in G$, we first define an automorphism $\psi(g)$ of N.
Define $\psi(g) : N \to N$ by

$$\psi(g)(n) = gng^{-1}.$$

Note that since N is a normal subgroup of G, the output $\psi(g)(n) = gng^{-1}$ actually lies in N.

We prove that so defined $\psi(g)$ is a group homomorphism from N to N for each fixed $g \in G$.
For $n_1, n_2 \in N$, we have

$$\begin{aligned} \psi(g)(n_1n_2) &= g(n_1n_2)g^{-1} && \text{by definition of } \psi(g) \\ &= gn_1g^{-1}gn_2g^{-1} && \text{by inserting } e = g^{-1}g \\ &= \psi(g)(n_1)\psi(g)(n_2) && \text{by definition of } \psi(g). \end{aligned}$$

It follows that $\psi(g)$ is a group homomorphism, and hence $\psi(g) \in \mathrm{Aut}(N)$.

We have defined a map $\psi : G \to \mathrm{Aut}(N)$. We now prove that ψ is a group homomorphism.
For any g_1, g_2, and $n \in N$, we have

$$\begin{aligned} \psi(g_1g_2)(n) &= (g_1g_2)n(g_1g_2)^{-1} \\ &= g_1g_2ng_2^{-1}g_1^{-1} \\ &= g_1\psi(g_2)(n)g_1^{-1} \\ &= \psi(g_1)\psi(g_2)(n). \end{aligned}$$

Thus, $\psi : G \to \mathrm{Aut}(N)$ is a group homomorphism.
By the first isomorphism theorem, we have

$$G/\ker(\psi) \cong \mathrm{im}(\psi) < \mathrm{Aut}(N). \tag{*}$$

Note that if $g \in N$, then $\psi(g)(n) = gng^{-1} = n$ since N is abelian. It yields that the subgroup N is in the kernel $\ker(\psi)$.

Then by the third isomorphism theorem, we have

$$G/\ker(\psi) \cong (G/N)/(\ker(\psi)/N). \tag{**}$$

It follows from (*) and (**) that the order of $G/\ker(\psi)$ divides both the order of $\mathrm{Aut}(N)$ and the order of G/N. Since the orders of the latter two groups are relatively prime by assumption, the order of $G/\ker(\psi)$ must be 1. Thus the quotient group is trivial and we have

$$G = \ker(\psi).$$

This means that for any $g \in G$, the automorphism $\psi(g)$ is the identity automorphism of N.
Thus, for any $g \in G$ and $n \in N$, we have $\psi(g)(n) = n$, and thus $gng^{-1} = n$.
As a result, the subgroup N is contained in the center of G.

Surjective Group Homomorphism to $\mathbb{Z}$ and Direct Product of Abelian Groups

Problem 342

Let G be an abelian group and let $f : G \to \mathbb{Z}$ be a surjective group homomorphism.
Prove that we have an isomorphism of groups:

$$G \cong \ker(f) \times \mathbb{Z}.$$

Proof.

Since $f : G \to \mathbb{Z}$ is surjective, there exists an element $a \in G$ such that

$$f(a) = 1.$$

Let $H = \langle a \rangle$ be the subgroup of G generated by the element a.
We show that $G \cong \ker(f) \times H$.
To prove this isomorphism, it suffices to prove the following three conditions.

1. The subgroups $\ker(f)$ and H are normal in G.
2. The intersection is trivial: $\ker(f) \cap H = \{e\}$, where e is the identity element of G.
3. Every element of G is a product of elements of $\ker(f)$ and H. That is, $G = \ker(f)H$.

The first condition follows immediately since the group G is abelian, hence all the subgroups of G are normal.

To check condition 2, let $x \in \ker(f) \cap H$.
Then $x = a^n$ for some $n \in \mathbb{Z}$ and we have

$$\begin{aligned} 0 &= f(x) && \text{since } x \in \ker(f) \\ &= f(a^n) \\ &= nf(a) && \text{since } f \text{ is a homomorphism.} \\ &= n && \text{since } f(a) = 1. \end{aligned}$$

Thus, as a result we have $x = a^0 = e$, and hence $\ker(f) \cap H = \{e\}$.
So condition 2 is met.

To prove condition 3, let b be an arbitrary element in G.
Let $n = f(b) \in \mathbb{Z}$. Then we have

$$f(b) = n = f(a^n),$$

and thus we have

$$f(ba^{-n}) = 0.$$

It follows that $ba^{-n} \in \ker(f)$.
So there exists $z \in \ker(f)$ such that $ba^{-n} = z$.
Therefore we have

$$b = za^n \in \ker(f)H.$$

This implies that $G = \ker(f)H$.

We have proved all the conditions, hence we obtain

$$G \cong \ker(f) \times H.$$

Since H is a cyclic group of infinite order, it is isomorphic to $\mathbb{Z}$.
(If H has a finite order, then there exists a positive integer n such that $a^n = e$. Then we have

$$0 = f(e) = f(a^n) = nf(a) = n,$$

and this contradicts the positivity of n.)
Combining these isomorphisms, we have

$$G \cong \ker(f) \times \mathbb{Z},$$

as required.

If Quotient G/H is Abelian Group and $H < K \triangleleft \quad G$, then G/K is Abelian

Problem 341

Let H and K be normal subgroups of a group G.
Suppose that $H < K$ and the quotient group G/H is abelian.
Then prove that G/K is also an abelian group.

Solution.

We will give two proofs.

Hint (The third isomorphism theorem)

Recall the third isomorphism theorem of groups:
Let G be a group and let H, K be normal subgroups of G with $H < K$.
Then we have G/K is a normal subgroup of G/H and we have an isomorphism

$$G/K \cong (G/H)/(G/K).$$

Proof 1 (Using third isomorphism theorem)

Since H, K are normal subgroups of G and $H < K$, the third isomorphism theorem yields that

$$G/K \cong (G/H)/(G/K).$$

Since the group G/H is abelian by assumption, and in general a quotient group of an abelian group is abelian, it follows $(G/H)/(G/K)$ is an abelian group.
Hence by the above isomorphism, the group G/K is also an abelian group.

Proof 2 (Using the commutator subgroup)

Here is another proof using the commutator subgroup $[G, G]$ of G.
Recall that for a subgroup N of G, the following two conditions are equivalent.

1. The subgroup N is normal and the G/N is an abelian.
2. The commutator subgroup $[G, G]$ is a subgroup of N.

For the proof of this fact, see the post "Commutator subgroup and abelian quotient group".
Now we prove the problem using this fact.
Since H is normal and the quotient G/H is an abelian group, the commutator subgroup $[G, G]$ is a subgroup of H by the fact (1 $\implies$ 2).
Then we have

$$[G, G] < H < K.$$

Hence $[G, G]$ is a subgroup of K, hence G/K is an abelian group by the fact again (2 $\implies$ 1).

Quotient Group of Abelian Group is Abelian

Problem 340

Let G be an abelian group and let N be a normal subgroup of G.
Then prove that the quotient group G/N is also an abelian group.

Proof.

Each element of G/N is a coset aN for some $a \in G$.
Let aN, bN be arbitrary elements of G/N, where $a, b \in G$.
Then we have

$$\begin{aligned}(aN)(bN) &= (ab)N \\ &= (ba)N && \text{since } G \text{ is abelian} \\ &= (bN)(aN).\end{aligned}$$

Here the first and the third equality is the definition of the group operation of G/N.

Remark

Since N is a normal subgroup of G, the set of left cosets G/H becomes a group with group operation

$$(aN)(bN) = (ab)N$$

for any $a, b \in G$.

Related Question.

As an application, try the following problem.

Problem.
Let H and K be normal subgroups of a group G. Suppose that $H < K$ and the quotient group G/H is abelian. Then prove that G/K is also an abelian group.

The proof of this problem is given in the post ↴

If quotient G/H is abelian group and $H < K \triangleleft G$, then G/K is abelian.

Special Linear Group is a Normal Subgroup of General Linear Group

Problem 332

Let $G = \mathrm{GL}(n, \mathbb{R})$ be the **general linear group** of degree n, that is, the group of all $n \times n$ invertible matrices.
Consider the subset of G defined by

$$\mathrm{SL}(n, \mathbb{R}) = \{X \in \mathrm{GL}(n, \mathbb{R}) \mid \det(X) = 1\}.$$

Prove that $\mathrm{SL}(n, \mathbb{R})$ is a subgroup of G. Furthermore, prove that $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of G.
The subgroup $\mathrm{SL}(n, \mathbb{R})$ is called **special linear group**

Hint.

We are going to use the following facts from linear algebra about the determinant of a matrix.
For any $n \times n$ matrices A, B, we have

$$\begin{aligned} \det(AB) &= \det(A)\det(B) \text{ and} \\ \det(A^{-1}) &= \det(A)^{-1} \end{aligned}$$

if A is invertible.

We give two proofs.

The first one proves that $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$ by directly verifying the defining property.

The second proof uses a fact about group homomorphism. If you are familiar with group homomorphism, the second proof is concise and nice.

Proof 1.

> The special linear group $\mathrm{SL}(n, \mathbb{R})$ is a subgroup.

Let $X, Y \in \mathrm{SL}(n, \mathbb{R})$ be arbitrary elements. We have

$$\det(X) = \det(Y) = 1$$

by definition of $\mathrm{SL}(n, \mathbb{R})$.

Then we obtain

$$\det(XY) = \det(X)\det(Y) = 1,$$

and hence XY is in $\mathrm{SL}(n, \mathbb{R})$.

Also, we have

$$\det(X^{-1}) = \det(X)^{-1} = 1,$$

and it follows that X^{-1} is in $\mathrm{SL}(n, \mathbb{R})$.

Thus, $\mathrm{SL}(n, \mathbb{R})$ is a subgroup of G.

The special linear group $\mathrm{SL}(n, \mathbb{R})$ is normal.

To prove that $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of G, let $X \in \mathrm{SL}(n, \mathbb{R})$ and let $P \in G$.

Then we have

$$\det(PXP^{-1}) = \det(P)\det(X)\det(P)^{-1} = \det(X) = 1,$$

and hence the conjugate PXP^{-1} is in $\mathrm{SL}(n, \mathbb{R})$.

Therefore, $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of G.

Proof 2.

Let $\mathbb{R}^*$ be the multiplicative group of nonzero real numbers.

Let $\phi : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$ be the map given by

$$\phi(X) = \det(X),$$

for each $X \in \mathrm{GL}(n, \mathbb{R})$.

Note that this is well-defined since $\det(X) \neq 0$ for $X \in \mathrm{GL}(n, \mathbb{R})$.

By the property of the determinant, we know that

$$\det(XY) = \det(X)\det(Y)$$

for any $X, Y \in \mathrm{GL}(n, \mathbb{R})$.

This implies that the map ϕ is a group homomorphism.

Then the kernel of ϕ is given by

$$\ker(\phi) = \{X \in \mathrm{GL}(n, \mathbb{R}) \mid \phi(X) = \det(X) = 1\} = \mathrm{SL}(n, \mathbb{R}).$$

As the kernel of the group homomorphism $\phi : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$ is alway a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$, we conclude that $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$.

If the Order of a Group is Even, then the Number of Elements of Order 2 is Odd

Problem 326

Prove that if G is a finite group of even order, then the number of elements of G of order 2 is odd.

Proof.

First observe that for $g \in G$,

$$g^2 = e \iff g = g^{-1},$$

where e is the identity element of G.

Thus, the identity element e and the elements of order 2 are the only elements of G that are equal to their own inverse elements.

Hence, each element x of order greater than 2 comes in pairs $\{x, x^{-1}\}$.

So we have

$$\begin{aligned} &G = \\ &\{e\} \cup \{ \text{ elements of order } 2 \} \cup \{x_1, x_1^{-1}, x_2, x_2^{-1}, \dots, x_k, x_k^{-1}\}, \end{aligned}$$

where x_i are elements of order greater than 2 for $i = 1, 2, \dots, k$.

As we noted above, the elements x_i, x_i^{-1} are distinct.

Thus the third set contains an even number of elements.

Therefore we have

$$\begin{aligned} &\underbrace{G}_{\text{even}} = \\ &\underbrace{\{e\}}_{\text{odd}} \cup \{ \text{ elements of order } 2 \} \cup \underbrace{\{x_1, x_1^{-1}, x_2, x_2^{-1}, \dots, x_k, x_k^{-1}\}}_{\text{even}} \end{aligned}$$

It follows that the number of elements of G of order 2 must be odd.

If the Order of a Group is Even, then it has a Non-Identity Element of Order 2

The consequence of the problem yields that the number of elements of order 2 is odd, in particular, it is not zero.

Hence we obtain:

If the order of a group is even, then it has a non-identity element of order 2.

A Group is Abelian if and only if Squaring is a Group Homomorphism

Problem 325

Let G be a group and define a map $f : G \to G$ by $f(a) = a^2$ for each $a \in G$.
Then prove that G is an abelian group if and only if the map f is a group homomorphism.

Proof.

($\implies$) If G is an abelian group, then f is a homomorphism.

Suppose that G is an abelian group. We prove that $f : G \to G, a \mapsto a^2$ is a group homomorphism.

Let a, b be arbitrary elements in G. Then we have

$$\begin{aligned} f(ab) &= (ab)^2 && (\text{ by definition of } f) \\ &= (ab)(ab) \\ &= a^2b^2 && (\text{ since } G \text{ is abelian}) \\ &= f(a)f(b) && (\text{ by definition of } f). \end{aligned}$$

Therefore, we obtain $f(ab) = f(a)f(b)$ for any $a, b \in G$.

Hence f is a group homomorphism from G to G.

($\Longleftarrow$) If f is a homomorphism, then G is an abelian group.

Suppose that $f : G \to G$ is a group homomorphism. We prove that G is an abelian group.

Let $a, b \in G$. We want to prove that $ab = ba$.

Since f is a group homomorphism, we have

$$f(ab) = f(a)f(b).$$

As a result we have

$$(ab)^2 = a^2b^2,$$

or equivalently

$$abab = aabb.$$

Multiplying this by a^{-1} on the left and by b^{-1} on the right, we obtain

$$ab = ba.$$

Since a and b are arbitrary, this implies that G is an abelian group.

Related Question.

Another problem about the relation between an abelian group and a group homomorphism is:

A group homomorphism and an abelian group.

The Additive Group $\mathbb{R}$ is Isomorphic to the Multiplicative Group $\mathbb{R}^+$ by Exponent Function

Problem 322

Let $\mathbb{R} = (\mathbb{R}, +)$ be the additive group of real numbers and let $\mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot)$ be the multiplicative group of real numbers.

(a) Prove that the map $\exp : \mathbb{R} \to \mathbb{R}^\times$ defined by

$$\exp(x) = e^x$$

is an injective group homomorphism.

(b) Prove that the additive group $\mathbb{R}$ is isomorphic to the multiplicative group

$$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}.$$

Proof.

(a) Prove $\exp : \mathbb{R} \to \mathbb{R}^\times$ is an injective group homomorphism.

We first prove that $\exp$ is a group homomorphism.

Let $x, y \in \mathbb{R}$. Then we have

$$\begin{aligned} \exp(x+y) &= e^{x+y} \\ &= e^x e^y \\ &= \exp(x)\exp(y). \end{aligned}$$

Thus, the map $\exp$ is a group homomorphism.

To show that $\exp$ is injective, suppose $\exp(x) = \exp(y)$ for $x, y \in \mathbb{R}$.
This implies that we have

$$e^x = e^y,$$

and thus $x = y$ by taking $\log$ of both sides.
Hence $\exp$ is an injective group homomorphism.

(b) Prove that the additive group $\mathbb{R}$ is isomorphic to the multiplicative group $\mathbb{R}^+$.

Since the image of $\exp : \mathbb{R} \to \mathbb{R}^\times$ consists of positive numbers, we can restrict the codomain of $\exp$ to $\mathbb{R}^+$, and we have the injective homomorphism

$$\exp : \mathbb{R} \to \mathbb{R}^+.$$

It suffices to show that this homomorphism is surjective.
For any $y \in \mathbb{R}^+$, we have $\log(y) \in \mathbb{R}$ and

$$\exp(\log(y)) = e^{\log(y)} = y.$$

Thus, $\exp : \mathbb{R} \to \mathbb{R}^+$ is a bijective homomorphism, hence isomorphism of groups.
This proves that the additive group $\mathbb{R}$ is isomorphic to the multiplicative group $\mathbb{R}^+$.

Note that the inverse homomorphism is given by

$$\log : \mathbb{R}^+ \to \mathbb{R}$$

sending $x \in \mathbb{R}^+$ to $\log(x)$.
This is a group homomorphism since we have for $x, y \in \mathbb{R}^+$,

$$\log(xy) = \log(x) + \log(y)$$

by the property of the log function.

Torsion Subgroup of an Abelian Group, Quotient is a Torsion-Free Abelian Group

Problem 307

Let A be an abelian group and let $T(A)$ denote the set of elements of A that have finite order.
(a) Prove that $T(A)$ is a subgroup of A.
(The subgroup $T(A)$ is called the **torsion subgroup** of the abelian group A and elements of $T(A)$ are called **torsion elements**.)
(b) Prove that the quotient group $G = A/T(A)$ is a **torsion-free abelian group**. That is, the only element of G that has finite order is the identity element.

Proof.

(a) $T(A)$ is a subgroup of A

We write the group operation multiplicatively.
Let $x, y \in T(A)$. Then x, y have finite order, hence there exists positive integers m, n such that

$x^m = e, y^n = e$, where e is the identity element of A. Then we have

$$\begin{aligned}(xy)^{mn} &= x^{mn}y^{mn} \qquad (\text{since } A \text{ is abelian}) \\ &= (x^m)^n (y^m)^n = e^m e^n = e.\end{aligned}$$

Therefore the element xy has also finite order, hence $xy \in T(A)$.

Also, we have

$$(x^{-1})^m = (x^m)^{-1} = e^{-1} = e.$$

Hence the inverse x^{-1} of x has finite order, hence $x^{-1} \in T(A)$.

Therefore, the subset $T(A)$ is closed under group operation and inverse, hence $T(A)$ is a subgroup of A.

(b) $A/T(A)$ is a torsion-free abelian group

Since A is an abelian group, the quotient $G = A/T(A)$ is also an abelian group.

For $a \in A$, let $\bar{a} = aT(A)$ be an element of $G = A/T(A)$. Suppose that $\bar{a}$ has finite order in G. We want to prove that $\bar{a} = \bar{e}$ the identity element of G.

Since $\bar{a}$ has finite order, there exists a positive integer n such that

$$\bar{a}^n = \bar{e}.$$

This implies that

$$a^n T(A) = T(A)$$

and thus $a^n \in T(A)$.

Since each element of $T(A)$ has finite order by definition, there exists a positive integer m such that $(a^n)^m = e$.

It follows from $a^{nm} = e$ that a has finite order, and thus $a \in T(A)$.

Therefore we have

$$\bar{a} = aT(A) = T(A) = \bar{e}.$$

We have proved that any element of $G = A/T(A)$ that has finite order is the identity, hence G is the torsion-free abelian subgroup of G.

If a Group G Satisfies $abc = cba$ then G is an Abelian Group

Problem 306

Let G be a group with identity element e.

Suppose that for any non identity elements a, b, c of G we have

$$abc = cba. \qquad (*)$$

Then prove that G is an abelian group.

Proof.

To show that G is an abelian group we need to show that

$$ab = ba$$

for any elements $a, b \in G$.

There are several cases we need to consider. Let us start with an easy case.

If $a = e$ or $b = e$, then we have $ab = ba$.

The next case to consider is $ab = e$. In this case, we have $b = a^{-1}$, and hence $ba = e = ab$.

The last case is $a \neq e, b \neq e, ab \neq e$.

Since $ab \neq e$, the inverse $(ab)^{-1}$ is not the identity as well.

We use the given relation $abc = cba$ with $c = (ab)^{-1}$. We have

$$\begin{aligned} e &= ab(ab)^{-1} \\ &= (ab)^{-1}ba \qquad \text{by the relation } (*) \end{aligned}$$

Multiplying this equality by ab on the left we obtain

$$ab = ba.$$

Therefore, for any elements $a, b \in G$ we have proved $ab = ba$, and thus G is an abelian group.

Non-Abelian Group of Order pq and its Sylow Subgroups

Problem 293

Let G be a non-abelian group of order pq, where p, q are prime numbers satisfying $q \equiv 1 \pmod{p}$.
Prove that a q-Sylow subgroup of G is normal and the number of p-Sylow subgroups are q.

Hint.

Use Sylow's theorem. To review Sylow's theorem, check out the post Sylow's Theorem (summary). Read the corollary there as well to understand the proof below.

Proof.

Let n_p, n_q be the number of p-Sylow subgroups and q-Sylow subgroups, respectively.

Then by Sylow's theorem, we have

$$n_p \equiv 1 \pmod{p}, \qquad n_p | q \tag{*}$$

and

$$n_q \equiv 1 \pmod{q}, \qquad n_q | p. \tag{**}$$

Since $q \equiv 1 \pmod{p}$, we have $q > p$. Thus n_q must be 1 from (**).

Hence, G has a unique q-Sylow subgroup, and it is normal.

From (*), the possibilities for n_p are either 1 or q.

We eliminate the possibility of $n_p = 1$ as follows.

If $n_p = 1$, then G has a unique p-Sylow subgroup, and hence it is normal.

Let P, Q be the unique normal p-Sylow subgroup and q-Sylow subgroup of G, respectively. Then P, Q are normal subgroup of order p and q, and hence $P \cap Q = \{e\}$, where e is the identity element of G.

Since the order $|PQ| = pq = |G|$, these conditions imply that we have

$$G \cong P \times Q.$$

Since P and Q are groups of prime order, hence it is cyclic, in particular abelian.

The direct product of abelian group is abelian, hence G is abelian.

This is a contradiction.

Thus, we must have $n_p = q$.

The Order of ab and ba in a Group are the Same

Problem 291

Let G be a finite group. Let a, b be elements of G.
Prove that the order of ab is equal to the order of ba.
(Of course do not assume that G is an abelian group.)

Proof.

Let n and m be the order of ab and ba, respectively. That is,

$$(ab)^n = e, (ba)^m = e,$$

where e is the identity element of G.

We compute

$$\begin{aligned} e = (ab)^n &= \underbrace{(ab) \cdot (ab) \cdot (ab) \cdots (ab)}_{n \text{ times}} \\ &= a \underbrace{\cdot (ba)(ba) \cdot (ba) \cdots (ba)}_{n-1 \text{ times}} b \\ &= a(ba)^{n-1}b. \end{aligned}$$

From this, we obtain

$$(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1},$$

and thus we have

$$(ba)^n = e.$$

Therefore the order m of ba divides n.

Similarly, we see that n divides m, and hence $m = n$.

Thus the orders of ab and ba are the same.

A Simple Abelian Group if and only if the Order is a Prime Number

Problem 290

Let G be a group. (Do not assume that G is a finite group.)
Prove that G is a simple abelian group if and only if the order of G is a prime number.

Definition.

A group G is called **simple** if G is a nontrivial group and the only normal subgroups of G is either the trivial group or G itself.

Proof.

($\implies$) If G is a simple abelian group, then the order of G is prime.

Suppose that G is a simple abelian group. Then G is a nontrivial group by definition.

We first show that G is a finite group.

Let $g \in G$ be a nonidentity element of G. Then the group $\langle g \rangle$ generated by g is a subgroup of G. Since G is an abelian group, every subgroup is a normal subgroup.

Since G is simple, we must have $\langle g \rangle = G$. If the order of g is not finite, then $\langle g^2 \rangle$ is a proper normal subgroup of $\langle g \rangle = G$, which is impossible since G is simple.

Thus the order of g is finite, and hence $G = \langle g \rangle$ is a finite group.

Let p be the order of g (hence the order of G).

Seeking a contradiction, assume that $p = mn$ is a composite number with integers $m > 1$, $n > 1$. Then $\langle g^m \rangle$ is a proper normal subgroup of G. This is a contradiction since G is simple.

Thus p must be a prime number.

Therefore, the order of G is a prime number.

($\Leftarrow$) If the order of G is prime, then G is a simple abelian group.

Let us now suppose that the order of G is a prime.

Let $g \in G$ be a nonidentity element. Then the order of the subgroup $\langle g \rangle$ must be a divisor of the order of G, hence it must be p.

Therefore we have $G = \langle g \rangle$, and G is a cyclic group and in particular an abelian group.

Since any normal subgroup H of G has order 1 or p, H must be either trivial $\{e\}$ or G itself. Hence G is simple.

Thus, G is a simple abelian group.

A Group of Order 20 is Solvable

Problem 286

Prove that a group of order 20 is solvable.

Hint.

Show that a group of order 20 has a unique normal 5-Sylow subgroup by Sylow's theorem.

See the post summary of Sylow's Theorem to review Sylow's theorem.

Proof.

Let G be a group of order 20. The prime factorization of 20 is $20 = 2^2 \cdot 5$.

Let n_5 be the number of 5-Sylow subgroups of G.

By Sylow's theorem, we have

$$n_5 \equiv 1 \pmod 5 \text{ and } n_5 | 4.$$

It follows from these constraints that we have $n_5 = 1$.

Let P be the unique 5-Sylow subgroup of G.

The subgroup P is normal in G as it is the unique 5-Sylow subgroup.

Then consider the subnormal series

$$G \triangleright P \triangleright \{e\},$$

where e is the identity element of G.

Then the factor groups G/P, $P/\{e\}$ have order 4 and 5 respectively, and hence these are cyclic groups and in particular abelian.

Therefore the group G of order 20 has a subnormal series whose factor groups are abelian groups, and thus G is a solvable group.

The Center of the Heisenberg Group Over a Field F is Isomorphic to the Additive Group F

Problem 283

Let F be a field and let

$$H(F) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \quad \middle| \quad \text{for any} a, b, c \in F \right\}$$

be the **Heisenberg group** over F.
(The group operation of the Heisenberg group is matrix multiplication.)
Determine which matrices lie in the center of $H(F)$ and prove that the center $Z\big(H(F)\big)$ is isomorphic to the additive group F.

Proof.

Suppose that the matrix

$$M = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$$

is in the center of the Heisenberg group $H(F)$.

Let

$$A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

be an arbitrary element in $H(F)$.

Since M is in the center, we have $AM = MA$, that is,

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}.$$

Computing the products, we obtain

$$\begin{bmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & b+cx+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix}.$$

Comparing $(1,3)$-entries, we have

$$az = cx.$$

This equality must be true for any $a, c \in F$.

We claim that $x = z = 0$.

Taking $a = 0, c = 1$ (Note that since F is a field, $0, 1 \in F$),

we have $x = 0$. Also if $a = 1, c = 0$, then we have $z = 0$.

Thus $x = z = 0$ and the matrix M becomes

$$M = \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It is clear from the computation of $AM = MA$ that this matrix is in the center for any y.

Therefore we have determined the center of the Heisenberg group:

$$Z\big(H(F)\big) = \left\{ \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \middle| \quad \text{for any } y \in F \right\}.$$

To prove that the center $Z\big(H(F)\big)$ is isomorphic to the additive group F, consider the map

$$\phi : Z\big(H(F)\big) \to F$$

which sends

$$M = \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in Z\big(H(F)\big)$$

to $y \in F$.

We prove that the map ϕ is a group isomorphism.

Let

$$M = \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, M' = \begin{bmatrix} 1 & 0 & y' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

be any two elements in the center $Z\big(H(F)\big)$.

Then we have

$$MM' = \begin{bmatrix} 1 & 0 & y+y' \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Therefore we have

$$\phi(MM') = y + y' = \phi(M) + \phi(M').$$

Thus, ϕ is a group homomorphism.

From the definition of ϕ, it is easy to see that the homomorphism ϕ is injective and surjective, and hence ϕ is a group isomorphism.

Therefore, the center $Z\big(H(F)\big)$ of the Heisenberg group is isomorphic to the additive group of F.

Related Question.

The inverse element of the matrix

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$$

is given by

$$\begin{bmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix}.$$

For a proof, see the post The inverse matrix of an upper triangular matrix with variables.

Sylow Subgroups of a Group of Order 33 is Normal Subgroups

Problem 278

Prove that any p-Sylow subgroup of a group G of order 33 is a normal subgroup of G.

Hint.

We use Sylow's theorem. Review the basic terminologies and Sylow's theorem.

Recall that if there is only one p-Sylow subgroup P of G for a fixed prime p, then P is a normal subgroup of G.

Then use Sylow's theorem show that the number of p-Sylow subgroups is 1 for $p=3, 11$.

Proof.

Since the order of G is $33=3\cdot 11$, we consider p-Sylow subgroups of G for $p=3, 11$.

Let n_p be the number of p-Sylow subgroups of G. It suffices to show that $n_p=1$ for $p=3, 11$. In fact, by Sylow's theorem any two p-Sylow subgroups are conjugate. If there is only one p-Sylow subgroup P, then $g^{-1}Pg=P$ for any $g\in G$, hence P is normal.

By Sylow's theorem, the number of p-Sylow subgroups of G satisfies

$$n_p \equiv 1 \pmod p$$

and $n_3|11$ and $n_{11}|3$.

From these two constraints, we see that we must have $n_3=n_{11}=1$.

Therefore, for each p, there is a unique p-Sylow subgroup of G.

By the consideration above, we conclude that any p-Sylow subgroup of G is a normal subgroup of G.

Eckmann–Hilton Argument: Group Operation is a Group Homomorphism

Problem 268

Let G be a group with the identity element e and suppose that we have a group homomorphism ϕ from the direct product $G\times G$ to G satisfying

$$\phi(e,g)=g \text{ and } \phi(g,e)=g, \tag{*}$$

for any $g\in G$.

Let $\mu : G\times G \to G$ be a map defined by

$$\mu(g,h)=gh.$$

(That is, μ is the group operation on G.)

Then prove that $\phi=\mu$.

Also prove that the group G is abelian.

Proof.

$\phi = \mu$

Since ϕ is a group homomorphism, for any $g, g' \in G$ and $h, h' \in H$, we have

$$\phi((g,h)(g',h')) = \phi(g,h)\phi(g',h').$$

The left hand side is equal to

$$\phi(gg', hh'),$$

and thus we have

$$\phi(gg', hh') = \phi(g,h)\phi(g',h').$$

Setting $g' = h = e$, we have

$$\begin{aligned} \phi(g,h') &= \phi(g,e)\phi(e,h') \\ &= gh' && \text{by } (*) \\ &= \mu(g,h'). \end{aligned}$$

Since this equality holds for any $g \in G$ and $h' \in H$, we obtain

$$\phi = \mu$$

as required.

G is an abelian group

Now we prove that G is an abelian group.

Let $g, h \in G$ be any two elements.

Then we have

$$\begin{aligned} gh &= \phi(e,g)\phi(h,e) && \text{by } (*) \\ &= \phi(eh, ge) && \text{since } \phi \text{ is a homomorphism} \\ &= \phi(h,g) \\ &= \mu(h,g) = hg. \end{aligned}$$

Thus we have proved that $gh = hg$ for any $g, h \in G$. Thus the group G is abelian.

Combined version

Here is a combined version of the proofs of the two claims at once.

We have for any $g, h \in G$,

$$
\begin{aligned}
&\mu(g,h)\\
&= gh = \phi(e,g)\phi(h,e) && \text{by } (*)\\
&= \phi((e,g)(h,e)) && \text{since } \phi \text{ is a homomorphism}\\
&= \phi(eh, ge)\\
&= \phi(h,g)\\
&= \phi(he, eg) = \phi((h,e)(e,g))\\
&= \phi(h,e)\phi(e,g) && \text{since } \phi \text{ is a homomorphism}\\
&= hg \qquad \text{by } (*)\\
&= \mu(h,g)
\end{aligned}
$$

From these equalities, we see that $\phi = \mu$ and G is an abelian group.

Remark.

This argument is called the **Eckmann–Hilton argument**.

Equivalent Definitions of Characteristic Subgroups. Center is Characteristic.

Problem 246

Let H be a subgroup of a group G. We call H **characteristic** in G if for any automorphism $\sigma \in \mathrm{Aut}(G)$ of G, we have $\sigma(H) = H$.
(a) Prove that if $\sigma(H) \subset H$ for all $\sigma \in \mathrm{Aut}(G)$, then H is characteristic in G.
(b) Prove that the center $Z(G)$ of G is characteristic in G.

Definition

Recall that an automorphism σ of a group G is a group isomorphism from G to itself.

The set of all automorphism of G is denoted by $\mathrm{Aut}(G)$.

Proof.

(a) If $\sigma(H) \subset H$ for all $\sigma \in \mathrm{Aut}(G)$, then H is characteristic in G

Since σ is an automorphism, the inverse σ^{-1} is also an automorphism of G.

Hence, we have

$$\sigma^{-1}(H) \subset H$$

by the assumption.

Applying σ, we have

$$\sigma\sigma^{-1}(H) \subset \sigma(H).$$

Then we obtain

$$H = \sigma\sigma^{-1}(H) \subset \sigma(H) \subset H.$$

Since the both ends are H, the inclusion is in fact the equality.

Thus, we obtain

$$\sigma(H) = H,$$

and the subgroup H is characteristic in the group G.

(b) The center $Z(G)$ of G is characteristic in G

By part (a), it suffices to prove that $\sigma(Z(G)) \subset Z(G)$ for every automorphism $\sigma \in \mathrm{Aut}(G)$ of G.

Let $x \in \sigma(Z(G))$. Then there exists $y \in Z(G)$ such that $x = \sigma(y)$.

To show that $x \in Z(G)$, consider an arbitrary $g \in G$.

Then since σ is an automorphism, we have $G = \sigma(G)$.

Thus there exists g' such that $g = \sigma(g')$.

We have

$$\begin{aligned} xg &= \sigma(y)\sigma(g') \\ &= \sigma(yg') && (\text{since } \sigma \text{ is a homomorphism}) \\ &= \sigma(g'y) && (\text{since } y \in Z(G)) \\ &= \sigma(g')\sigma(y) && (\text{since } \sigma \text{ is a homomorphism}) \\ &= gx. \end{aligned}$$

Since this is true for all $g \in G$, it follows that $x \in Z(G)$, and thus

$$\sigma(Z(G)) \subset Z(G).$$

This completes the proof.

Comment.

In some textbook, a subgroup H of G is said to be characteristic in G if $\sigma(H) \subset H$ for all $\sigma \in \mathrm{Aut}(G)$.

Problem (a) implies that our definition of characteristic and this alternative definition are in fact equivalent.

Related Question.

Read the post Basic properties of characteristic groups for more problems about characteristic subgroups.

Group of Order pq Has a Normal Sylow Subgroup and Solvable

Problem 245

Let p, q be prime numbers such that $p > q$.

If a group G has order pq, then show the followings.

(a) The group G has a normal Sylow p-subgroup.

(b) The group G is solvable.

Definition/Hint

For (a), apply Sylow's theorem. To review Sylow's theorem, read the post Sylow's Theorem (summary).

In particular, we will use Sylow's theorem (3) and (4), and its corollary in the proof below.

For (b), recall that a group G is solvable if G has a subnormal series

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G$$

such that the factor groups G_i/G_{i-1} are all abelian groups for $i = 1, 2, \dots, n$.

Proof.

(a) The group G has a normal Sylow p-subgroup

By Sylow's theorem, the number n_p of Sylow p-subgroups of G satisfies $n_p \equiv 1 \pmod{p}$ and n_p divides q.

The only such number is $n_p = 1$.

Thus G has the unique Sylow p-subgroup P of order p.

Since P is the unique Sylow p-subgroup, it is a normal subgroup of G.

(b) The group G is solvable

Let P be the normal Sylow subgroup of G obtained in (a).

Then we have the following subnormal series

$$\{e\} \triangleleft P \triangleleft G,$$

where e is the identity element of G.

The factor groups are G/P and $P/\{e\} \cong P$.

The order of the group P is the prime p, and hence P is an abelian group.

The order $|G/P| = |G|/|P| = pq/q = q$ is also a prime, and thus G/P is an abelian group.

Thus the factor groups are abelian. Thus G is a solvable group.

Related Question.

The similar problems are

- Group of order 18 is solvable
- A group of order pqr contains a normal subgroup of order either p, q, or r

Pullback Group of Two Group Homomorphisms into a Group

Problem 244

Let G_1, G_1, and H be groups. Let $f_1 : G_1 \to H$ and $f_2 : G_2 \to H$ be group homomorphisms.
Define the subset M of $G_1 \times G_2$ to be

$$M = \{(a_1, a_2) \in G_1 \times G_2 \mid f_1(a_1) = f_2(a_2)\}.$$

Prove that M is a subgroup of $G_1 \times G_2$.

Proof.

M is closed under the group operation

Suppose that $(a_1, a_2), (b_1, b_2) \in M$.

By definition, we have

$$f_1(a_1) = f_2(a_2) \text{ and } f_1(b_1) = f_2(b_2). \tag{*}$$

The product of (a_1, a_2) and (b_1, b_2) is

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2).$$

We want to prove that this is in M. To see this, note that we have

$$\begin{aligned} f_1(a_1 b_1) &= f_1(a_1) f_1(b_1) && (f_1 \text{ is a homomorphism}) \\ &= f_2(a_2) f_2(b_2) && (\text{by } (*)) \\ &= f_2(a_2 b_2) && (f_2 \text{ is a homomorphism}). \end{aligned}$$

Therefore we have obtained

$$f_1(a_1 b_1) = f_2(a_2 b_2),$$

and the product $(a_1 b_1, a_2 b_2)$ is in M by definition.

M is closed under inverses

We next prove that if $(a_1, a_2) \in M$ then the inverse

$$(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$$

is also in M.
Since $(a_1, a_2) \in M$, we have

$$f_1(a_1) = f_2(a_2). \tag{**}$$

Then we have

$$\begin{aligned} f_1(a_1^{-1}) &= (f_1(a_1))^{-1} && (f_1 \text{ is a homomorphism}) \\ &= (f_2(a_2))^{-1} && (\text{by } (**)) \\ &= f_2(a_2^{-1}) && (f_2 \text{ is a homomorphism}). \end{aligned}$$

Thus by definition the inverse (a_1^{-1}, a_2^{-1}) is in M.
Since M is closed under the group operation and inverses, it is a subgroup of $G_1 \times G_2$.

Comment.

In category theory, the subgroup M in the problem is called a **pullback** of homomorphisms $f_1 : G_1 \to H$ and $f_2 : G_2 \to H$.

A Group Homomorphism is Injective if and only if Monic

Problem 243

Let $f : G \to G'$ be a group homomorphism. We say that f is **monic** whenever we have $fg_1 = fg_2$, where $g_1 : K \to G$ and $g_2 : K \to G$ are group homomorphisms for some group K, we have $g_1 = g_2$.
Then prove that a group homomorphism $f : G \to G'$ is injective if and only if it is monic.

Proof.

($\Longrightarrow$) Injective implies monic

Suppose that $f : G \to G'$ is an injective group homomorphism.
We show that f is monic.
So suppose that we have $fg_1 = fg_2$, where $g_1 : K \to G$ and $g_2 : K \to G$ are group homomorphisms for some group K.
Then for any $x \in K$, we have

$$f(g_1(x)) = f(g_2(x)).$$

Since f is injective, it follows that

$$g_1(x) = g_2(x)$$

for any $x \in K$, and thus we obtain $g_1 = g_2$. Thus f is monic.

($\Longleftarrow$) Monic implies injective

For the opposite implication, we prove the contrapositive statement. Namely, we prove that if f is not injective, then f is not monic.

Suppose that f is not injective. Then the kernel $\ker(f)$ is a non-trivial subgroup of G.

We define the group homomorphism $g_1 : \ker(f) \to G$ to be the identity map on $\ker(f)$. That is $g_1(x) = x$ for all $x \in \ker(f)$.

Also we define the group homomorphism $g_2 : \ker(f) \to G$ by the formula $g_2(x) = e$ for all $x \in \ker(f)$, where e is the identity element of G.

Since $\ker(f)$ is a nontrivial group, these two homomorphisms are distinct: $g_1 \neq g_2$.

However, we have

$$fg_1 = fg_2.$$

In fact, we have for $x \in \ker(f)$

$$fg_1(x) = f(x) = e',$$

where e' is the identity element of G',

and

$$fg_2(x) = f(e) = e'.$$

Thus, by definition, the homomorphism f is not monic as required to complete the proof.

No Finite Abelian Group is Divisible

Problem 240

A nontrivial abelian group A is called **divisible** if for each element $a \in A$ and each nonzero integer k, there is an element $x \in A$ such that $x^k = a$.

(Here the group operation of A is written multiplicatively. In additive notation, the equation is written as $kx = a$.) That is, A is divisible if each element has a k-th root in A.

(a) Prove that the additive group of rational numbers $\mathbb{Q}$ is divisible.

(b) Prove that no finite abelian group is divisible.

Proof.

(a) The additive group of rational numbers $\mathbb{Q}$ is divisible.

We know that $\mathbb{Q}$ is a nontrivial abelian group.

Let $a \in Q$ and k be a nonzero integer.

Since $\mathbb{Q}$ is an additive group, we are seeking $x \in \mathbb{Q}$ such that

$$kx = a.$$

Since k is a nonzero integer, we have a solution $x = a/k \in \mathbb{Q}$.

Thus $\mathbb{Q}$ is divisible.

(b) No finite abelian group id divisible.

Let G be a finite abelian group of order $|G| = n$.

If G is trivial, that is, $n = 1$, then by definition, G is not divisible.

So let us assume that G is nontrivial.

We claim that G is not divisible since there is no n-th root of a nonidentity element of G.

Let $a \in G$ be a nonidentity element of G.

(Such an element exists because G is nontrivial.)

If there is $x \in G$ such that

$$x^n = a,$$

then by Lagrange's theorem we have $x^n = e$, the identity element of G.

This implies that $a = e$, and this contradicts our choice of a.

Thus G is not divisible.

Subgroup of Finite Index Contains a Normal Subgroup of Finite Index

Problem 232

Let G be a group and let H be a subgroup of finite index. Then show that there exists a normal subgroup N of G such that N is of finite index in G and $N \subset H$.

Proof.

The group G acts on the set of left cosets G/H by left multiplication.

Hence it induces the permutation representation $\rho : G \to S_n$, where $n = |G : H|$.

(Note that a permutation representation is a group homomorphism.)

Let $N = \ker \rho$ be the kernel of the homomorphism ρ. Then $N \lhd G$.

By the first isomorphism theorem, the quotient group G/N is isomorphic to a subgroup of S_n. In particular, G/N is a finite group, hence the index $[G : N]$ is finite.

Finally, we show that $N \subset H$.

For any $x \in N = \ker \rho$, we have $x(gH) = gH$ for any $g \in G$.

In particular we have $xH = H$, hence $x \in H$.

Subgroup Containing All p-Sylow Subgroups of a Group

Problem 227

Suppose that G is a finite group of order $p^a n$, where p is a prime number and p does not divide n.
Let N be a normal subgroup of G such that the index $|G : N|$ is relatively prime to p.
Then show that N contains all p-Sylow subgroups of G.

Hint.

We give two proof.

The first one uses Sylow's theorem. The second one consider indexes of groups.

To review Sylow's theorem, read the post Sylow's Theorem (summary)

Proof 1.

Since p does not divide the index $|G : N|$, the order of N is of the form

$$|N| = p^a m, \text{ where } m|n.$$

By Sylow's theorem, the group N has a p-Sylow subgroup P.

Since the order of P is p^a and P is a subgroup of G, it is also a Sylow subgroup of G.

Let P' be any p-Sylow subgroup of G. Then by Sylow's theorem, two p-Sylow subgroups are conjugate.

Thus there exists $g \in G$ such that

$$g^{-1} P g = P'.$$

Then since N is normal in G, we have

$$P' = g^{-1}Pg < g^{-1}Ng = N$$

and P' is a subgroup of N.

Proof 2.

Let P be any p-Sylow subgroup of G. Seeking a contradiction, assume that $P \not\subset N$. Thus there exists $x \in P \setminus N$.

Let $H = \langle x \rangle$ be a subgroup of G generated by x.

Since the order of x is a power of p, the order of H is a power of p.

Since $N \triangleleft G$, by the second isomorphism theorem, we have

$$|HN : N| = |H : H \cap N|. \qquad (*)$$

Also, the chain of subgroups $N < HN < G$ implies

$$|G : N| = |G : HN||HN : N|.$$

Combining this with (*), we obtain

$$|G : N| = |G : HN||H : H \cap N|.$$

Since $H \not\subset N$, $|H : H \cap N|$ is a positive power of p. However, this contradicts that p does not divide $|G : N|$. Hence P must be contained in N.

If a Sylow Subgroup is Normal in a Normal Subgroup, it is a Normal Subgroup

Problem 226

Let G be a finite group. Suppose that p is a prime number that divides the order of G.
Let N be a normal subgroup of G and let P be a p-Sylow subgroup of G.
Show that if P is normal in N, then P is a normal subgroup of G.

Hint.

It follows from Sylow's theorem that if Q_1 and Q_2 are both p-Sylow subgroups of a group H, then they are conjugate.

Namely, there exists $h \in H$ such that $h^{-1}Q_1h = Q_2$.

For more details, check out the post Sylow's theorem (summary)

To prove the problem, let $g \in G$ be any element and try to show that both P and $g^{-1}Pg$ are p-Sylow subgroups of N.

Then use the fact above with $Q_1 = P$, $Q_2 = g^{-1}Pg$, and $H = N$.

We use the following notations: $A < B$ means that A is a subgroup of a group B, and $A \triangleleft B$ denotes that A is a normal subgroup of B.

Proof.

For any $g \in G$, since $P < N$ and $N \triangleleft G$, we have

$$g^{-1}Pg < g^{-1}Ng = N.$$

Thus $g^{-1}Pg$ is a p-Sylow subgroup in N. In general, any two p-Sylow subgroups in a group are conjugate by Sylow's theorem. Since P and $g^{-1}Pg$ are both p-Sylow subgroups in N, there exists $n \in N$ such that

$$n^{-1}Pn = g^{-1}Pg.$$

Since $n \in N$ and P is normal in N, we have $n^{-1}Pn = P$. Hence we obtain

$$P = g^{-1}Pg.$$

Since $g \in G$ is arbitrary, this implies that P is a normal subgroup in G.

Cyclic Group if and only if There Exists a Surjective Group Homomorphism From $\mathbb{Z}$

Problem 225

Show that a group G is cyclic if and only if there exists a surjective group homomorphism from the additive group $\mathbb{Z}$ of integers to the group G.

Proof.

($\Longrightarrow$): If G is cyclic, then there exists a surjective homomorhpism from $\mathbb{Z}$

Suppose that G is a cyclic group. Then we have

$$G = \langle a \rangle$$

for some $a \in G$. Namely, G is generated by a. Define a map $f : Z \to G$ by sending $n \in \mathbb{Z}$ to $a^n \in G$.
Since any element of G is of the form a^n for some $n \in Z$, the map f is surjective.
It remains to prove that f is a group homomorphism.
For any $m, n \in \mathbb{Z}$, we have

$$f(m+n) = a^{m+n} = a^m a^n = f(m)f(n).$$

Thus f is a group homomorphism.

($\Longleftarrow$): If there exists a surjective homomorphism from $\mathbb{Z}$, then G is cyclic

On the other hand, suppose that there exists a surjective group homomorphism $f : \mathbb{Z} \to G$. Define

$$a = f(1).$$

Then we claim that G is generated by a, that is, $G = \langle a \rangle$.
Since $a = f(1) \in G$, we have $\langle a \rangle \subset G$.
On the other hand, for any $g \in G$ there exists $n \in Z$ such that $f(n) = g$ since f is surjective.
Since f is a group homomorphism, we have

$$\begin{aligned} g &= f(n) \\ &= f(\underbrace{1 + \cdots + 1}_{n \text{ times}}) \\ &= \underbrace{f(1) + \cdots + f(1)}_{n \text{ times}} = nf(1) \\ &= na \in \langle a \rangle. \end{aligned}$$

Therefore we have $G \subset \langle a \rangle$, hence $G = \langle a \rangle$ and G is a cyclic group.

Group of p-Power Roots of 1 is Isomorphic to a Proper Quotient of Itself

Problem 221

Let p be a prime number. Let

$$G = \{z \in \mathbb{C} \mid z^{p^n} = 1\}$$

be the group of p-power roots of 1 in $\mathbb{C}$.
Show that the map $\Psi : G \to G$ mapping z to z^p is a surjective homomorphism.
Also deduce from this that G is isomorphic to a proper quotient of G itself.

Proof.

$\Psi : G \to G$ is a group homomorphism

We first show that $\Psi : G \to G$ is a group homomorphism.
To see this, let $z, w \in G$. Then we have

$$\Psi(zw) = (zw)^p = z^p w^p = \Psi(z)\Psi(w).$$

The second equality follows since G is an abelian group.
Thus Ψ is a group homomorphism.

Ψ is surjective

To prove that Ψ is surjective, let z be an arbitrary element in G.
Then there exists nonnegative integer n such that $z^n = 1$.
Let $w \in \mathbb{C}$ be a p-th root of z, that is, w is a solution of the equation $x^p - z = 0$.
(By the fundamental theorem of algebra, such a solution exists.)
We check that $w \in G$ as follows.
We have

$$w^{p^{n+1}} = (w^p)^{p^n} = z^{p^n} = 1.$$

Therefore w is a p-power root of 1, hence $w \in G$.
It follows from

$$\Psi(w) = w^p = z$$

that Ψ is a surjective homomorphism.

G is isomorphic to the proper quotient

Now by the first isomorphism theorem, we have an isomorphism

$$G/\ker(\Psi) \cong \mathrm{im}(\Psi) = G.$$

Since we have

$$\ker(\Psi) = \{z \in G \mid z^p = 1\},$$

the subgroup $\ker(\Psi)$ consists of p-th roots of unity.
There are p p-th roots of unity in $\mathbb{C}$ (and hence in G), and hence the kernel $\ker(\Psi)$ is a nontrivial subgroup of G.
Hence $G/\ker(\Psi)$ is a proper quotient, and thus G is isomorphic to the proper quotient $G/\ker(\Psi)$.

Use Lagrange's Theorem to Prove Fermat's Little Theorem

Problem 219

Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is a prime number then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

Before the proof, let us recall Lagrange's Theorem.

Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then the order $|H|$ of H divides the order $|G|$ of G.

Proof.

If $a = 0$, then we clearly have $a^p \equiv a \pmod{p}$.

So we assume that $a \neq 0$.

Then $\bar{a} = a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Let H be a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ generated by $\bar{a}$.

Then the order of the subgroup H is the order of the element $\bar{a}$.

By Lagrange's Theorem, the order $|H|$ divides the order of the group $(\mathbb{Z}/p\mathbb{Z})^\times$, which is $p-1$.

So we write $p - 1 = |H|m$ for some $m \in \mathbb{Z}$.

Therefore, we have

$$\bar{a}^{p-1} = \bar{a}^{|H|m} = \bar{1}^m = \bar{1}.$$

(Note that this is a computation in $(\mathbb{Z}/p\mathbb{Z})^\times$.)

This implies that we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Multiplying by a, we obtain

$$a^p \equiv a \pmod{p},$$

and hence Fermat's Little Theorem is proved.

If Every Nonidentity Element of a Group has Order 2, then it's an Abelian Group

Problem 212

Let G be a group. Suppose that the order of nonidentity element of G is 2.
Then show that G is an abelian group.

Proof.

Let x and y be elements of G. Then we have

$$1 = (xy)^2 = (xy)(xy).$$

Multiplying the equality by yx from the right, we obtain

$$\begin{aligned} yx &= (xy)(xy)(yx) \\ &= xyxy^2x \\ &= xyx^2 \quad (\text{since } y^2 = 1) \\ &= xy \quad (\text{since } x^2 = 1). \end{aligned}$$

Thus we obtain $xy = yx$ for any elements $x, y \in G$. Thus the group G is an abelian group.

Group Homomorphism, Conjugate, Center, and Abelian group

Problem 209

Let G be a group. We fix an element x of G and define a map

$$\Psi_x : G \to G$$

by mapping $g \in G$ to $xgx^{-1} \in G$.
Then prove the followings.
(a) The map Ψ_x is a group homomorphism.
(b) The map $\Psi_x = \mathrm{id}$ if and only if $x \in Z(G)$, where $Z(G)$ is the center of the group G.
(c) The map $\Psi_y = \mathrm{id}$ for all $y \in G$ if and only if G is an abelian group.

Proof.

(a) The map Ψ_x is a group homomorphism

For any elements $g, h \in G$, we have

$$\Psi_x(gh) = x(gh)x^{-1} \overset{(*)}{=} xgx^{-1}xhx^{-1} = \Psi_x(g)\Psi_x(h),$$

where we inserted the identity element $e = x^{-1}x$ between g and h to obtain (*).
Hence Ψ_x is a group homomorphism.

(b) The map $\Psi_x = \mathrm{id}$ if and only if $x \in Z(G)$

$(\implies)$ Suppose that $\Psi_x = \mathrm{id}$. Then for any $g \in G$, we have

$$\Psi_x(g) = \mathrm{id}(g)$$

and thus we have

$$xgx^{-1} = g.$$

This implies that we have $xg = gx$ for all $g \in G$, and hence $x \in Z(G)$.

$(\impliedby)$ On the other hand, if x is in the center $Z(G)$, then we have

$$\Psi_x(g) = xgx^{-1} = xx^{-1}g = g$$

for any $g \in G$, where the second equality follows since $x \in Z(G)$.
This yields that $\Psi_x = \mathrm{id}$.

(c) The map $\Psi_y = \mathrm{id}$ for all $y \in G$ if and only if G is an abelian group

$(\implies)$ Suppose that the map $\Psi_y = \mathrm{id}$ for all $y \in G$. Then by part (b), we have $y \in Z(G)$ for all $y \in G$.
This means that we have $G = Z(G)$, and hence G is an abelian group.

($\Longleftarrow$) Now suppose that G is an abelian group. Then for any $y \in G$ we have

$$\Psi_y(g) = ygy^{-1} = yy^{-1}g = g = \mathrm{id}(g)$$

for any $g \in G$, where the second equality follows since G is an abelian group.
Thus we have $\Psi_y = \mathrm{id}$ for any $y \in G$.

Group Homomorphism, Preimage, and Product of Groups

Problem 208

Let G, G' be groups and let $f : G \to G'$ be a group homomorphism.
Put $N = \ker(f)$. Then show that we have

$$f^{-1}(f(H)) = HN.$$

Proof.

($\subset$) Take an arbitrary element $g \in f^{-1}(f(H))$. Then we have $f(g) \in f(H)$.
It follows that there exists $h \in H$ such that $f(g) = f(h)$.
Since f is a group homomorphism, we obtain

$$f(h^{-1}g) = e',$$

where e' is the identity element of the group G'.
This implies that $h^{-1}g \in \ker(f) = N$, hence we have

$$g \in hN \subset HN.$$

Therefore we have $f^{-1}(f(H)) \subset HN$.

($\supset$) On the other hand, let $g \in HN$ be an arbitrary element.
Then we can write $g = hn$ with $h \in H$ and $n \in N$.
We have

$$\begin{aligned} f(g) &= f(hn) = f(h)f(n) \\ &= f(h)e' = f(h) \in f(H) \end{aligned}$$

since f is a group homomorphism and $f(n) = e'$.
Thus we have

$$g \in f^{-1}(f(H))$$

and $f^{-1}(f(H)) \supset HN$.

Therefore, putting the two continents together gives

$$f^{-1}(f(H)) = HN$$

as required.

A Group Homomorphism and an Abelian Group

Problem 207

Let G be a group. Define a map $f : G \to G$ by sending each element $g \in G$ to its inverse $g^{-1} \in G$.
Show that G is an abelian group if and only if the map $f : G \to G$ is a group homomorphism.

Proof.

($\Longrightarrow$) If G is an abelian group, then f is a homomorphism.

Suppose that G is an abelian group. Then we have for any $g, h \in G$

$$\begin{aligned} f(gh) &= (gh)^{-1} = h^{-1}g^{-1} \\ &= g^{-1}h^{-1} \text{ since } G \text{ is abelian} \\ &= f(g)f(h). \end{aligned}$$

This implies that the map f is a group homomorphism.

($\Longleftarrow$) If f is a homomorphism, then G is an abelian group.

Now we suppose that the map $f : G \to G$ is a group homomorphism.
Then for any $g, h \in G$, we have

$$f(gh) = f(g)f(h) \tag{*}$$

since f is a group homomorphism.
The left hand side of (*) is

$$f(gh) = (gh)^{-1} = h^{-1}g^{-1}.$$

Thus we obtain from (*) that

$$h^{-1}g^{-1} = g^{-1}h^{-1}.$$

Taking the inverse of both sides, we have

$$gh = hg$$

for any $g, h \in G$.
It follows that G is an abelian group.

Related Question.

Another problem about the relation between an abelian group and a group homomorphism is:

A group is abelian if and only if squaring is a group homomorphism

Order of the Product of Two Elements in an Abelian Group

Problem 205

Let G be an abelian group with the identity element 1. Let a, b be elements of G with order m and n, respectively.
If m and n are relatively prime, then show that the order of the element ab is mn.

Proof.

Let r be the order of the element ab.

Since we have

$$\begin{aligned}(ab)^{mn} &= a^{mn}b^{mn} \quad (\text{since } G \text{ is an abelian group})\\ &= (a^m)^n(b^n)^m\\ &= 1\end{aligned}$$

since $a^m = 1$ and $b^n = 1$.

This implies that the order r of ab divides mn, that is, we have

$$r|mn. \tag{*}$$

Now, since r is the order of ab we have

$$1 = (ab)^r = a^r b^r.$$

Then we have

$$1 = 1^n = a^{rn}b^{rn} = a^{rn}$$

since $b^n = 1$. This yields that the order m of the element a divides rn.

Since m and n are relatively prime, this implies that we have

$$m|r.$$

Similarly (switch the role of n and m), we obtain

$$n|r.$$

Thus we have

$$mn|r \tag{**}$$

since m and n are relatively prime.

From (*) and (**), we have $r = mn$, and hence the order of the element ab is mn.

Related Question.

As a generalization of this problem, try the following problem.

Problem.Let G be an abelian group.

Let a and b be elements in G of order m and n, respectively.

Prove that there exists an element c in G such that the order of c is the least common multiple of m and n.

A proof of this problem is given in the post "The Existence of an Element in an Abelian Group of Order the Least Common Multiple of Two Elements".

Also See the post "Order of product of two elements in a group" for a similar problem about the order of elements in a non-abelian group.

Two Normal Subgroups Intersecting Trivially Commute Each Other

Problem 196

Let G be a group. Assume that H and K are both normal subgroups of G and $H \cap K = 1$. Then for any elements $h \in H$ and $k \in K$, show that $hk = kh$.

Proof.

It suffices to show that $h^{-1}k^{-1}hk \in H \cap K$.

In fact, if this it true then we have $h^{-1}k^{-1}hk = 1$, and thus $hk = kh$.

Since $h \in H$ and H is a normal subgroup of G, we see that the conjugate $k^{-1}hk \in H$.

Thus we have

$$h^{-1}k^{-1}hk = h^{-1}(k^{-1}hk) \in H. \tag{*}$$

Also, since $k^{-1} \in K$ and K is a normal subgroup of G, we have the conjugate $h^{-1}k^{-1}h \in K$.

Hence, we see that

$$h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k \in K. \tag{**}$$

From (*) and (**), we see that the element $h^{-1}k^{-1}hk$ is in both H and K, hence in $H \cap K$ as claimed.

Abelian Normal Subgroup, Intersection, and Product of Groups

Problem 195

Let G be a group and let A be an abelian subgroup of G with $A \triangleleft G$.
(That is, A is a normal subgroup of G.)
If B is any subgroup of G, then show that

$$A \cap B \triangleleft AB.$$

Proof.

First of all, since $A \triangleleft G$, the product AB is a subgroup of G.

To show that $A \cap B$ is a normal subgroup of AB, let $x \in A \cap B$ and $ab \in AB$, where $a \in A$ and $b \in B$.

Then we have the conjugate

$$(ab)x(ab)^{-1} = a(bxb^{-1})a^{-1}. \tag{*}$$

We show that the right hand side of (*) is in both A and B.

Since $x \in A \cap B \subset A$ and A is a normal subgroup of G, we have

$$bxb^{-1} \in A.$$

Thus the right hand side of (*) is in A.

Also, since the elements a, bxb^{-1}, a^{-1} are all in the abelian group A, we have

$$a(bxb^{-1})a^{-1} = aa^{-1}(bxb^{-1}) = bxb^{-1} \in B$$

since $x, b \in B$.

Therefore $(ab)x(ab)^{-1}$ is in both A and B, and hence

$$(ab)x(ab)^{-1} \in A \cap B$$

and the group $A \cap B$ is a normal subgroup of AB.

Abelian Groups and Surjective Group Homomorphism

Problem 167

Let G, G' be groups. Suppose that we have a surjective group homomorphism $f : G \to G'$.
Show that if G is an abelian group, then so is G'.

Definitions.

Recall the relevant definitions.

- A group homomorphism $f : G \to G'$ is a map from G to G' satisfying

$$f(xy) = f(x)f(y)$$

  for any $x, y \in G$.
- A map $f : G \to G'$ is called surjective if for any $a \in G'$, there exists $x \in G$ such that

$$f(x) = a.$$

- A surjective group homomorphism is a group homomorphism which is surjective.

Proof.

Let $a, b \in G'$ be arbitrary two elements in G'. Our goal is to show that $ab = ba$.
Since the group homomorphism f is surjective, there exists $x, y \in G$ such that

$$f(x) = a, f(y) = b.$$

Now we have

$$\begin{aligned} ab &= f(x)f(y) \\ &= f(xy) \text{ since } f \text{ is a group homomorphism} \\ &= f(yx) \text{ since } G \text{ is an abelian group} \\ &= f(y)f(x) \text{ since } f \text{ is a group homomorphism} \\ &= ba. \end{aligned}$$

Therefore, we obtain $ab = ba$ for any two elements in G', thus G' is an abelian group.

A Homomorphism from the Additive Group of Integers to Itself

Problem 163

Let $\mathbb{Z}$ be the additive group of integers. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a group homomorphism.
Then show that there exists an integer a such that

$$f(n) = an$$

for any integer n.

Hint.

Let us first recall the definition of a group homomorphism.

A group homomorphism from a group G to a group H is a map $f : G \to H$ such that we have

$$f(gg') = f(g)f(g')$$

for any elements $g, g \in G$.

If the group operations for groups G and H are written additively, then a group homomorphism $f : G \to H$ is a map such that

$$f(g + g') = f(g) + f(g')$$

for any elements $g, g' \in G$.

Here is a hint for the problem.

For any integer n, write it as

$$n = 1 + 1 + \cdots + 1$$

and compute $f(n)$ using the property of a homomorphism.

Proof.

Let us put $a := f(1) \in \mathbb{Z}$. Then for any integer n, writing

$$n = 1 + 1 + \cdots + 1,$$

we have

$$\begin{aligned} f(n) &= f(1 + 1 + \cdots + 1) \\ &= f(1) + f(1) + \cdots + f(1) \quad \text{since } f \text{ is a homomorphism} \\ &= a + a + \cdots + a \\ &= an. \end{aligned}$$

Thus we have $f(n) = an$ with $a = f(1) \in \mathbb{Z}$ as required.

Image of a Normal Subgroup Under a Surjective Homomorphism is a Normal Subgroup

Problem 161

Let $f : H \to G$ be a surjective group homomorphism from a group H to a group G.
Let N be a normal subgroup of H. Show that the image $f(N)$ is normal in G.

Proof.

To show that $f(N)$ is normal, we show that $gf(N)g^{-1} = f(N)$ for any $g \in G$. Equivalently, it suffices to show that $gf(n)g^{-1} \in f(N)$ for all $g \in G, n \in N$.

Since f is surjective, for each $g \in G$ there exists $h \in H$ such that $f(h) = g$.

Then we have

$$\begin{aligned} gf(n)g^{-1} &= f(h)f(n)f(h)^{-1} \\ &= f(hnh^{-1}), \end{aligned}$$

where the second equality follows since f is a group homomorphism.

Since N is a normal subgroup in H, the element hnh^{-1} is in N.

Therefore we have $gf(n)g^{-1} \in f(N)$, hence $f(N)$ is a normal subgroup in G.

Finite Group and Subgroup Criteria

Problem 160

Let G be a finite group and let H be a subset of G such that for any $a, b \in H$, $ab \in H$.

Then show that H is a subgroup of G.

Proof.

Let $a \in H$. To show that H is a subgroup of G, it suffices to show that the inverse a^{-1} is in H.

If $a = e$ is the identity element, this is trivial. So we assume that $a \neq e$.

Note that $a^2 = a \cdot a \in H$, $a^3 = a^2 \cdot a \in H$, and repeating this we see that $a^n \in H$ for any positive integer n.

Since G is finite, not all of a^n can be different.

Thus there exists positive integers m, n such that $a^m = a^n$ and $m > n$.

Note that we actually have $m > n + 1$.

For if $m = n + 1$, then we have $a^{n+1} = a^n$ and this implies that $a = e$.

This contradicts out choice of a. Thus we have $m > n + 1$, or equivalently we have

$$m - n - 1 > 0.$$

Since we have

$$a^{m-n} = e,$$

multiplying by a^{-1} we obtain

$$a^{-1} = a^{m-n-1}.$$

Since $m - n - 1 > 0$, the element $a^{m-n-1} \in H$, hence the inverse $a^{-1} \in H$.

Therefore, H is closed under the group operation and inverse, thus H is a subgroup of G.

Remark.

In fact, the group G itself can be an infinite group.

We just need that H is a finite subset satisfying the closure property:for any $a, b \in H$, $ab \in H$.

The proof of this generalization is identical to the proof given above.

Non-Abelian Simple Group is Equal to its Commutator Subgroup

Problem 149

Let G be a non-abelian simple group. Let $D(G) = [G, G]$ be the commutator subgroup of G. Show that $G = D(G)$.

Definitions/Hint.

We first recall relevant definitions.

- A group is called **simple** if its normal subgroups are either the trivial subgroup or the group itself.
- The **commutator subgroup** $D(G) = [G, G]$ is a subgroup of G generated by all commutators $[a, b] = a^{-1}b^{-1}ab$ for $a, b \in G$.

The commutator subgroup $D(G) = [G, G]$ is a normal subgroup of G.

For a proof, see: A condition that a commutator group is a normal subgroup.

Proof.

Note that the commutator subgroup $D(G)$ is a normal subgroup.

Since G is simple, any normal subgroup of G is either the trivial group $\{e\}$ or G itself. Thus we have either

$D(G) = \{e\}$ or $D(G) = G$.
If $D(G) = \{e\}$, then for any two elements $a, b \in G$ the commutator $[a, b] \in D(G) = \{e\}$.
Thus we have

$$a^{-1}b^{-1}ab = [a, b] = e.$$

Therefore we have $ab = ba$ for any $a, b \in G$. This means that the group G is abelian, which contradicts with the assumption that G is non-abelian.
Therefore, we must have $D(G) = G$ as required.

Two Quotients Groups are Abelian then Intersection Quotient is Abelian

Problem 148

Let K, N be normal subgroups of a group G. Suppose that the quotient groups G/K and G/N are both abelian groups.
Then show that the group

$$G/(K \cap N)$$

is also an abelian group.

Hint.

We use the following fact to prove the problem.
Lemma: For a subgroup H of a group G, H is normal in G and G/H is an abelian group if and only if the commutator subgroup $D(G) = [G, G]$ of G is contained in H.
For a proof of this fact, see Commutator subgroup and abelian quotient group

Proof.

By the lemma mentioned above, we know that G/K is an abelian group if and only if the commutator subgroup $D(G) = [G, G]$ is contained in K.
Similarly, since G/N is abelian, $D(G)$ is contained in N.
Therefore, the commutator subgroup $D(G) \subset K \cap N$. This implies, again by Lemma, that the quotient group

$$G/(K \cap N)$$

is an abelian group as required.

Commutator Subgroup and Abelian Quotient Group

Problem 147

Let G be a group and let $D(G) = [G, G]$ be the commutator subgroup of G.
Let N be a subgroup of G.
Prove that the subgroup N is normal in G and G/N is an abelian group if and only if $N \supset D(G)$.

Definitions.

Recall that for any $a, b \in G$, the ***commutator*** of a and b is

$$[a, b] = a^{-1}b^{-1}ab \in G.$$

The ***commutator subgroup*** $D(G) = [G, G]$ is a subgroup of G generated by all commutators.
That is,

$$D(G) = [G, G] = \langle [a, b] \mid a, b \in G \rangle.$$

Proof.

($\implies$) Suppose that N is a normal subgroup of G and the quotient G/N is an abelian group.
Then for any elements $a, b \in G$, we have

$$abN = aN \cdot bN = bN \cdot aN = baN.$$

(Here we used the fact that N is normal, hence G/N is a group.)
From this, we obtain that

$$a^{-1}b^{-1}abN = N$$

and thus $[a, b] = a^{-1}b^{-1}ab \in N$.
Since any generator $[a, b]$ is in N, we have $D(G) \subset N$.

($\impliedby$) On the other hand, let us assume that $N \supset D(G)$.
We first show that N is a normal subgroup of G.
For any $g \in G$, $x \in N$, we have

$$gxg^{-1} = gxg^{-1}x^{-1}x = [g^{-1}, x^{-1}] \cdot x \in N$$

since the commutator $[g^{-1}, x^{-1}] \in D(G) \subset N$ and $x \in N$.
Thus N is normal in G.
Now that N is normal in G, the quotient G/N is a group. We show that G/N is an abelian group.
For any $a, b \in G$, we have

$$\begin{aligned} aN \cdot bN &= abN \\ &= baa^{-1}b^{-1}abN \\ &= ba[a, b]N \\ &= baN \qquad \text{since } [a, b] \in N \\ &= bN \cdot aN. \end{aligned}$$

Therefore the group operations of G/N is commutative, and hence G/H is abelian.

Related Question.

For another abelian group problem, check out

Two quotients groups are abelian then intersection quotient is abelian

Finite Group and a Unique Solution of an Equation

Problem 145

Let G be a finite group of order n and let m be an integer that is relatively prime to $n = |G|$. Show that for any $a \in G$, there exists a unique element $b \in G$ such that

$$b^m = a.$$

Proof 1.

Since m and n are relatively prime integers, there exists integers s, t such that

$$sm + tn = 1.$$

Then we have

$$a = a^1 = a^{sm+tn} = a^{sm}a^{tn} \qquad (*)$$

Note that since the order of the group G is n, any element of G raised by the power of n is the identity element e of G.

Thus we have

$$a^{tn} = (a^n)^t = e^t = e.$$

Putting $b := a^s$, we have from (*) that

$$a = b^m e = b^m.$$

Now we show the uniqueness of such b. Suppose there is another $g' \in G$ such that

$$a = b'^m.$$

Then we have

$$\begin{aligned} & b^m = a = b'^m \\ \Rightarrow\ & b^{sm} = b'^{sm} \quad \text{by taking } s\text{-th power} \\ \Rightarrow\ & b^{1-tn} = b'^{1-tn} \\ \Rightarrow\ & b(b^n)^t = b'(b'^n)^t \\ \Rightarrow\ & b = b' \quad \text{since } b^n = e = b'^n. \end{aligned}$$

Therefore, we have $b = b'$ and the element b satisfying $a = b^m$ is unique.

Proof 2.

Consider a map f from G to G itself defined by sending g to $f(g) = g^m$.

We show that this map is injective.

Suppose that $f(g) = f(g')$.

Since m and n are relatively prime integers, there exists integers s, t such that

$$sm + tn = 1.$$

We have

$$\begin{aligned} f(g) = f(g') & \\ \Rightarrow\ & g^m = g'^m \\ \Rightarrow\ & g^{sm} = g'^{sm} \quad \text{by taking } s\text{-th power} \\ \Rightarrow\ & g^{1-tn} = g'^{1-tn} \\ \Rightarrow\ & g(g^n)^t = g'(g'^n)^t \\ \Rightarrow\ & g = g' \quad \text{since } g^n = e = g'^n, n = |G|. \end{aligned}$$

Therefore the map f is injective. Since G is a finite set, it also follows that the map is bijective.

Thus for any $a \in G$, there is a unique $b \in G$ such that $f(b) = a$, namely, $b^m = a$.

A Group Homomorphism is Injective if and only if the Kernel is Trivial

Problem 144

Let G and H be groups and let $f : G \to K$ be a group homomorphism. Prove that the homomorphism f is injective if and only if the kernel is trivial, that is, $\ker(f) = \{e\}$, where e is the identity element of G.

Definitions/Hint.

We recall several relevant definitions.

- A **group homomorphism** $f : G \to H$ is a map such that for any $g_1, g_2 \in G$, we have
$$f(g_1 g_2) = f(g_1)f(g_2).$$
- A group homomorphism $f : G \to H$ is **injective** if for any $g_1, g_2 \in G$
the equality
$$f(g_1) = f(g_2)$$
implies $g_1 = g_2$.
- The **kernel** of a group homomorphism $f : G \to H$ is a set of all elements of G that is mapped to the identity element of H.
Namely,
$$\ker(f) = \{g \in G \mid f(g) = e'\},$$
where e' is the identity element of H.

Proof.

Injective $\implies$ the kernel is trivial

Suppose the homomorphism $f : G \to H$ is injective.
Then since f is a group homomorphism, the identity element e of G is mapped to the identity element e' of H.
Namely, we have $f(e) = e'$.
If $g \in \ker(f)$, then we have $f(g) = e'$, and thus we have
$$f(g) = f(e).$$
Since f is injective, we must have $g = e$. Thus we have $\ker(f) = \{e\}$.

The kernel is trivial $\implies$ injective

On the other hand, suppose that $\ker(f) = \{e\}$.
If g_1, g_2 are elements of G such that
$$f(g_1) = f(g_2), \tag{$*$}$$
then we have
$$\begin{aligned} f(g_1 g_2^{-1}) &= f(g_1)f(g_2^{-1}) && \text{since } f \text{ is a homomorphism} \\ &= f(g_1)f(g_2)^{-1} && \text{since } f \text{ is a homomorphism} \\ &= f(g_1)f(g_1)^{-1} && \text{by } (*) \\ &= e'. \end{aligned}$$

In the second step, we used the fact $f(g_2^{-1}) = f(g_2)^{-1}$, which is proved in the post "Group Homomorphism Sends the Inverse Element to the Inverse Element".

Thus the element $g_1 g_2^{-1}$ is in the kernel $\ker(f) = \{e\}$, and hence $g_1 g_2^{-1} = e$.

This implies that we have $g_1 = g_2$ and f is injective.

Multiplicative Groups of Real Numbers and Complex Numbers are not Isomorphic

Problem 130

Let $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ be the multiplicative group of real numbers.
Let $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ be the multiplicative group of complex numbers.
Then show that $\mathbb{R}^\times$ and $\mathbb{C}^\times$ are not isomorphic as groups.

Recall.

Let G and K be groups.

Recall that a map $f : G \to K$ is a group homomorphism if

$$f(ab) = f(a)f(b)$$

for all $a, b \in G$.

A group isomorphism is a bijective homomorphism.

If there is a group isomorphism from G to K, we say that G and K are isomorphic (as groups).

We give two proofs.

Proof 1.

Seeking a contradiction, assume that there is a group isomorphism $\phi : \mathrm{C}^\times \to \mathrm{R}^\times$.

Since ϕ is a group homomorphism, $\phi(1) = 1$. Thus we have

$$1 = \phi(1) = \phi((-1)(-1)) = \phi(-1)\phi(-1) = \phi(-1)^2.$$

Hence $\phi(-1) = \pm 1$. But since ϕ is injective and $\phi(1) = 1$, we must have $\phi(-1) = -1$.

Now we have

$$-1 = \phi(-1) = \phi(i^2) = \phi(i)^2.$$

Since $\phi(i) \in \mathrm{R}^\times$, $\phi(i)^2$ must be a positive number. Thus we reached a contradiction.

Hence there is no isomorphism between $\mathrm{R}^\times$ and $\mathrm{C}^\times$.

Proof 2.

Suppose that there is a group isomorphism $\phi : \mathrm{C}^\times \to \mathrm{R}^\times$.

We want to find a contradiction.

Let $\zeta = e^{2\pi i/3}$ be a primitive third root of unity.

Since $\zeta^3 = 1$ and ϕ is a group homomorphism, we have

$$1 = \phi(1) = \phi(\zeta^3) = \phi(\zeta)^3.$$

Since $\phi(\zeta)$ is a real number, this implies that $\phi(\zeta) = 1$.

This is a contradiction since ϕ is injective, but we have $\phi(1) = 1 = \phi(\zeta)$.

Therefore, there cannot be a group isomorphism between $\mathrm{R}^{\times}$ and $\mathrm{C}^{\times}$.

Group Generated by Commutators of Two Normal Subgroups is a Normal Subgroup

Problem 129

Let G be a group and H and K be subgroups of G.
For $h \in H$, and $k \in K$, we define the commutator $[h, k] := hkh^{-1}k^{-1}$.
Let $[H, K]$ be a subgroup of G generated by all such commutators.
Show that if H and K are normal subgroups of G, then the subgroup $[H, K]$ is normal in G.

Proof.

We first prove that a conjugate of each generator is in $[H, K]$.
Let $h \in H, k \in K$. For any $g \in G$, we have by inserting $g^{-1}g = e$ inbetweens

$$\begin{aligned} g[h, k]g^{-1} &= ghkh^{-1}k^{-1} = (ghg^{-1})(gkg^{-1})(gh^{-1}g^{-1})(gk^{-1}g^{-1}) \\ &= (ghg^{-1})(gkg^{-1})(ghg^{-1})^{-1}(gkg^{-1})^{-1}. \end{aligned}$$

Now note that $ghg^{-1} \in H$ since H is normal in G, and $gkg^{-1} \in K$ since K is normal in G. Thus $g[h, k]g^{-1} \in [H, K]$.
By taking the inverse of the above equality, we also see that $g[k, h]g^{-1} \in [H, K]$. Thus the conjugate of the inverse $[h, k]^{-1} = [k, h]$ is in $[H, K]$.

Next, note that any element $x \in [H, K]$ is a product of generators or their inverses. So let us write

$$x = [h_1, k_1]^{\pm 1}[h_2, k_2]^{\pm 1} \cdots [h_n, k_n]^{\pm 1},$$

where $h_i \in H, k_i \in K$ for $i = 1, \dots, n$.
Then for any $g \in G$, we have

$$gxg^{-1} = (g[h_1, k_1]^{\pm 1}g^{-1})(g[h_2, k_2]^{\pm 1}g^{-1}) \cdots (g[h_n, k_n]^{\pm 1}g^{-1}).$$

We saw that the conjugate of a generator, or its inverse, by $g \in G$ is in $[H, K]$.
Thus gxg^{-1} is also in $[H, K]$.
This proves that the group $[H, K]$ is a normal subgroup of G.

Related Question.

Another problem about a commutator group is

A condition that a commutator group is a normal subgroup

If a Subgroup H is in the Center of a Group G and G/H is Nilpotent, then G is Nilpotent

Problem 128

Let G be a nilpotent group and let H be a subgroup such that H is a subgroup in the center $Z(G)$ of G.
Suppose that the quotient G/H is nilpotent.
Then show that G is also nilpotent.

Definition (Nilpotent Group)

We recall here the definition of a nilpotent group.

Let G be group. Define $G^0 = G$,

$$G^1 = [G,G] = \langle [x,y] := xyx^{-1}y^{-1} \mid x,y \in G \rangle,$$

and inductively define

$$G^i = [G^{i-1}, G] = \langle [x,y] \mid x \in G^{i-1}, y \in G \rangle.$$

Then we obtain so called the lower central series of G:

$$G^0 \triangleright G^1 \triangleright \cdots \triangleright G^i \triangleright \cdots.$$

If there exists $m \in \mathbb{Z}$ such that $G^m = \{e\}$, then the group G is called ***nilpotent***.

Proof.

Consider the natural projection $p : G \to G/H$.

Then we have $p(G^i) = (G/H)^i$.

Since G/H is nilpotent, there exists $m \in \mathbb{Z}$ such that $(G/H)^m = \{eH\}$.

Thus we obtain

$$p(G^m) = (G/H)^m = \{eH\}.$$

Thus for any $g \in G^m$, $g \in H \subset Z(G)$.

It follows that for any $g \in G^m$, $x \in G$ we have $gxg^{-1}x^{-1} = e$.

Since the elements $gxg^{-1}x^{-1}$ are generators of $G^{m+1} = [G^m, G]$, we conclude that $G^{m+1} = \{e\}$ and G is nilpotent.

Normal Subgroups, Isomorphic Quotients, But Not Isomorphic

Problem 127

Let G be a group. Suppose that H_1, H_2, N_1, N_2 are all normal subgroup of G, $H_1 \lhd N_2$, and $H_2 \lhd N_2$.
Suppose also that N_1/H_1 is isomorphic to N_2/H_2. Then prove or disprove that N_1 is isomorphic to N_2.

Proof.

We give a counterexample.

Let $G = \mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, where p and q are distinct prime numbers. Then G is an abelian group and thus any subgroups are normal.

We denote e for identity elements of possibly different groups.

Let

$$N_1 = \mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \{e\} \subset G$$

and

$$N_2 = \mathbb{Z} \times \{e\} \times \mathbb{Z}/q\mathbb{Z} \subset G.$$

Also define subgroups

$$H_1 = q\mathbb{Z} \times \{e\} \times \{e\} \subset N_1$$

and

$$H_2 = p\mathbb{Z} \times \{e\} \times \{e\} \subset N_2.$$

Then both H_1 and H_2 are isomorphic to $\mathbb{Z}$.

The quotients groups N_1/H_1 and N_2/H_2 are both isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Since p and q are distinct primes, the groups N_1 and N_2 are not isomorphic.

Therefore, we disprove the claim.

The Index of the Center of a Non-Abelian p-Group is Divisible by p^2

Problem 124

Let p be a prime number.

Let G be a non-abelian p-group.

Show that the index of the center of G is divisible by p^2.

Proof.

Suppose the order of the group G is p^a, for some $a \in \mathbb{Z}$.

Let $Z(G)$ be the center of G. Since $Z(G)$ is a subgroup of G, the order of the center is also a power of p, that is, $|Z(G)| = p^b$, for some $b \in \mathbb{Z}$.

Then we have the index $[G : Z(G)] = p^{a-b}$.

If $a - b = 0$, then we have $G = Z(G)$ and G is an abelian group. This contradicts with the assumption that G is non-abelian. So $a - b \neq 0$.

If $a - b = 1$, then the order of the quotient $|G/Z(G)| = [G : Z(G)] = p$ is a prime, thus $G/Z(G)$ is a cyclic group.

Recall that if the quotient by the center is cyclic, then the group is abelian.

Thus the group G is abelian, which again a contradiction.

Therefore, we must have $a - b \geq 2$, hence p^2 divides the index $[G : Z(G)] = p^{a-b}$.

This concludes the proof.

Infinite Cyclic Groups Do Not Have Composition Series

Problem 123

Let G be an infinite cyclic group. Then show that G does not have a composition series.

Proof.

Let $G = \langle a \rangle$ and suppose that G has a composition series

$$G = G_0 \rhd G_1 \rhd \cdots G_{m-1} \rhd G_m = \{e\},$$

where e is the identity element of G.

Note that each G_i is an infinite cyclic subgroup of G.

Let $G_{m-1} = \langle b \rangle$. Then we have

$$G_{m-1} = \langle b \rangle \rhd \langle b^2 \rangle \rhd \{e\}$$

and the inclusions are proper.

(Since a cyclic group is abelian, these subgroups are normal in G.)

But this contradicts that G_{m-1} is a simple group.

Thus, there is no composition series for an infinite cyclic group G.

Related Question.

You might also be interested in

Any finite group has a composition series

Any Finite Group Has a Composition Series

Problem 122

Let G be a finite group. Then show that G has a composition series.

Proof.

We prove the statement by induction on the order $|G| = n$ of the finite group.

When $n = 1$, this is trivial.

Suppose that any finite group of order less than n has a composition series.

Let G be a finite group of order n.

If G is simple, then $G \rhd \{e\}$, where e is the identity element of G, is a composition series and we are done.

Thus, suppose that G is not simple. Then it has a nontrivial proper normal subgroup.

Since G is a finite group, there exists a maximal proper normal subgroup H.

Then the quotient G/H is a simple group.

In fact, if N is a proper normal subgroup of G/H, then the preimage of N under the natural projection homomorphism $\pi : G \to G/H$ is a proper normal subgroup of G containing H by the fourth isomorphism theorem.

Since H is maximal, the preimage $\pi^{-1}(N)$ must be H. This implies N is trivial in G/H and thus G/H is simple.

Since H is a proper subgroup of G, the order of H is less than that of G.

Thus by the induction hypothesis, H has a composition series

$$H = N_1 \rhd N_1 \rhd \cdots \rhd N_m = \{e\}.$$

The series

$$G = N_0 \rhd H = N_1 \rhd N_1 \rhd \cdots \rhd N_m = \{e\}$$

has a simple factors N_i/N_{i+i}, hence it is a composition series for G.

Related Question.

You might also be interested in

Infinite cyclic groups do not have composition series

Group of Order 18 is Solvable

Problem 118

Let G be a finite group of order 18.

Show that the group G is solvable.

Definition

Recall that a group G is said to be **solvable** if G has a subnormal series

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

such that the factor groups G_i/G_{i-1} are all abelian groups for $i = 1, 2, \dots, n$.

Proof.

Since $18 = 2 \cdot 3^2$, the number n_3 of Sylow 3-subgroups is 1 by the Sylow theorem.

(Sylow's theorem implies that $n_3 \equiv 1 \pmod 3$ and n_3 divides 2.)

Hence the unique Sylow 3-subgroup P is a normal subgroup of G.

The order of P is 9, a square of a prime number, thus P is abelian.

(See A group of order the square of a prime is abelian.)

Also, the order of the quotient group G/P is 2, thus G/P is an abelian (cyclic) group.

Thus we have a filtration

$$G \triangleright P \triangleright \{e\}$$

whose factors $G/P, P/\{e\}$ are abelian groups, hence G is solvable.

Related Question.

Check the following similar questions.

- Group of order pq has a normal Sylow subgroup and solvable
- A group of order pqr contains a normal subgroup of order either p, q, or r

If a Subgroup Contains a Sylow Subgroup, then the Normalizer is the Subgroup itself

Problem 117

Let G be a finite group and P be a nontrivial Sylow subgroup of G.
Let H be a subgroup of G containing the normalizer $N_G(P)$ of P in G.
Then show that $N_G(H) = H$.

Hint.

Use the conjugate part of the Sylow theorem.

See the second statement of the Sylow theorem.

Proof.

It is clear that $H \subset N_G(H)$.

So we show that $N_G(H) \subset H$.

Take any $a \in N_G(H)$. Since $P \subset N_G(P) \subset H$, we have

$$aPa^{-1} \subset aHa^{-1} = H,$$

where the last step follows from $a \in N_G(H)$.

It follows that P and aPa^{-1} are both Sylow subgroups in H.

By the Sylow theorem, any two p-Sylow subgroups are conjugate. Thus there exists $b \in H$ such that $bPb^{-1} = aPa^{-1}$.

This implies that $(b^{-1}a)P(b^{-1}a)^{-1} = P$ and thus $b^{-1}a \in N_G(P) \subset H$. Hence we have $a \in H$ since $b \in H$.

This shows that $N_G(H) \subset H$, hence $N_G(H) = H$ as required.

Corollary (The Normalizer of the Normalizer of a Sylow subgroup)

We apply the result to the case $H = N_G(P)$, and obtain the following result.

The normalizer of the normalizer of a Sylow subgroup P of a finite group G is the normalizer of P.
That is, we have

$$N_G(N_G(P)) = N_G(P).$$

The Preimage of a Normal Subgroup Under a Group Homomorphism is Normal

Problem 116

Let G and G' be groups and let $f : G \to G'$ be a group homomorphism.
If H' is a normal subgroup of the group G', then show that $H = f^{-1}(H')$ is a normal subgroup of the group G.

Proof.

We prove that H is normal in G. (The fact that H is a subgroup in G is left as an exercise.)
For any element $g \in G$ and $h \in H$, we have

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1}$$

since f is a group homomorphism.
Since $f(g) \in G'$, $f(h) \in H'$, and H' is normal in G', we see that

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'.$$

Thus by the definition of H, the element $ghg^{-1} \in H$.
This proves that H is a normal subgroup in G.

Isomorphism Criterion of Semidirect Product of Groups

Problem 113

Let A, B be groups. Let $\phi : B \to \mathrm{Aut}(A)$ be a group homomorphism.
The semidirect product $A \rtimes_\phi B$ with respect to ϕ is a group whose underlying set is $A \times B$ with group operation

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1\phi(b_1)(a_2), b_1b_2),$$

where $a_i \in A, b_i \in B$ for $i = 1, 2$.
Let $f : A \to A'$ and $g : B \to B'$ be group isomorphisms. Define $\phi' : B' \to \mathrm{Aut}(A')$ by sending $b' \in B'$ to $f \circ \phi(g^{-1}(b')) \circ f^{-1}$.

$$\begin{array}{ccc} B & \xrightarrow{\phi} & \mathrm{Aut}(A) \\ {\scriptstyle g^{-1}}\uparrow & & \downarrow{\scriptstyle \sigma_f} \\ B' & \xrightarrow{\phi'} & \mathrm{Aut}(A') \end{array}$$

Here $\sigma_f : \mathrm{Aut}(A) \to \mathrm{Aut}(A')$ is defined by $\alpha \in \mathrm{Aut}(A) \mapsto f\alpha f^{-1} \in \mathrm{Aut}(A')$.
Then show that

$$A \rtimes_\phi B \cong A' \rtimes_{\phi'} B'.$$

Proof.

Define $\Psi : A \rtimes_\phi B \to A' \rtimes_{\phi'} B'$ by

$$(a,b) \mapsto (f(a), g(b))$$

for $(a,b) \in A \rtimes_\phi B$.

We show that this is a group isomorphism. Since f, g are group isomorphisms, it suffices to show that Ψ is a group homomorphism.

Let $(a_1,b_1),(a_2,b_2) \in A \rtimes_\phi B$. We compute the product in$A \rtimes_\phi$ is

$$(a_1,b_1)\cdot(a_2,b_2) = (a_1\phi(b_1)(a_2), b_1b_2).$$

Thus we have

$$\begin{aligned}\Psi\left((a_1,b_1)\cdot(a_2,b_2)\right) &= \Psi\left((a_1\phi(b_1)(a_2), b_1b_2)\right)\\ &= \Big(f\big(a_1\phi(b_1)(a_2)\big), g(b_1b_2)\Big). \qquad (*)\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\Psi\left((a_1,b_1)\right)\cdot\Psi\left((a_2,b_2)\right) &= (f(a_1),g(b_1))\cdot(f(a_2),g(b_2)).\\ &= \Big(f(a_1)\phi'\big(g(b_2)\big)\big(f(a_2)\big), g(b_1)g(b_2)\Big) \qquad (**)\end{aligned}$$

Here we used group operation in $A' \rtimes_{\phi'} B'$ in the second equality.

Now by the definition of ϕ' we have

$$\phi'(g(b_2)) = f\circ\phi(g^{-1}(g(b_2)))\circ f^{-1} = f\circ\phi(b_2)\circ f^{-1}.$$

Thus we have

$$\phi'(g(b_2))(f(a_2)) = f\circ\phi(b_2)a_2.$$

Hence we have

$$\begin{aligned}(**) &= \Big(f(a_1)f\big(\phi(b_2)a_2\big), g(b_1)g(b_2)\Big)\\ &= \Big(f\big(a_1\phi(b_1)(a_2)\big), g(b_1b_2)\Big),\end{aligned}$$

where the last equality follows since f, g are group homomorphisms.

Comparing this with (*), we see that

$$\Psi\left((a_1,b_1)\cdot(a_2,b_2)\right) = \Psi\left((a_1,b_1)\right)\cdot\Psi\left((a_2,b_2)\right)$$

and thus Ψ is a group homomorphism, hence it is a group isomorphism.

Corollary

In particular, taking $A = A'$ and $B = B'$, we have the following corollary.

Let $A \rtimes_\phi B$ be the semidirect product of groups A and B with respect to a homomorphism $\phi : B \to \mathrm{Aut}(A)$.

If $\phi' : B \to \mathrm{Aut}(A)$ is defined by the following diagram, then we have

$$A \rtimes_\phi \cong A \rtimes_{\phi'} B.$$

$$\begin{array}{ccc} B & \xrightarrow{\phi} & \mathrm{Aut}(A) \\ {\scriptstyle g^{-1}}\uparrow & & \downarrow{\scriptstyle \sigma_f} \\ B & \xrightarrow{\phi'} & \mathrm{Aut}(A) \end{array}$$

Application

Determine all isomorphism classes of semidirect product groups $(C_2 \times C_2) \rtimes C_3$, where C_i denotes a cyclic group of order i.

Proof.

We first determine all homomorphism $\phi : C_3 \to \mathrm{Aut}(C_2 \times C_2)$.

Note that $\mathrm{Aut}(C_2 \times C_2) \cong S_3$. ($C_2 \times C_2$ has three degree 2 elements and an automorphism permutes these elements.)

Let g be a generator of C_3. Then since g is of order 3, the image $\phi(g)$ is one of 1, (123), (132).

Thus there are three homomorphism from $C_3 \to \mathrm{Aut}(C_2 \times C_2)$ defined by

$$\phi_0(g) = 1, \phi_1(g) = (123), \phi_2(g) = (132).$$

Since ϕ_0 is a trivial homomorphism, the semidirect product is actually a direct product. Thus

$$(C_2 \times C_2) \rtimes_{\phi_0} C_3 = (C_2 \times C_2) \times C_3,$$

which is an abelian group.

For ϕ_1 and ϕ_2, we obtain nonabelian groups

$$(C_2 \times C_2) \rtimes_{\phi_1} C_3 \text{ and } (C_2 \times C_2) \rtimes_{\phi_2} C_3.$$

We claim that these two groups are isomorphic.

Note that we have

$$\phi_1(x) = \tau \phi_2(x) \tau^{-1}$$

for all $x \in C_3$, where $\tau = (23) \in S_3$.

Thus the claim follows from Corollary.

(In the notations in Corollary, $A = C_2 \times C_2$, $B = C_3$, $f \in \mathrm{Aut}(A) \cong S_3$ is (23) and $g : B \to B$ is the identity.)

Therefore we have two isomorphism classes for $(C_2 \times C_2) \rtimes C_3$, one is abelian, the other is nonabelian.

(In fact, the nonabelian group is isomorphic to A_4.)

Nontrivial Action of a Simple Group on a Finite Set

Problem 112

Let G be a simple group and let X be a finite set.

Suppose G acts nontrivially on X. That is, there exist $g \in G$ and $x \in X$ such that $g \cdot x \neq x$.

Then show that G is a finite group and the order of G divides $|X|!$.

Proof.

Since G acts on X, it induces a permutation representation

$$\rho : G \to S_X.$$

Let $N = \ker(\rho)$ be the kernel of ρ.

Since a kernel is normal in G and G is simple, we have either $N = \{e\}$ or $N = G$.

If $N = G$, then for any $g \in G$ we have $\rho(g)$ is a trivial action, that is, $g \cdot x = x$ for any X.

This contradicts the assumption that G acts nontrivially on X.

Hence we have $N = \{e\}$, and it follows that the homomorphism ρ is injective.

Thus we have

$$G \cong \mathrm{im}(\rho) < S_X.$$

Since S_X is a finite group and G is isomorphic to its subgroup, the group G is finite.

By Lagrange's theorem, the order $|G| = |\mathrm{im}(\rho)|$ of G divides the order $|S_X| = |X|!$ of S_X.

Conjugate of the Centralizer of a Set is the Centralizer of the Conjugate of the Set

Problem 109

Let X be a subset of a group G. Let $C_G(X)$ be the centralizer subgroup of X in G.
For any $g \in G$, show that $gC_G(X)g^{-1} = C_G(gXg^{-1})$.

Proof.

$(\subset)$ We first show that $gC_G(X)g^{-1} \subset C_G(gXg^{-1})$.

Take any $h \in C_G(X)$. Then for any element $x \in X$, we have

$$\begin{aligned} ghg^{-1}(gxg^{-1}) &= ghxg^{-1} \\ &= gxhg^{-1} \quad \text{since } h \in C_G(X) \\ &= gxg^{-1}(ghg^{-1}). \end{aligned}$$

This computation shows that $ghg^{-1} \in C_G(gXg^{-1})$ for any $h \in C_G(X)$.

Thus this proves $gC_G(X)g^{-1} \subset C_G(gXg^{-1})$.

$(\supset)$ Conversely, take any element $k \in C_G(gXg^{-1})$.

Then for any $x \in X$, we have

$$\begin{aligned} g^{-1}kg(x) &= g^{-1}k(gxg^{-1})g \\ &= g^{-1}(gxg^{-1})kg \quad \text{since } k \in C_G(gXg^{-1}) \\ &= x(g^{-1}kg). \end{aligned}$$

This implies that $g^{-1}kg \in C_G(X)$, hence $k \in gC_G(X)g^{-1}$ for any $k \in C_G(gXg^{-1})$. This proves $C_G(gXg^{-1}) \subset gC_G(X)g^{-1}$.

Group of Invertible Matrices Over a Finite Field and its Stabilizer

Problem 108

Let $\mathbb{F}_p$ be the finite field of p elements, where p is a prime number.

Let $G_n = \mathrm{GL}_n(\mathbb{F}_p)$ be the group of $n \times n$ invertible matrices with entries in the field $\mathbb{F}_p$. As usual in linear algebra, we may regard the elements of G_n as linear transformations on $\mathbb{F}_p^n$, the n-dimensional vector space over $\mathbb{F}_p$. Therefore, G_n acts on $\mathbb{F}_p^n$.

Let $e_n \in \mathbb{F}_p^n$ be the vector $(1, 0, \dots, 0)$.

(The so-called first standard basis vector in $\mathbb{F}_p^n$.)

Find the size of the G_n-orbit of e_n, and show that $\mathrm{Stab}_{G_n}(e_n)$ has order $|G_{n-1}| \cdot p^{n-1}$.

Conclude by induction that

$$|G_n| = p^{n^2} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right).$$

Proof.

Let $\mathcal{O}$ be the orbit of e_n in $\mathbb{F}_p^n$.
We claim that $\mathcal{O} = \mathbb{F}_p^n \setminus \{0\}$, hence

$$|\mathcal{O}| = p^n - 1.$$

To prove the claim, let $a_1 \in \mathbb{F}_p^n$ be a nonzero vector.
Then we can extend this vector to a basis of $\mathbb{F}_p^n$, that is, there is $a_2, \ldots, a_n \in \mathbb{F}_p^n$ such that $a_1,\ a_2, \ldots, a_n$ is a basis of $\mathbb{F}_P^n$.
Since they are a basis the matrix $A = [a_1 \ldots a_n]$ is invertible, that is , $A \in G_n$.
We have

$$Ae_n = a_1$$

Thus $a_1 \in \mathcal{O}$. It is clear that $0 \notin \mathcal{O}$. Thus we proved the claim.

Next we show that

$$|\mathrm{Stab}_{G_n}(e_n)| = |G_{n-1}| \cdot p^{n-1}. \qquad (*)$$

Note that $A \in \mathrm{Stab}_{G_n}(e_n)$ if and only if $Ae_n = e_n$.
Thus A is of the form

$$\left[\begin{array}{c|c} 1 & A_2 \\ \hline \mathbf{0} & A_1 \end{array}\right],$$

where A_1 is an $(n-1) \times (n-1)$ matrix, A_2 is a $1 \times (n-1)$ matrix , and $\mathbf{0}$ is the $(n-1) \times 1$ zero matrix.
Since A is invertible, the matrix A_1 must be invertible as well, hence $A_1 \in G_{n-1}$.
The matrix A_2 can be anything.
Thus there are $|G_{n-1}|$ choices for A_1 and p^{n-1} choices for A_2.
In total, there are $|G_{n-1}|p^{n-1}$ possible choices for $A \in \mathrm{Stab}_{G_n}(e_n)$. This proves (*).

Finally we prove that

$$|G_n| = p^{n^2} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right)$$

by induction on n.

When $n = 1$, we have

$$|G_1| = |\mathbb{F}_p \setminus \{0\}| = p - 1 = p\left(1 - \frac{1}{p}\right).$$

Now we assume that the formula is true for $n-1$.

By the orbit-stabilizer theorem, we have

$$|G_n : \mathrm{Stab}_{G_n}(e_n)| = |\mathcal{O}|.$$

Since G_n is finite, we have

$$\begin{aligned}
|G_n| &= |\mathrm{Stab}_{G_n}(e_n)||\mathcal{O}| \\
&= (p^n-1)|G_{n-1}|p^{n-1} \\
&= (p^n-1)p^{n-1}\cdot p^{(n-1)^2}\prod_{i=1}^{n-1}\left(1-\frac{1}{p^i}\right) \text{ by the induction hypothesis} \\
&= p^n\left(1-\frac{1}{p^n}\right)p^{n-1}p^{n^2-2n+1}\prod_{i=1}^{n-1}\left(1-\frac{1}{p^i}\right) \\
&= p^{n^2}\prod_{i=1}^{n}\left(1-\frac{1}{p^i}\right).
\end{aligned}$$

Thus the formula is true for n as well.

By induction, the formula is true for any n.

If a Group is of Odd Order, then Any Nonidentity Element is Not Conjugate to its Inverse

Problem 106

Let G be a finite group of odd order. Assume that $x \in G$ is not the identity element.
Show that x is not conjugate to x^{-1}.

Proof.

Assume the contrary, that is, assume that there exists $g \in G$ such that $gx^{-1}g^{-1} = x$.

Then we have

$$xg = gx^{-1}. \tag{*}$$

Then we compute

$$\begin{aligned}
(xg)^2 &= (gx^{-1})(xg) = g^2 \\
(xg)^3 &= (xg)(xg)^2 = (xg)(g^2) = xg^3 \\
(xg)^4 &= (xg)^2(xg)^2 = g^2g^2 = g^4.
\end{aligned}$$

In general, we have by induction

$$(xg)^k = \begin{cases} xg^k & \text{if } k \text{ is odd} \\ g^k & \text{if } k \text{ is even.} \end{cases} \tag{**}$$

Let m be the order of g. Since G is a finite group of odd order, m is odd.

We have by (**)

$$(xg)^{m-1}g = g^{m-1}g = g^m = 1.$$

Thus we have $g^{-1} = (xg)^{m-1}$. Multiplying by xg from the right, we have

$$\begin{aligned} g^{-1}xg &= (xg)^m \\ &= xg^m \text{ by (**)} \\ &= x. \end{aligned}$$

Thus we have $gx = xg$, and combining with (*) we obtain $gx = gx^{-1}$.

This implies that $x^2 = 1$, and since the order of G is odd, this implies $x = 1$.

This contradicts our choice of x.

Therefore x cannot be conjugate to x^{-1}.

A Subgroup of the Smallest Prime Divisor Index of a Group is Normal

Problem 105

Let G be a finite group of order n and suppose that p is the smallest prime number dividing n.
Then prove that any subgroup of index p is a normal subgroup of G.

Hint.

Consider the action of the group G on the left cosets G/H by left multiplication.

Proof.

Let H be a subgroup of index p.

Then the group G acts on the left cosets G/H by left multiplication.

It induces the permutation representation $\rho : G \to S_p$.

Let $K = \ker \rho$ be the kernel of ρ.

Since $kH = H$ for $k \in K$, we have $K \subset H$.

Let $[H : K] = m$.

By the first isomorphism theorem, the quotient group G/K is isomorphic to the subgroup of S_p, thus $[G : K]$ divides $|S_p| = p!$ by Lagrange's theorem.

Since $[G : K] = [G : H][H : K] = pm$, we have $pm | p!$ and hence $m|(p-1)!$.

If m has a prime factor q, then $q \geq p$ since the minimality of p but the factors of $(p-1)!$ are only prime numbers less than p.

Thus $m|(p-1)!$ implies that $m = 1$, hence $H = K$. Therefore H is normal since a kernel is always normal.

Are Groups of Order 100, 200 Simple?

Problem 100

Determine whether a group G of the following order is simple or not.
(a) $|G| = 100$.
(b) $|G| = 200$.

Hint.

Use Sylow's theorem and determine the number of 5-Sylow subgroup of the group G.

Check out the post Sylow's Theorem (summary) for a review of Sylow's theorem.

Proof.

(a) When $|G| = 100$.

The prime factorization of 100 is $2^2 \cdot 5^2$. Let us determine the number n_5 of 5-Sylow subgroup of G.
By Sylow's theorem, we know that $n_5 \equiv 1 \pmod 5$ and n_5 divides 2^2.
The only number satisfies both constraints is $n_5 = 1$. Thus there is only one 5-Sylow subgroup of G. This implies that the 5-Sylow subgroup is a normal subgroup of G.
Since the order of the 5-Sylow subgroup is 25, it is a proper normal subgroup. Thus, the group G is not simple.

(b) When $|G| = 200$

The prime factorization is $200 = 2^3 \cdot 5^2$.
We again consider the number n_5 of 5-Sylow subgroups of G.
Sylow's theorem implies that $n_5 \equiv 1 \pmod 5$ and n_5 divides 2^3.
These two constraints has only one solution $n_5 = 1$.
Thus the group G has a unique proper normal 5-Sylow subgroup of order 25. Hence G is a simple group.

Similar problem

For an analogous problem, check out the post: If the order is an even perfect number, then a group is not simple

Comment.

This is the 100th problems in this blog.
To post 100 problems were not so simple.
The next goal is to archive the 200th problem.
This problem suggests that this goal is again not simple.
(Update: On 11/25/2016 I achieved the 200th problem: Maximize the dimension of the null space of $A - aI$.)

Abelian Group and Direct Product of Its Subgroups

Problem 95

Let G be a finite abelian group of order mn, where m and n are relatively prime positive integers.
Then show that there exists unique subgroups G_1 of order m and G_2 of order n such that $G \cong G_1 \times G_2$.

Hint.

Consider subgroups

$$G_1 = \{x \in G \mid x^m = 1\}$$

and

$$G_2 = \{x \in G \mid x^n = 1\}.$$

Proof.

We first show that the existence of such subgroups of G.
Let

$$G_1 = \{x \in G \mid x^m = 1\}$$

and

$$G_2 = \{x \in G \mid x^n = 1\}.$$

We claim that $G = G_1 \times G_2$.

To show this, we prove the following conditions.

(a) G_1 and G_2 are normal in G,

(b) $G_1 \cap G_2 = e$, where e is the identity element of G, and

(c) $G = G_1 G_2$

Conditions (a) and (b) imply that $G_1 G_2 \cong G_1 \times G_2$ and condition (c) concludes that $G \cong G_1 \times G_2$.

Condition (a) is clear since G is an abelian group.

To show condition (b), take $x \in G_1 \cap G_2$, thus $x^m = x^n = 1$.

Since m and n are relatively prime, there exist integers a, b such that $am + bn = 1$.

Then we have

$$x = x^1 = x^{am+bn} = x^{am} x^{bn} = (x^m)^a (x^n)^b = e^a e^b = e.$$

Therefore we proved $G_1 \cap G_2 = e$, hence condition (b) holds as well and we conclude that $G_1 G_2 = G_1 \times G_2$.

Next we prove condition (c).

The inclusion $G_1 G_2 \subset G$ is clear. For any $x \in G$, we can write

$$x = x^{am+bn} = x^{bn} x^{am}.$$

Then x^{bn} is in G_1 since

$$(x^{bn})^m = (x^{mn})^b = e^b = e$$

where the second equality follows since the order of G is mn.

Similarly, x^{an} is in G_2 since

$$(x^{an})^m = (x^{mn})^a = e^a = e.$$

Hence $x = x^{bn} x^{am} \in G_1 G_2$, and we have $G = G_1 G_2$.

We checked all the conditions and hence $G \cong G_1 \times G_2$. From this it follows that the order of G_1 is m and the order of G_2 is n.

Now we show the uniqueness of such subgroups.

If G_1' is a subgroup of G of order m, then by the definition of G_1, we have

$$G_1' \subset G_1.$$

Since both groups are of order m, they must be equal. Thus G_1 is the unique subgroup of order m. Similarly for G_2. This completes the proof.

Normalizer and Centralizer of a Subgroup of Order 2

Problem 94

Let H be a subgroup of order 2. Let $N_G(H)$ be the normalizer of H in G and $C_G(H)$ be the centralizer of H in G.
(a) Show that $N_G(H) = C_G(H)$.
(b) If H is a normal subgroup of G, then show that H is a subgroup of the center $Z(G)$ of G.

Definitions.

Recall that the ***centralizer*** of H in G is

$$C_G(H) = \{g \in G \mid gh = hg \text{ for any } h \in H\}.$$

The ***normalizer*** of H in G is

$$N_G(H) = \{g \in G \mid gH = Hg\}.$$

Proof.

(a) Prove $N_G(H) = C_G(H)$

In general, we have $C_G(H) \subset N_G(H)$. We show that $N_G(H) \subset C_G(H)$.
Take any $g \in N_G(H)$. We have $gH = Hg$. Since $|H| = 2$, let $H = \{1, h\}$.
Then $gH = \{g, gh\}$ and $Hg = \{g, hg\}$. Since $gH = Hg$, we have $gh = hg$. Namely $g \in C_G(H)$.
This proves that $N_G(H) \subset C_G(H)$, hence $N_G(H) = C_G(H)$.

(b) If H is normal, then H is a subgroup of $Z(G)$

Suppose that H is a normal subgroup of G, that is $G = N_G(H)$.
By part (a), this implies that $G = C_G(H)$. Hence $H < Z(G)$.

A Group of Order pqr Contains a Normal Subgroup of Order Either p, q, or r

Problem 81

Let G be a group of order $|G| = pqr$, where p, q, r are prime numbers such that $p < q < r$.
Show that G has a normal subgroup of order either p, q or r.

Hint.

Show that using Sylow's theorem that G has a normal Sylow subgroup of order either p, q, or r.

Review Sylow's theorem (Especially (3) and (4) in the theorem).

The group G has a normal Sylow p-subgroup if and only if the number n_p of Sylow p-subgroup is 1.

Proof.

We show that the group G has a normal Sylow subgroup of order either p, q, or r.

Let n_p be the number of the Sylow p-subgroups of G and similarly define n_q and n_r.

Seeking a contradiction, suppose that G has no normal Sylow subgroups.

This is equivalent to saying that $n_p > 1$, $n_q > 1$, and $n_r > 1$.

Sylow's theorem yields that $n_r \equiv 1 \pmod{r}$ and $n_r | pq$. Since $n_r > 1$ and $r > p, q$, we must have $n_r = pq$.

Also Sylow's theorem implies that $n_q \equiv 1 \pmod{q}$ and $n_q | pr$. Since $n_q > 1$ and $q > p$, we must have $n_q \geq r$.

We also have $n_p \equiv 1 \pmod{p}$ and $n_p | qr$ by Sylow's theorem and $n_p > 1$, we must have $n_p \geq q$.

Each Sylow r-subgroup contains $r-1$ elements of order r. Since distinct Sylow r-subgroups intersect trivially, there are $(r-1)n_r = (r-1)pq$ elements of order r in G.

By the similar argument, the number of elements of order either p, q, or r is greater than or equal to

$$(r-1)pq + (q-1)r + (p-1)q = pqr + qr - r - q.$$

Of course, this number must be less than or equal to $|G| = pqr$.

Hence $qr - r - q \leq 0$. This implies that

$$2 < q \leq \frac{r}{r-1} \leq 2$$

and this is a contradiction.

If the Order is an Even Perfect Number, then a Group is not Simple

Problem 74

(a) Show that if a group G has the following order, then it is not simple.

1. 28
2. 496
3. 8128

(b) Show that if the order of a group G is equal to an even ***perfect number*** then the group is not simple.

Hint.

Use Sylow's theorem.

(See the post Sylow's Theorem (summary) to review the theorem.)

Proof.

(a) A group of the following order is not simple

(1) A group of order 28

Note that $28 = 2^2 \cdot 7$. The number n_7 of the Sylow 7-subgroups of G satisfies

$$n_7 \equiv 1 \pmod 7 \text{ and } n_7 | 2^2.$$

Thus, the only possible value is $n_7 = 1$. The unique Sylow 7-subgroup is a proper nontrivial normal subgroup of G, hence G is not simple.

(2) A group of order 496

Note that $496 = 2^4 \cdot 31$. By the same argument as in (1), there is a normal Sylow 31-subgroup in G, hence G is not simple.

(3) A group of order 8128

We have $8128 = 2^6 \cdot 127$, where 127 is a prime number.

Again the same reasoning proves that the group G has the unique normal Sylow 127-subgroup in G, hence G is not simple.

(b) If the order is an even perfect number, a group is not simple

From elementary number theory, all even perfect numbers are of the form

$$2^{p-1}(2^p-1),$$

where p is a prime number and 2^p-1 is also a prime number.

(For a proof, see the post "Even Perfect Numbers and Mersenne Prime Numbers".)

Suppose the order of a group G is $2^{p-1}(2^p-1)$, with prime p, 2^p-1.

Then the number n_{2^p-1} of Sylow (2^p-1)-subgroup satisfies

$$n_{2^p-1} \equiv 1 \pmod{2^p-1} \text{ and } n_{2^p-1} | 2^{p-1}.$$

These force that $n_{2^p-1}=1$.

Therefore the group G contains the unique normal Sylow (2^p-1)-subgroup, hence G is not simple.

Similar problem

For an analogous problem, check out: Groups of order 100, 200. Is it simple?

Comment.

In about 300 BC Euclid showed that a number of the form $2^{p-1}(2^p-1)$ where p and 2^p-1 are prime numbers.

(If 2^p-1 is a prime number, then p must be a prime.)

The converse was proved by Euler in the 18th century. Namely, Euler proved that any even perfect number is of the form $2^{p-1}(2^p-1)$ with prime 2^p-1.

The number of the form 2^p-1 is called a ***Mersenne number*** and if it is a prime number, then it is called a ***Mersenne Prime***.

It is unknown whether there are infinitely many Mersenne prime numbers.

Also it is unknown whether there is an ***odd perfect number***.

Sylow's Theorem (Summary)

In this post we review Sylow's theorem and as an example we solve the following problem.

Problem 64

Show that a group of order 200 has a normal Sylow 5-subgroup.

Review of Sylow's Theorem

One of the important theorems in group theory is Sylow's theorem.

Sylow's theorem is a very powerful tool to solve the classification problem of finite groups of a given order.

In this article, we review several terminologies, the contents of Sylow's theorem, and its corollary.

We also give an example that can be solved using Sylow's theorem.

At the end of this post, the links to various Sylow's theorem problems are given.

We first introduce several definitions.

Definition 1.

Let G be a group and p be a prime number.

1. A group of order p^α for some non-negative integer α is called a ***p-group***.
2. A subgroup of G which is a p-subgroup is called ***p-subgroup***.

Definition 2.

Let G be a finite group of order n. Let p be a prime number dividing n.

Write $n = p^{\alpha}m$, where $\alpha, m \in \mathbb{Z}$ and p does not divide m.

Then any subgroup H of G is called a ***Sylow p-group*** of G if the order of H is p^{α}.

Sylow's theorem

Let G be a finite group of order $p^{\alpha}m$, where the prime number p does not divide m.

1. There exists at least one Sylow p-subgroup of G.
2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that Q is a subgroup of gPg^{-1}.

   In particular, any two Sylow p-subgroups of G are conjugate in G.
3. The number n_p of Sylow p-subgroups of G is

$$n_p \equiv 1 \pmod{p}.$$

   That is, $n_p = pk + 1$ for some $k \in \mathbb{Z}$.
4. The number n_p of Sylow p-subgroup of G is the index of the normalizer $N_G(P)$ in G for any Sylow p-subgroup P, hence n_p divides m.

Corollary

In the notation of the previous theorem, if the number n_p of Sylow p-subgroup of G is $n_p = 1$, then the Sylow p-subgroup is a normal subgroup of G.

Example/Problem.

Now as an example we solve the problem.

Problem.

Show that a group of order 200 has a normal Sylow 5-subgroup.

Solution.

We have the factorization $200 = 2^3 \cdot 5^2$.

By Sylow's theorem the number of Sylow 5-subgroup satisfies $n_5 \equiv 1 \pmod{5}$ and n_5 divides 8.

The numbers satisfies $n_5 \equiv 1 \pmod{5}$ are $n_5 = 1, 6, 11, \cdots$.

Among these numbers, only 1 divides 8.

Thus the only number satisfies both conditions is 1.

Hence $n_5 = 1$ and there is only one Sylow 5-subgroup.

Then by the corollary, the Sylow 5-subgroup is normal.

More Problems on Sylow's theorem

Sylow's theorem is a handy tool to determine the group structure of a finite group.

We list here several problems/examples that can be solved using Sylow's theorem.

All solutions are given in the links below.

- Sylow subgroups of a group of order 33 is normal subgroups
- Group of order pq has a normal Sylow subgroup and solvable
- If the order is an even perfect number, then a group is not simple

- A group of order pqr contains a normal subgroup
- Groups of order 100, 200. Is it simple?
- If a Sylow subgroup is normal in a normal subgroup, it is a normal subgroup
- subgroup containing all p-Sylow subgroups of a group
- A group of order 20 is solvable
- Non-abelian group of order pq and its Sylow subgroups
- Prove that a Group of Order 217 is Cyclic and Find the Number of Generators
- Every Group of Order 20449 is an Abelian Group
- Every Sylow 11-Subgroup of a Group of Order 231 is Contained in the Center $Z(G)$
- Every Group of Order 72 is Not a Simple Group

All the Conjugacy Classes of the Dihedral Group D_8 of Order 8

Problem 54

Determine all the conjugacy classes of the dihedral group

$$D_8 = \langle r, s \mid r^4 = s^2 = 1, sr = r^{-1}s \rangle$$

of order 8.

Hint.

You may directly compute the conjugates of each element
but we are going to use the following theorem to simplify the computations.

Theorem.

The number of conjugates of an element g in a group is the index $|G : C_G(s)|$ of the centralizer of s.

Solution.

Let us denote $G = D_8$.
Let K_x be the conjugacy class in G containing the element x.

Note that $\langle r \rangle < C_G(r) \subsetneq G$ and the order $|\langle r \rangle| = 4$.
Hence we must have $C_G(r) = \langle r \rangle$.
Thus the element r has $|G : C_G(r)| = 2$ conjugates in G.
Since $srs^{-1} = r^3$, the conjugacy class K_r containing r is $\{r, r^3\}$.

Since $\langle s \rangle < C_G(s) \subsetneq G$ and $|\langle s \rangle| = 2$, we have either $C_G(s) = \langle s \rangle$ or $|C_G(s)| = 4$.
Since $r^2 s = sr^2$, we must have $|C_G(s)| = 4$ and hence the conjugacy class K_s containing s has
$|G : C_G(s)| = 2$ elements.
Since $rsr^{-1} = sr^2$, we have $K_s = \{s, sr^2\}$.

We know the center is $Z(G) = \{1, r^2\}$ by Problem Centralizer, normalizer, and center of the dihedral group D8.
Thus $K_1 = \{1\}$ and $K_{r^2} = \{r^2\}$.

The remaining elements sr and sr^3 should be in the same conjugacy class (otherwise these elements are in the center), thus $K_{sr} = \{sr, sr^3\}$.

In summary, the conjugacy classes of the dihedral group are

$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}.$$

Centralizer, Normalizer, and Center of the Dihedral Group D_8

Problem 53

Let D_8 be the dihedral group of order 8.
Using the generators and relations, we have

$$D_8 = \langle r, s \mid r^4 = s^2 = 1, sr = r^{-1}s \rangle.$$

(a) Let A be the subgroup of D_8 generated by r, that is, $A = \{1, r, r^2, r^3\}$.
Prove that the centralizer $C_{D_8}(A) = A$.
(b) Show that the normalizer $N_{D_8}(A) = D_8$.
(c) Show that the center $Z(D_8) = \langle r^2 \rangle = \{1, r^2\}$, the subgroup generated by r^2.

Definitions (centralizer, normalizer, center).

Recall the definitions.

1. The ***centralizer*** $C_{D_8}(A)$ is a subgroup of D_8 whose elements commute with A.
   That is $C_{D_8}(A) = \{g \in D_8 \mid gxg^{-1} = x \text{ for all } x \in A\}$.
2. The ***normalizer*** $N_{D_8}(A)$ is a subgroup of D_8 defined as
   $N_{D_8}(A) = \{g \in D_8 \mid gxg^{-1} \in A \text{ for any } x \in A\}$.
3. The ***center*** $Z(D_8)$ is a subgroup of D_8 whose elements commute with all elements of D_8.
   That is, $Z(D_8) = \{g \in D_8 \mid gxg^{-1} = x \text{ for all } x \in D_8\}$.

Proof.

(a) The centralizer $C_{D_8}(A) = A$

Since any power of r commutes with each other we have $A < C_{D_8}(A)$.
Since $sr = r^{-1}s$ and $r^{-1}s \neq rs$ (otherwise $r^2 = 1$), we see that $s \notin C_{D_8}(A)$.
This also implies that any element of the form $r^a s \in D_8$ is not in $C_{D_8}(A)$. In fact, if $r^a s \in C_{D_8}(A)$, then $s = (r^{-a}) \cdot (r^a s)$ is also in $C_{D_8}(A)$ because $r^{-a} \in C_{D_8}(A)$ and $C_{D_8}(A)$ is a group.
This is a contradiction. Therefore $C_{D_8}(A) = A$.

(b) The normalizer $N_{D_8}(A) = D_8$

In general, the centralizer of a subset is contained in the normalizer of the subset. From this fact we have $A = C_{D_8}(A) < N_{D_8}(A)$.
Thus it suffices to show that the other generator $s \in D_8$ belongs to $N_{D_8}(A)$.
We have $sr^a s^{-1} = r^{-1}ss^{-1} = r^{-1} \in A$ using the relation $sr = r^{-1}s$.
Thus $s \in N_{D_8}(A)$ as required.

(c) The center $Z(D_8) = \langle r^2 \rangle = \{1, r^2\}$

The center $Z(D_8)$ is contained in the centralizer $C_{D_8}(A) = A$.
Since $rsr^{-1} = sr^2 \neq s$ and $r^3 s (r^3)^{-1} = r^{-1}sr = sr^2 \neq s$, the elements r and r^3 are not in the center $Z(D_8)$.

On the other hand, we have $sr^2 = r^{-1}sr = r^{-2}s = r^2 s$. Thus $r^2 s(r^2)^{-1} = s$ and $r^2 \in Z(D_8)$.
Therefore we have $Z(D_8) = \{1, r^2\}$.

Dihedral Group and Rotation of the Plane

Problem 52

Let n be a positive integer. Let D_{2n} be the dihedral group of order $2n$. Using the generators and the relations, the dihedral group D_{2n} is given by

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle.$$

Put $\theta = 2\pi/n$.

(a) Prove that the matrix $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ is the matrix representation of the linear transformation T which rotates the x-y plane about the origin in a counterclockwise direction by θ radians.

(b) Let $\mathrm{GL}_2(\mathbb{R})$ be the group of all 2×2 invertible matrices with real entries. Show that the map $\rho : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ defined on the generators by

$$\rho(r) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \text{ and } \rho(s) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

extends to a homomorphism of D_{2n} into $\mathrm{GL}_2(\mathbb{R})$.

(c) Determine whether the homomorphism ρ in part (b) is injective and/or surjective.

Hint.

1. For (a), consider the unit vectors of the plane and consider where do the unit vector go by the linear transformation T.
2. Show that $\rho(r)$ and $\rho(s)$ satisfy the same relations as D_{2n}.
3. Consider the determinant.

Proof.

(a) The matrix representation of the linear transformation T

Let $\mathbf{e}_1, \mathbf{e}_2$ be the standard basis of the plane $\mathbb{R}^2$. That is

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Then by the θ rotation $\mathbf{e}_1$ moves to the point $\begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}$ and $\mathbf{e}_2$ moves to the point $\begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}$.
Therefore the matrix representation of T is the matrix $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.
(Recall that if T is a linear transformation from a vector space V to itself with a basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$, its representation matrix is given by the matrix $[T(\mathbf{e}_1) \cdots T(\mathbf{e}_n)]$ whose i-th column is the vector $T(\mathbf{e}_i)$.)

(b) ρ is a homomorphism of D_{2n} into $\mathrm{GL}_2(\mathbb{R})$

Any element $x \in D_{2n}$ can be written as $x = r^a s^b$ using the relations.

Then we define the value of ρ on x by

$$\rho(x) := \rho(r)^a \rho(s)^b = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^a \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^b.$$

We need to show that this is well defined.

To do this, we show that $\rho(r)$ and $\rho(s)$ satisfy the same relation as D_{2n}.

We have

$$\rho(r)^n = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos(n\theta) & -\sin(n\theta) \\ \sin(n\theta) & \cos(n\theta) \end{bmatrix} = I_2,$$

where I_2 is the 2×2 identity matrix. Also we have $\rho(s) = I_2$.

Finally, we compute

$$\begin{aligned} \rho(r)\rho(s)\rho(r) &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \\ &= \begin{bmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \\ &= \begin{bmatrix} 0 & \sin^2\theta + \cos^2\theta \\ \cos^2 + \sin^2\theta & 0 \end{bmatrix} = I_2 \end{aligned}$$

Therefore, the extension of ρ does not depend on the expression of $x = r^a s^b$.

(c) Determine whether the homomorphism ρ in part (b) is injective and/or surjective.

We first show that ρ is injective.

Suppose that we have $\rho(x) = I_2$ for $x \in D_{2n}$. Write $x = r^a s^b$.

Then we have $\rho(r)^a \rho(s)^b = I_2$.

We compute the determinant of both sides and get

$$\det(\rho(r))^a \det(\rho(s))^b = 1.$$

Since $\det(\rho(r)) = 1$ and $\det(\rho(s)) = -1$ we have $(-1)^b = 1$, thus b must be even.

Then $x = r^a$ since the order of s is two.

Then $\rho(r)^a = I_2$ implies that $r\theta = 2\pi m$ for some $m \in \mathbb{Z}$.

Hence $r = nm$ and we obtain $x = r^{nm} = 1$ since the order of r is n. Therefore the kernel of ρ is trivial, hence the homomorphism ρ is injective.

As the argument shows, the determinant of $\rho(x)$ is either ± 1. The homomorphism ρ is not surjective since $\mathrm{GL}_2(\mathbb{R})$ contains elements with determinants not equal to ± 1.

Normal Subgroups Intersecting Trivially Commute in a Group

Problem 49

Let A and B be normal subgroups of a group G. Suppose $A \cap B = \{e\}$, where e is the unit element of the group G.
Show that for any $a \in A$ and $b \in B$ we have $ab = ba$.

Hint.

Consider the commutator of a and b, that is, $aba^{-1}b^{-1}$.

Solution.

Consider the product $aba^{-1}b^{-1}$. Since A is normal in G, the element $ba^{-1}b^{-1} \in A$ as it is the conjugate of $a^{-1} \in A$.
Thus $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in A$.
Similarly, since B is normal in G, we have $aba^{-1} \in B$.
Hence $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B$.
Therefore $aba^{-1}b^{-1} \in A \cap B = \{e\}$ and we see that $aba^{-1}b^{-1} = e$, thus $ab = ba$.

The Center of the Symmetric group is Trivial if $n > 2$

Problem 31

Show that the center $Z(S_n)$ of the symmetric group with $n \geq 3$ is trivial.

Steps/Hint

1. Assume $Z(S_n)$ has a non-identity element σ.
2. Then there exist numbers i and j, $i \neq j$, such that $\sigma(i) = j$
3. Since $n \geq 3$ there exists another number k.
4. Let $\tau = (ik) \in S_n$ and find a contradiction.

Proof.

Seeking a contradiction, assume that the center $Z(S_n)$ is non-trivial.
Then there exists a non-identity element $\sigma \in Z(G)$.
Since σ is a non-identity element, there exist numbers i and j, $i \neq j$, such that $\sigma(i) = j$.
Now by assumption $n \geq 3$, there exists another number k that is different from i and j. Let us consider the transposition $\tau = (ik) \in S_n$.
Then we have

$$\tau\sigma(i) = \tau(j) = j$$
$$\sigma\tau(i) = \sigma(k) \neq j$$

since $\sigma(i) = j$ and σ is bijective.
Thus $\tau\sigma \neq \sigma\tau$ but this contradicts that $\sigma \in Z(S_n)$.
Therefore $Z(S_n)$, $n \geq 3$, must be trivial.

Group of Order pq is Either Abelian or the Center is Trivial

Problem 30

Let G be a group of order $|G| = pq$, where p and q are (not necessarily distinct) prime numbers.
Then show that G is either abelian group or the center $Z(G) = 1$.

Hint.

Use the result of the problem "If the Quotient by the Center is Cyclic, then the Group is Abelian".

Proof.

Since the center $Z(G)$ is a (normal) subgroup of G, the order of $Z(G)$ divides the order of G by Lagrange's theorem.
Thus the order of $Z(G)$ is one of $1, p, q, pq$.

Suppose that $Z(G) \neq 1$.

Then the order of the quotient group $G/Z(G)$ is one of $1, p, q$.

Hence the group $G/Z(G)$ is a cyclic group.

We conclude that G is abelian group by Problem "If the Quotient by the Center is Cyclic, then the Group is Abelian".

Therefore, either $Z(G) = 1$ or G is abelian.

Basic Properties of Characteristic Groups

Problem 22

Definition (automorphism).

An isomorphism from a group G to itself is called ***automorphism*** of G.
The set of all automorphism is denoted by $\mathrm{Aut}(G)$.

Definition (characteristic subgroup).

A subgroup H of a group G is called ***characteristic*** in G if for any $\phi \in \mathrm{Aut}(G)$, we have $\phi(H) = H$. In words, this means that each automorphism of G maps H to itself.
Prove the followings.
(a) If H is characteristic in G, then H is a normal subgroup of G.
(b) If H is the unique subgroup of G of a given order, then H is characteristic in G.
(c) Suppose that a subgroup K is characteristic in a group H and H is a normal subgroup of G. Then K is a normal subgroup in G.

Proof.

(a) If H is characteristic in G, then H is a normal subgroup of G.

For each $g \in G$, define a map $\phi_g : G \to G$ defined by $\phi_g(x) = gxg^{-1}$. This is an automorphism of G with the inverse $\phi_{g^{-1}}$.
Since H is characteristic, we have $\phi_g(H) = H$, equivalently we have $gHg^{-1} = H$.
Therefore H is a normal subgroup of G.

(b) If H is the unique subgroup of G of a given order, then H is characteristic in G.

For any automorphism $\phi \in \mathrm{Aut}(G)$, we have $\phi(H) \subset \phi(G) = G$ and $|H| = |\phi(H)|$. The uniqueness of H implies that $H = \phi(H)$ and thus H is characteristic.

(c) K is characteristic in H and H is normal$G$. Then K is a normal subgroup in G.

For each $g \in G$, consider the automorphism ϕ_g of G defined in the proof of (a). Since $H \triangleleft G$, we have $\phi_g(H) = H$.
Hence the restriction $\phi_g|_H$ belongs to $\mathrm{Aut}(H)$.
Now since K is characteristic in H, we have $\phi_g|_H(K) = K$, or equivalently we have $gKg^{-1} = K$ and K is normal in G.

Comment.

Let K, H be subgroups of G. Suppose that K is a normal subgroup of H, and H is a normal subgroup of G.
In general, we cannot conclude that K is a normal subgroup of G.
(For example, consider the dihedral group D_8 of order 8.)

Thus, normality is not transitive.

Part (c) of the problem claims that if in addition, K is characteristic in H, then K is normal in G.

Related Question.

Check out the post Equivalent definitions of characteristic subgroups. Center is characteristic. for more problems about characteristic subgroups.

A Group of Order the Square of a Prime is Abelian

Problem 20

Suppose the order of a group G is p^2, where p is a prime number.

Show that

(a) the group G is an abelian group, and

(b) the group G is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ without using the fundamental theorem of abelian groups.

Hint.

Review the following problems.

1. The center of a p-group is not trivial (post 1)
2. If the quotient by the center is cyclic, then the group is abelian (post 2)

Proof.

(a) A group of order p^2 is abelian.

Since G is a p-group, its center is not trivial (see post 1 for a proof.)

If the center $Z(G) = G$, then G is abelian so assume that $Z(G)$ is a proper nontrivial subgroup. Then the center must have order p and it follows that the order of the quotient $G/Z(G)$ is p, hence $G/Z(G)$ is a cyclic group.

Thus G is abelian by the fact proved in post 2.

(b) The group G is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Let $x \in G$ be any nontrivial element of G. If $x \in G$ has order p^2, then $G = \langle x \rangle \cong \mathbb{Z}/p^2\mathbb{Z}$. If the order of x is p, then take $y \in G \setminus \langle x \rangle$. Then the order of y is also p.

Since the subgroup $\langle x, y \rangle$ generated by x and y is properly bigger than the subgroup $\langle x \rangle$, we must have $G = \langle x, y \rangle$.

We claim that $\langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle$.

Define a map $f : \langle x \rangle \times \langle y \rangle \to \langle x, y \rangle$ by sending (x^a, y^b) to $x^a y^b$. This is a group homomorphism because for any elements (x^{a_1}, y^{b_1}) and (x^{a_2}, y^{b_2}), we have

$$\begin{aligned} f\left((x^{a_1}, y^{b_1})(x^{a_2}, y^{b_2})\right) &= f\left(x^{a_1+a_2}, y^{b_1+b_2}\right) = x^{a_1+a_2} y^{b_1+b_2} \\ &= x^{a_1} y^{b_1} x^{a_2} y^{b_2} = f\left((x^{a_1}, y^{b_1})\right) f\left((x^{a_2}, y^{b_2})\right). \end{aligned}$$

Here we used the result of part (a) that G is abelian in the third equality.

We claim that the homomorphism f is injective.
If $f\left(x^a, y^b\right)=1$, we have $x^a=y^b$ but since $y \notin\langle x\rangle$ we must have $a=b=0$. Thus the kernel is trivial, hence f is injective.
Since $\langle x\rangle \times\langle y\rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has order p^2 and f is injective, the homomorphism must be surjective as well, hence it is an isomorphism.

If the Quotient by the Center is Cyclic, then the Group is Abelian

Problem 18

Let $Z(G)$ be the center of a group G.
Show that if $G/Z(G)$ is a cyclic group, then G is abelian.

Steps.

1. Write $G/Z(G)=\langle \bar{g} \rangle$ for some $g \in G$.
2. Any element $x \in G$ can be written as $x=g^a z$ for some $z \in Z(G)$ and $a \in \mathbb{Z}$.
3. Using this expression, show that $xy=yx$ for any $x, y \in G$.

Proof.

Since the quotient group $G/Z(G)$ is cyclic, it is generated by one element.
Let $g \in G$ be an element such that $\bar{g}=gZ(G)$ is a generator of $G/Z(G)$. Namely, $\langle \bar{g} \rangle = G/Z(G)$.
Then for any element $x \in G$, we have $\bar{x} \in G/Z(G)=\langle \bar{g} \rangle$ and hence $\bar{x}=\bar{g}^a$ for some $a \in \mathbb{Z}$.
It follows that any element of G can be written as $x=g^a z$ for some $z \in Z(G)$ and $a \in \mathbb{Z}$.
Take any two elements $x, y \in G$ and write $x=g^a z$ and $y=g^b w$, where $a, b \in \mathbb{Z}$ and $z, w \in Z(G)$.
Then we claim that $xy=yx$. To see this we calculate as follows.

$$
\begin{aligned}
xy &= g^a z g^b w \\
&= g^a g^b z w && \text{since } z \in Z(G) \\
&= g^{a+b} w z && \text{since } w \in Z(G) \\
&= g^b g^a w z \\
&= g^b w g^a z && \text{since } w \in Z(G) \\
&= yx.
\end{aligned}
$$

Since the product of any two elements of G is commutative, we conclude that G is abelian.

A Group with a Prime Power Order Elements Has Order a Power of the Prime.

Problem 17

Let p be a prime number. Suppose that the order of each element of a finite group G is a power of p. Then prove that G is a p-group. Namely, the order of G is a power of p.

Hint.

You may use *Sylow's theorem*.
For a review of Sylow's theorem, please check out the post Sylow's Theorem (summary).

Proof.

If G is a trivial group, then the claim is trivial. So assume that $|G|>1$.

Seeking a contradiction, suppose that $|G| = p^n m$ for some $n, m \in \mathbb{Z}$ and p and $m > 1$ are relatively prime.
Let l be a prime factor of m. Then by Sylow's theorem, there exists a Sylow l-subgroup of G.
The order of a nontrivial element of this subgroup is divisible by the prime l and this contradicts that each element has order power of p since l and p are relatively prime.

Comment.

If we assume Sylow's theorem, then the proof of this problem is straightforward.
How about proving it more directly (without using Sylow's theorem)?

Any Subgroup of Index 2 in a Finite Group is Normal

Problem 16

Show that any subgroup of index 2 in a group is a normal subgroup.

Hint.

1. Left (right) cosets partition the group into disjoint sets.
2. Consider both left and right cosets.

Proof.

Let H be a subgroup of index 2 in a group G.
Let $e \in G$ be the identity element of G.
To prove that H is a normal subgroup, we want to show that for any $g \in G$, $gH = Hg$.
If $g \in H$, then this is true. So we assume that $g \notin H$.
Note that left cosets partition G into two disjoint sets since the index is 2.
Since $g \notin H$, these are eH and gH. (If $gH = H$, then $g \in H$.)
Similarly right cosets partition G into two disjoint sets.
These disjoint right cosets are He and Hg.
Because of these partitions, we have as sets

$$gH = G - eH = G - H = G - He = Hg.$$

Therefore H is a normal subgroup in G.

The Center of a p-Group is Not Trivial

Problem 10

Let G be a group of order $|G| = p^n$ for some $n \in \mathbb{N}$.
(Such a group is called a *p-group*.)
Show that the center $Z(G)$ of the group G is not trivial.

Hint.

Use the class equation.

Proof.

If $G = Z(G)$, then the statement is true. So suppose that $G \neq Z(G)$.
Then by *the class equation*, we have

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|,$$

where g_i are representatives of the distinct conjugacy class not contained in the center $Z(G)$, and $C_G(g_i)$ is the centralizer of g_i.
(Since we are assuming that $G \neq Z(G)$ such g_i exist.)

Since $g_i \notin Z(G)$, the groups $C_G(g_i)$ are proper subgroups of G and hence p divides $|G : C_G(g_i)|$. Of course p divides $|G|$, thus p should divide $|Z(G)|$ as well.
Therefore the center $Z(G)$ cannot be trivial.

Comment.

This problems is a simple/nice application of the class equation of group theory. The only information about the group is that its order is a prime power. From this we can conclude that the center of the group is not trivial.

A Group of Linear Functions

Problem 6

Define the functions $f_{a,b}(x) = ax + b$, where $a, b \in \mathbb{R}$ and $a > 0$.
Show that $G := \{f_{a,b} \mid a, b \in \mathbb{R}, a > 0\}$ is a group . The group operation is function composition.

Steps.

Check one by one the followings.

1. The group operation on G is associative.
2. Determine/guess the identity element and show that it is in fact the identity element.
3. Determine/guess the inverse of each element and show that it is in fact the inverse.

Proof.

The product of f_{a_1,b_1} and f_{a_2,b_2} is given by

$$f_{a_2,b_2}(x) \circ f_{a_1,b_1}(x) = a_2(a_1x + b_1) + b_2 = a_2a_1x + a_2b_1 + b_2.$$

Since the group operation is function composition, it is associative.

The identity element is $f_{1,0} = x$ since for any $f_{a,b} \in G$, we have

$$f_{a,b}(x) \circ f_{1,0}(x) = af_{1,0}(x) + b = ax + b = f_{a,b}(x)$$

and

$$f_{1,0}(x) \circ f_{a,b}(x) = x \circ f_{a,b}(x) = f_{a,b}(x).$$

Now we find the inverse of f_{a_1,b_1}.
If $f_{a_2,b_2}(x) \circ f_{a_1,b_1}(x) = x(= f_{1,0})$, then we should have $a_2a_1 = 1$ and $a_2b_1 + b_2 = 0$. Solving these, we obtain $a_2 = 1/a_1 > 0$ and $b_2 = -a_2b_1 = -b_1/a_1$.
Thus our candidate of the inverse $f_{a,b}^{-1}$ is

$$f_{1/a_1,-b_1/a_1} = x/a_1 - b_1/a_1.$$

In fact it is the inverse since it also satisfies

$$f_{a_1,b_1} \circ f_{1/a_1,-b_1/a_1} = a_1(x/a_1 - b_1/a_1) + b_1 = x - b_1 + b_1 = x.$$

Thus $f_{a,b}^{-1} = f_{1/a_1,-b_1/a_1}$ and we conclude that G is a group.

The Quotient by the Kernel Induces an Injective Homomorphism

Problem 4

Let G and G' be a group and let $\phi : G \to G'$ be a group homomorphism.
Show that ϕ induces an injective homomorphism from $G/\ker\phi \to G'$.

Outline.

1. Define $\tilde{\phi}([g]) = \phi(g)$ and show that this is well-defined.
2. Show that $\tilde{\phi}$ is a homomorphism.
3. Show that $\tilde{\phi}$ is injective.

Proof.

Define the map $\tilde{\phi} : G/\ker\phi \to G'$ by sending $[g]$ to $\phi(g)$. Here $[g]$ is the element of $G/\ker\phi$ represented by $g \in G$.

We need to show that this is well-defined.
Namely, we need to show that $\tilde{\phi}$ does not depend on the choice of representative.
So suppose $[g] = [h]$ for $g, h \in G$. Then we have $x := gh^{-1} \in \ker\phi$. Thus we have

$$e' = \phi(x) = \phi(gh^{-1}) = \phi(g)\phi(h)^{-1},$$

where $e' \in G'$ is the identity element of G'.
Here the third equality follows because ϕ is a homomorphism.
Hence we obtain $\phi(g) = \phi(h)$, equivalently $\tilde{\phi}([g]) = \tilde{\phi}([h])$. Thus $\tilde{\phi}$ is well-defined.

Now we show that $\tilde{\phi} : G/\ker\phi \to G'$ is a homomorphism. Let $[g], [h] \in G/\ker\phi$. Then we have

$$\tilde{\phi}([g][h]) = \tilde{\phi}([gh]) = \phi(gh) = \phi(g)\phi(h) = \tilde{\phi}([g])\tilde{\phi}([h])$$

and $\tilde{\phi}$ is a homomorphism.

Finally, we prove that $\tilde{\phi}$ is injective. Suppose that $\tilde{\phi}([g]) = e'$. Then this means $\phi(g) = e'$, hence $g \in \ker\phi$.
Thus $[g] = [e]$, where e is the identity element of G.
Hence $\tilde{\phi}$ is injective and the proof is complete.

A Condition that a Commutator Group is a Normal Subgroup

Problem 3

Let H be a normal subgroup of a group G.
Then show that $N := [H, G]$ is a subgroup of H and $N \triangleleft G$.
Here $[H, G]$ is a subgroup of G generated by commutators $[h, k] := hkh^{-1}k^{-1}$.
In particular, the commutator subgroup $[G, G]$ is a normal subgroup of G

Proof.

First, we show that $N = [H, G]$ is a subgroup of H.

A generator of N is of the form either $hgh^{-1}g^{-1}$ or $ghg^{-1}h^{-1}$, where $h \in H$ and $g \in G$. Since H is normal in G, we see that these are elements in H. Thus $N < H$.

Next, we show that N is normal in G.

Let $x = hgh^{-1}g^{-1}$ be a generator element of N.

Then for any $a \in G$, we have

$$axa^{-1} = ahgh^{-1}g^{-1}a^{-1} = (aha^{-1})(aga^{-1})(ah^{-1}a^{-1})(ag^{-1}a^{-1}) \in [H, G].$$

Similarly, if x is a generator of the form $ghg^{-1}h^{-1}$, then we see that $ghg^{-1}h^{-1} \in [H, G]$ by the same argument.

Thus the conjugate of a generator of N by $a \in G$ stays in N.

Now any element $x \in N$ is of the form $x = x_1x_2 \cdots x_n$, where x_i are generators of N.

For any $a \in H$, we have

$$axa^{-1} = ax_1x_2 \cdots x_na^{-1} = (ax_1a^{-1})(ax_2a^{-1}) \cdots (ax_na^{-1}) \in [H, G].$$

Thus $N \triangleleft G$.

In particular, we apply the result to $H = G$. Then we see that the commutator subgroup $[G, G]$ is a normal subgroup of G.

Related Question.

You might also be interested in the problems:

- A condition that a commutator group is a normal subgroup
- Non-abelian simple group is equal to its commutator subgroup

Problems in Ring Theory

Ring Homomorphisms and Radical Ideals

Problem 624

Let R and R' be commutative rings and let $f : R \to R'$ be a ring homomorphism.
Let I and I' be ideals of R and R', respectively.

(a) Prove that $f(\sqrt{I}) \subset \sqrt{f(I)}$.
(b) Prove that $\sqrt{f^{-1}(I')} = f^{-1}(\sqrt{I'})$
(c) Suppose that f is surjective and $\ker(f) \subset I$. Then prove that $f(\sqrt{I}) = \sqrt{f(I)}$

Proof.

(a) Prove that $f(\sqrt{I}) \subset \sqrt{f(I)}$.

Let $x \in f(\sqrt{I})$ be an arbitrary element. Then there is $a \in \sqrt{I}$ such that $f(a) = x$. As $a \in \sqrt{I}$, there exists a positive integer n such that $a^n \in I$.
It follows that we have

$$x^n = f(a)^n = f(a^n) \in f(I).$$

This implies that $x \in \sqrt{f(I)}$.
Hence we have $f(\sqrt{I}) \subset \sqrt{f(I)}$.

(b) Prove that $\sqrt{f^{-1}(I')} = f^{-1}(\sqrt{I'})$

$(\subset)$ Let $x \in \sqrt{f^{-1}(I')}$. Then there is a positive integer n such that $x^n \in f^{-1}(I')$ and thus $f(x^n) \in I'$.
As f is a ring homomorphism, it follows that $f(x)^n = f(x^n) \in I'$.
Hence $f(x) \in \sqrt{I'}$, and then $x \in f^{-1}(\sqrt{I'})$.
This proves that $\sqrt{f^{-1}(I')} \subset f^{-1}(\sqrt{I'})$.

$(\supset)$ Let $x \in f^{-1}(\sqrt{I'})$. Then $f(x) \in \sqrt{I'}$. It follows that there exists a positive integer n such that $f(x^n) = f(x)^n \in I'$.
Hence $x^n \in f^{-1}(I')$, and we deduce that $x \in \sqrt{f^{-1}(I')}$.
This proves that $f^{-1}(\sqrt{I'}) \subset \sqrt{f^{-1}(I')}$.
Combining this with the previous inclusion yields that $\sqrt{f^{-1}(I')} = f^{-1}(\sqrt{I'})$.

(c) Suppose that f is surjective and $\ker(f) \subset I$. Then prove that $f(\sqrt{I}) = \sqrt{f(I)}$

We now suppose that f is surjective and $\ker(f) \subset I$. We proved $f(\sqrt{I}) \subset \sqrt{f(I)}$ in part (a). To show the reverse inclusion, let $x \in \sqrt{f(I)} \subset R'$.
Then there is a positive integer n such that $x^n \in f(I)$.
So there exists $a \in I$ such that $f(a) = x^n$.
Since $f : R \to R'$ is surjective, there exists $y \in R$ such that $f(y) = x$.
Then we have

$$f(a) = x^n = f(y)^n = f(y^n),$$

and hence $f(a - y^n) = 0$.
Thus $a - y^n \in \ker(f) \subset I$ by assumption.
As $a \in I$, it follows that $y^n \in I$ as well.
We deduce that $y \in \sqrt{I}$ and

$$x = f(y) \in f(\sqrt{I}),$$

which completes the proof that $\sqrt{f(I)} \subset f(\sqrt{I})$.

Putting together this inclusion and the inclusion in (a) yields the required equality $f(\sqrt{I}) = \sqrt{f(I)}$.

Example of an Element in the Product of Ideals that Cannot be Written as the Product of Two Elements

Problem 623

Let $I = (x, 2)$ and $J = (x, 3)$ be ideal in the ring $\mathbb{Z}[x]$.
(a) Prove that $IJ = (x, 6)$.
(b) Prove that the element $x \in IJ$ cannot be written as $x = f(x)g(x)$, where $f(x) \in I$ and $g(x) \in J$.

Hint.

If $I = (a_1, \dots, a_m)$ and $J = (b_1, \dots, b_n)$ are ideals in a commutative ring, then we have

$$IJ = (a_i b_j),$$

where $1 \leq i \leq m$ and $1 \leq j \leq n$.

Proof.

(a) Prove that $IJ = (x, 6)$.

Note that the product ideal IJ is generated by the products of generators of I and J, that is, $x^2, 2x, 3x, 6$. That is, $IJ = (x^2, 2x, 3x, 6)$.
It follows that IJ contains $x = 3x - 2x$ as well. As the first three generators can be generated by x, we deduce that $IJ = (x, 6)$.

(b) Prove that the element $x \in IJ$ cannot be written as $x = f(x)g(x)$, where $f(x) \in I$ and $g(x) \in J$.

Assume that $x = f(x)g(x)$ for some $f(x) \in I$ and $g(x) \in J$.
As $\mathbb{Z}[x]$ is a UFD, we have either

$$f(x) = \pm x, g(x) = \pm 1, \text{ or } f(x) = \pm 1, g(x) = \pm x.$$

In the former case, we have $1 \in J$ and hence $J = \mathbb{Z}[x]$, which is a contradiction.
Similarly, in the latter case, we have $1 \in I$ and hence $I = \mathbb{Z}[x]$, which is a contradiction.
Thus, in either case, we reached a contradiction.
Hence, x cannot be written as the product of elements in I and J.

Comment.

Let I and J be an ideal of a commutative ring R.
Then the product of ideals I and J is defined to be

$$IJ := \{\sum_{i=1}^{k} a_i b_i \mid a_i \in I, b_i \in J, k \in \mathbb{N}\}.$$

The above problems shows that in general, there are elements in the product IJ that cannot be expressed simply as ab for $a \in I$ and $b \in J$.

Is the Set of Nilpotent Element an Ideal?

Problem 620

Is it true that a set of nilpotent elements in a ring R is an ideal of R?
If so, prove it. Otherwise give a counterexample.

Proof.

We give a counterexample.

Let R be the noncommutative ring of 2×2 matrices with real coefficients.

Consider the following matrices A, B in R.

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Direct computation shows that A^2 and B^2 are the zero matrix, hence A, B are nilpotent elements.

However, the sum $A + B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is not nilpotent as we have

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{cases} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \text{if } n \text{ is odd} \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \text{if } n \text{ is even.} \end{cases}$$

Hence the set of nilpotent elements in R is not an ideal as it is not even an additive abelian group.

Comment.

If a ring R is commutative, then it is true that the set of nilpotent elements form an ideal, which is called the **nilradical** of R.

Boolean Rings Do Not Have Nonzero Nilpotent Elements

Problem 618

Let R be a commutative ring with 1 such that every element x in R is idempotent, that is, $x^2 = x$. (Such a ring is called a **Boolean ring**.)

(a) Prove that $x^n = x$ for any positive integer n.

(b) Prove that R does not have a nonzero nilpotent element.

Proof.

(a) Prove that $x^n = x$ for any positive integer n.

By assumption, $x^n = x$ is true for $n = 1, 2$.

Suppose that $x^k = x$ for some $k \geq 2$ (induction hypothesis).

Then we have

$$\begin{aligned} x^{k+1} &= xx^k \\ &= xx && \text{by induction hypothesis} \\ &= x^2 = x && \text{by assumption.} \end{aligned}$$

Thus, we conclude that $x^n = x$ for any positive integer n by induction.

(b) Prove that R does not have a nonzero nilpotent element.

Let x be a nilpotent element in R. That is, there is a positive integer n such that $x^n = 0$.

It follows from part (a) that $x = x^n = 0$.

Thus every nilpotent element in R is 0.

If the Localization is Noetherian for All Prime Ideals, Is the Ring Noetherian?

Problem 617

Let R be a commutative ring with 1.

Suppose that the localization $R_{\mathfrak{p}}$ is a Noetherian ring for every prime ideal $\mathfrak{p}$ of R.

Is it true that A is also a Noetherian ring?

Proof.

The answer is no. We give a counterexample.

Let

$$R = \prod_{i=1}^{\infty} R_i,$$

where $R_i = \mathbb{Z}/2\mathbb{Z}$.

As R is not finitely generated, it is not Noetherian.

Note that every element $x \in R$ is idempotent, that is, we have $x^2 = x$.

Let $\mathfrak{p}$ be a prime ideal in R.

Then $R/\mathfrak{p}$ is a domain and we have $x^2 = x$ for any $x \in R/\mathfrak{p}$.

It follows that $x = 0, 1$ and $R/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$.

This also shows that every prime ideal in R is maximal.

Now let us determine the localization $R_{\mathfrak{p}}$.

As the prime ideal $\mathfrak{p}$ does not contain any proper prime ideal (since every prime is maximal), the unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ of $R_{\mathfrak{p}}$ contains no proper prime ideals.

Recall that in general the intersection of all prime ideals is the ideal of all nilpotent elements.

Since $R_{\mathfrak{p}}$ does not have any nonzero nilpotent element, we see that $\mathfrak{p}R_{\mathfrak{p}} = 0$.

(Remark: every Boolean ring has no nonzero nilpotent elements.)

It follows that $R_{\mathfrak{p}}$ is a filed, in particular an integral domain.

As before, since every element x of $R_{\mathfrak{p}}$ satisfies $x^2 = x$, we conclude that $x = 0, 1$ and $R_{\mathfrak{p}} \cong \mathbb{Z}/2\mathbb{Z}$.

Since a field is Noetherian the localization $R_{\mathfrak{p}}$ is Noetherian for every prime ideal $\mathfrak{p}$ of R.

In summary, R is not a Noetherian ring but the localization $R_{\mathfrak{p}}$ is Noetherian for every prime ideal $\mathfrak{p}$ of R.

A Ring is Commutative if Whenever $ab = ca$, then $b = c$

Problem 615

Let R be a ring and assume that whenever $ab = ca$ for some elements $a, b, c \in R$, we have $b = c$.

Then prove that R is a commutative ring.

Proof.

Let x, y be arbitrary elements in R. We want to show that $xy = yx$.

Consider the identity

$$y(xy) = (yx)y.$$

This can be written as $ab = ca$ if we put $a = y, b = xy, c = yx$.

It follows from the assumption that we have $b = c$.

Equivalently, we have $xy = yx$.

As this is true for any $x, y \in R$, we conclude that R is a commutative ring.

If Every Proper Ideal of a Commutative Ring is a Prime Ideal, then It is a Field.

Problem 598

Let R be a commutative ring with 1.

Prove that if every proper ideal of R is a prime ideal, then R is a field.

Proof.

As the zero ideal (0) of R is a proper ideal, it is a prime ideal by assumption.

Hence $R = R/\{0\}$ is an integral domain.

Let a be an arbitrary nonzero element in R.

We prove that a is invertible.

Consider the ideal (a^2) generated by the element a^2.

If $(a^2) = R$, then there exists $b \in R$ such that $1 = a^2 b$ as $1 \in R = (a^2)$.

Hence we have $1 = a(ab)$ and a is invertible.

Next, if (a^2) is a proper ideal, then (a^2) is a prime ideal by assumption.

Since the product $a \cdot a = a^2$ is in the prime ideal (a^2), it follows that $a \in (a^2)$.

Thus, there exists $b \in R$ such that $a = a^2 b$.

Equivalently, we have $a(ab - 1) = 0$.

We have observed above that R is an integral domain. As $a \neq 0$, we must have $ab - 1 = 0$, and hence $ab = 1$.

This implies that a is invertible.

Therefore, every nonzero element of R is invertible.

Hence R is a field.

Is the Quotient Ring of an Integral Domain still an Integral Domain?

Problem 589

Let R be an integral domain and let I be an ideal of R.

Is the quotient ring R/I an integral domain?

Definition (Integral Domain).

Let R be a commutative ring.

An element a in R is called a **zero divisor** if there exists $b \neq 0$ in R such that $ab = 0$.

If R contain no nonzero zero divisors, then R is called an **integral domain**.

Solution.

The quotient ring R/I of an integral domain is not necessarily an integral domain.

Consider, for example, the ring of integers $\mathbb{Z}$ and ideal $I = 4Z$.

Note that $\mathbb{Z}$ is an integral domain.

We claim that the quotient ring $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.

In fact, the element $2 + 4\mathbb{Z}$ is a nonzero element in $\mathbb{Z}/4\mathbb{Z}$.

However, the product

$$(2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) = 4 + \mathbb{Z} = 0 + \mathbb{Z}$$

is zero in $\mathbb{Z}/4\mathbb{Z}$.

This implies that $2 + 4\mathbb{Z}$ is a zero divisor, and thus $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.

Comment.

Note that in general, the quotient R/I is an integral domain if and only if I is a prime ideal of R.

In our above example, the ideal $I = 4\mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$.

Polynomial Ring with Integer Coefficients and the Prime Ideal $I = \{f(x) \in \mathbb{Z}[x] \mid f(-2) = 0\}$

Problem 573

Let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients.
Prove that

$$I = \{f(x) \in \mathbb{Z}[x] \mid f(-2) = 0\}$$

is a prime ideal of $\mathbb{Z}[x]$. Is I a maximal ideal of $\mathbb{Z}[x]$?

Proof.

Define a map $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ defined by

$$\phi(f(x)) = f(-2).$$

We first prove that ϕ is a ring homomorphism.

For any $f(x), g(x) \in \mathbb{Z}[x]$, we have

$$\begin{aligned} \phi(fg) &= (fg)(-2) = f(-2)g(-2) = \phi(f)\phi(g) \\ \phi(f+g) &= (f+g)(-2) = f(-2) + g(-2) = \phi(f) + \phi(g), \end{aligned}$$

hence ϕ is a ring homomorphism.

Then by definition of ϕ, we see that $\ker(\phi) = I$:

$$\begin{aligned} \ker(\phi) &= \{f(x) \in \mathbb{Z}[x] \mid \phi(f(x)) = 0\} \\ &= \{f(x) \in \mathbb{Z}[x] \mid f(-2) = 0\} \\ &= I. \end{aligned}$$

Next, we prove that $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ is surjective.

Let n be an arbitrary integer.

Consider the polynomial $f(x) := x + 2 + n \in \mathbb{Z}[x]$.

Then we have

$$\phi(f(x)) = f(-2) = (-2) + 2 + n = n.$$

Hence ϕ is surjective.

(Or we could've considered the constant function $f(x) := n$.)

These observations together with the first isomorphism theorem give

$$Z[x]/I \cong \phi(\mathbb{Z}[x]) = \mathbb{Z}.$$

It follows that the quotient $\mathbb{Z}[x]/I$ is an integral domain as so is $\mathbb{Z}$.

Hence I is a prime ideal of $\mathbb{Z}[x]$.

On the other hand, since $\mathbb{Z}[x]/I \cong \mathbb{Z}$ is not a field, the ideal I is not a maximal ideal of $\mathbb{Z}[x]$.

Related Question.

Problem.

Let R be the ring of all continuous functions on the interval $[0, 2]$.

Let I be the subset of R defined by

$$I := \{f(x) \in R \mid f(1) = 0\}.$$

Then prove that I is an ideal of the ring R.

Moreover, show that I is maximal and determine R/I .

The proof of this problem is given in the post ↴

A Maximal Ideal in the Ring of Continuous Functions and a Quotient Ring

A Ring Has Infinitely Many Nilpotent Elements if $ab = 1$ and $ba \neq 1$

Problem 543

Let R be a ring with 1.

Suppose that a, b are elements in R such that

$$ab = 1 \text{ and } ba \neq 1.$$

(a) Prove that $1 - ba$ is idempotent.

(b) Prove that $b^n(1 - ba)$ is nilpotent for each positive integer n.

(c) Prove that the ring R has infinitely many nilpotent elements.

Proof.

(a) Prove that $1 - ba$ is idempotent.

We compute

$$(1-ba)^2=(1-ba)(1-ba)=1-ba-ba+b\underbrace{ab}_{=1}a$$
$$=1-ba-ba+ba=1-ba.$$

Thus, we have $(1-ba)^2=1-ba$, and hence $1-ba$ is idempotent.

(b) Prove that $b^n(1-ba)$ is nilpotent for each positive integer n.

As a lemma, we show that $(1-ba)b=0$.

To see this, we calculate

$$(1-ba)b=b-b\underbrace{ab}_{=1}=b-b=0.$$

Now we compute

$$b^n(1-ba)\cdot b^n(1-ba)=b^n\underbrace{(1-ba)bb}_{=0 \text{ by lemma}}{}^{n-1}(1-ba)=0.$$

This proves that $b^n(1-ba)$ is nilpotent.

(c) Prove that the ring R has infinitely many nilpotent elements.

In part (a), we showed that the element $b^n(1-ba)$ is a nilpotent element of R for each positive integer n.

We claim that $b^n(1-ba)\neq b^m(1-ba)$ for each pair of distinct integers m,n.

Without loss of generality, we may assume that $m>n$.

We state simple facts which are needed below.

We have

$$\begin{aligned} a^nb^n &= 1\\ a^nb^m &= b^{m-n}. \end{aligned}$$

Note that a^nb^n and a^nb^m look like

$$aa\cdots a\cdot bb\cdots b.$$

Then we use the relation $ab=1$ from the middle successively, and we obtain the right-hand sides.

Now we prove that $b^n(1-ba)\neq b^m(1-ba)$ for each pair of distinct integers m,n.

Assume on the contrary $b^n(1-ba)=b^m(1-ba)$ for $m>n$.

Then we multiply by a^n on the left and get

$$a^nb^n(1-ba)=a^nb^m(1-ba).$$

Using the facts stated above, we obtain

$$1 - ba = b^{m-n}(1 - ba).$$

Note that the left-hand side is a nonzero idempotent element by part (a).

On the other hand, the right-hand side is nilpotent by part (b).

Since a nonzero idempotent element can never be nilpotent, this is a contradiction.

Therefore, $b^n(1 - ba) \neq b^m(1 - ba)$ for each pair of distinct integers m, n .

Hence there are infinitely many nilpotent elements in R .

If $ab = 1$ in a Ring, then $ba = 1$ when a or b is Not a Zero Divisor

Problem 542

Let R be a ring with $1 \neq 0$. Let $a, b \in R$ such that $ab = 1$.
(a) Prove that if a is not a zero divisor, then $ba = 1$.
(b) Prove that if b is not a zero divisor, then $ba = 1$.

Definition.

An element $x \in R$ is called a **zero divisor** if there exists a nonzero element $y \in R$ such that $xy = 0$ or $yx = 0$.

So if x is not a zero dividor, then $xy = 0$ implies that $y = 0$. Similarly, $yx = 0$ implies that $y = 0$.

Proof.

(a) Prove that if a is not a zero divisor, then $ba = 1$.

Suppose that a is not a zero divisor. We compute

$$\begin{aligned} a(ba - 1) &= aba - a && \text{by distributivity} \\ &= 1 \cdot a - a && \text{by } ab = 1 \\ &= a - a = 0. \end{aligned}$$

Since a is not a zero divisor, this yields that $ba - 1 = 0$, and hence $ba = 1$.

(b) Prove that if b is not a zero divisor, then $ba = 1$.

Suppose that b is not a zero divisor. We calculate

$$\begin{aligned} (ba - 1)b &= bab - b && \text{by distributivity} \\ &= b \cdot 1 - b && \text{by } ab = 1 \\ &= b - b = 0. \end{aligned}$$

As b is not a zero divisor, the equality $(ba - 1)b = 0$ implies that $ba - 1 = 0$.

Hence we have $ba = 1$.

Every Ideal of the Direct Product of Rings is the Direct Product of Ideals

Problem 536

Let R and S be rings with $1 \neq 0$.
Prove that every ideal of the direct product $R \times S$ is of the form $I \times J$, where I is an ideal of R, and J is an ideal of S.

Proof.

Let K be an ideal of the direct product $R \times S$.

Define

$$I = \{a \in R \mid (a, b) \in K \text{ for some } b \in S\}$$

and

$$J = \{b \in S \mid (a, b) \in K \text{ for some } a \in R\}.$$

We claim that I and J are ideals of R and S, respectively.

Let $a, a' \in I$. Then there exist $b, b' \in S$ such that $(a, b), (a', b') \in K$.
Since K is an ideal we have

$$(a, b) + (a', b') = (a + a', b + b) \in k.$$

It follows that $a + a' \in I$.
Also, for any $r \in R$ we have

$$(r, 0)(a, b) = (ra, 0) \in K$$

because K is an ideal.
Thus, $ra \in I$, and hence I is an ideal of R.
Similarly, J is an ideal of S.

Next, we prove that $K = I \times J$.
Let $(a, b) \in K$. Then by definitions of I and J we have $a \in I$ and $b \in J$.
Thus $(a, b) \in I \times J$. So we have $K \subset I \times J$.
On the other hand, consider $(a, b) \in I \times J$.
Since $a \in I$, there exists $b' \in S$ such that $(a, b') \in K$.
Also since $b \in J$, there exists $a' \in R$ such that $(a', b) \in K$.
As K is an ideal of $R \times S$, we have

$$(1, 0)(a, b') = (a, 0) \in K \text{ and } (0, 1)(a', b) = (0, b) \in K.$$

It yields that

$$(a, b) = (a, 0) + (0, b) \in K.$$

Hence $I \times J \subset K$.
Putting these inclusions together gives $k = I \times J$ as required.

Remark.

The ideals I and J defined in the proof can be alternatively defined as follows.
Consider the natural projections

$$\pi_1 : R \times S \to R \text{ and } \pi_2 : R \times S \to S.$$

Define

$$I = \pi_1(K) \text{ and } J = \pi_2(K).$$

Since the natural projections are surjective ring homomorphisms, the images I and J are ideals in R and S, respectively.

(see the post The Image of an Ideal Under a Surjective Ring Homomorphism is an Ideal.)

Every Prime Ideal in a PID is Maximal / A Quotient of a PID by a Prime Ideal is a PID

Problem 535

(a) Prove that every prime ideal of a Principal Ideal Domain (PID) is a maximal ideal.
(b) Prove that a quotient ring of a PID by a prime ideal is a PID.

Proof.

(a) Prove that every PID is a maximal ideal.

Let R be a Principal Ideal Domain (PID) and let P be a nonzero prime ideal of R.
Since R is a PID, every ideal of R is principal.
Hence there exists $p \in R$ such that $P = (p)$.
Because P is a nonzero ideal, we see that $p \neq 0$.

Let $I = (a)$ be an ideal of R such that $P \subset I \subset R$.
To show that P is a maximal ideal, we must show that $I = P$ or $I = R$.
Since $p \in (p) \subset (a)$, we have $p = ra$ for some $r \in R$.
As $p = ra$ is in the prime ideal (p), we have either $a \in (p)$ or $r \in (p)$.

If $a \in (p)$, then it follows that $(a) \subset (p)$, and hence $(a) = (p)$.
So, in this case, we have $I = P$.

If $r \in (p)$, then we have $r = sp$ for some $s \in R$.
It yields that

$$p = ra = spa \quad \Leftrightarrow \quad p(1 - sa) = 0.$$

Since R is an integral domain and $p \neq 0$, this gives $sa = 1$.
It follows that $1 \in (a)$ and thus $I = (a) = R$.

We have shown that if $P \subset I \subset R$ for some ideal I, then we have either $I = P$ or $I = R$.
Hence we conclude that P is a maximal ideal of R.

(b) Prove that a quotient ring of a PID by a prime ideal is a PID.

Let P be a prime ideal of a PID R.
It follows from part (a) that the ideal P is maximal.
Thus the quotient R/P is a field.
The only ideals of the field R/P are the zero ideal (0) and $R/P = (1)$ itself, which are principal.
Hence R/P is a PID.

The Quotient Ring $\mathbb{Z}[i]/I$ is Finite for a Nonzero Ideal of the Ring of Gaussian Integers

Problem 534

Let I be a nonzero ideal of the ring of Gaussian integers $\mathbb{Z}[i]$.
Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite.

Proof.

Recall that the ring of Gaussian integers is a Euclidean Domain with respect to the norm

$$N(a+bi) = a^2 + b^2$$

for $a+bi \in \mathbb{Z}[i]$.
In particular, $\mathbb{Z}[i]$ is a Principal Ideal Domain (PID).

Since I is a nonzero ideal of the PID $\mathbb{Z}[i]$, there exists a nonzero element $\alpha \in \mathbb{Z}[i]$ such that $I = (\alpha)$.
Let $a+bi+I$ be an arbitrary element in the quotient $\mathbb{Z}[i]/I$.
The Division Algorithm yields that

$$a+bi = q\alpha + r,$$

for some $q, r \in \mathbb{Z}[i]$ and $N(r) < N(\alpha)$.

Since $a+bi-r = q\alpha \in I$, we have

$$a+bi+I = r+I.$$

It follows that every element of $\mathbb{Z}[i]/I$ is represented by an element r whose norm is less than $N(\alpha)$.
There are only finitely many elements in $\mathbb{Z}[i]$ whose norm is less than $N(\alpha)$.
(There are only finitely many integers a, b satisfying $a^2 + b^2 < N(\alpha)$.)

Hence the quotient ring $\mathbb{Z}[i]/I$ is finite.

The Image of an Ideal Under a Surjective Ring Homomorphism is an Ideal

Problem 532

Let R and S be rings. Suppose that $f : R \to S$ is a surjective ring homomorphism.
Prove that every image of an ideal of R under f is an ideal of S.
Namely, prove that if I is an ideal of R, then $J = f(I)$ is an ideal of S.

Proof.

As in the statement of the problem, let I be an ideal of R.
Our goal is to show that the image $J = f(I)$ is an ideal of S.
For any $a, b \in J$ and $s \in S$, we need to show that

(1) $a+b \in J$,
(2) $sa \in J$.

Since $a, b \in J = f(I)$, there exists $a', b' \in I$ such that

$$f(a') = a \text{ and } f(b') = b.$$

Then we have

$$a + b = f(a') + f(b') = f(a' + b')$$

since f is a homomorphism.
Since I is an ideal, the sum $a' + b'$ is in I.
This yields that $a + b \in f(I) = J$, which proves (1).

Since $f : R \to S$ is surjective, there exists $r \in R$ such that $f(r) = s$.
It follows that

$$sa = f(r)f(a') = f(ra')$$

since f is a homomorphism.
Since I is an ideal of R, the product ra' is in I.
Hence $sa \in f(I) = J$, and (2) is proved.
Therefore the image $J = f(I)$ is an ideal of S.

No Nonzero Zero Divisor in a Field / Direct Product of Rings is Not a Field

Problem 531

(a) Let F be a field. Show that F does not have a nonzero zero divisor.
(b) Let R and S be nonzero rings with identities.
Prove that the direct product $R \times S$ cannot be a field.

Proof.

(a) Show that F does not have a nonzero zero divisor.

Seeking a contradiction, suppose that x is a nonzero zero divisor of the field F. This means that there exists a nonzero element $y \in F$ such that

$$yx = 0.$$

Since y is a nonzero element in F, we have the inverse y^{-1} in F.
Hence we have

$$0 = y^{-1} \cdot 0 = y^{-1}(yx) = (y^{-1}y)x = x.$$

This is a contradiction because x is a nonzero element.
We conclude that the field F does not have a nonzero zero divisor.
(Remark that it follows that a field is an integral domain.)

(b) Prove that the direct product $R \times S$ cannot be a field.

Since R and S have identities, the direct product $R \times S$ contains nonzero elements $(1, 0)$ and $(0, 1)$.

The product of these elements is

$$(1,0)\cdot(0,1)=(1\cdot 0,\,0\cdot 1)=(0,0).$$

Similarly we also have

$$(0,1)\cdot(1,0)=(0,0).$$

It follows that $(1,0)$ is a nonzero zero divisor of $R\times S$. By part (a), a field does not have a nonzero zero divisor. Hence $R\times S$ is never a field.

Every Prime Ideal is Maximal if $a^n=a$ for any Element a in the Commutative Ring

Problem 530

Let R be a commutative ring with identity $1\neq 0$. Suppose that for each element $a\in R$, there exists an integer $n>1$ depending on a.
Then prove that every prime ideal is a maximal ideal.

Hint.

Let R be a commutative ring with 1 and I be an ideal of R.

Recall the following facts:

- I is a prime ideal if and only if R/I is an integral domain.
- I is a maximal ideal if and only if R/I is a field.

Proof.

Let I be a prime ideal of the ring R. To prove that I is a maximal ideal, it suffices to show that the quotient R/I is a field.

Let $\bar{a}=a+I$ be a nonzero element of R/I, where $a\in R$.

It follows from the assumption that there exists an integer $n>1$ such that $a^n=a$.

Then we have

$$\bar{a}^n=a^n+I=a+I=\bar{a}.$$

Thus we have

$$\bar{a}(\bar{a}^{n-1}-1)=0$$

in R/I.

Note that R/I is an integral domain since I is a prime ideal.

Since $\bar{a}\neq 0$, the above equality yields that $\bar{a}^{n-1}-1=0$, and hence

$$\bar{a}\cdot\bar{a}^{n-2}=1.$$

It follows that $\bar{a}$ has a multiplicative inverse $\bar{a}^{n-2}$.

This proves that each nonzero element of R/I is invertible, hence R/I is a field.

We conclude that I is a field.

A ring is Local if and only if the set of Non-Units is an Ideal

Problem 526

A ring is called **local** if it has a unique maximal ideal.
(a) Prove that a ring R with 1 is local if and only if the set of non-unit elements of R is an ideal of R.
(b) Let R be a ring with 1 and suppose that M is a maximal ideal of R.
Prove that if every element of $1+M$ is a unit, then R is a local ring.

Proof of (a).

$(\Longrightarrow)$: If R is a local ring then the set of non-units is an ideal

Suppose that R is a local ring and let M be the unique maximal ideal of R.
We denote by I the set of non-unit elements of R.

Let $a, b \in I$.
Since a, b are non-unit elements, the ideals (a) and (b) generated by a and b, respectively, are proper ideals of R.
Since M is the only maximal ideal of R, it follows that

$$(a) \subset M \text{ and } (b) \subset M.$$

It yields that $a-b \in M$ since $a, b \in M$ and M is an ideal.
As M is a proper ideal, $a-b$ is a non-unit, hence $a-b \in I$.
Also for any $r \in R$, we have $ra \in M$ since $a \in M$ and M is an ideal of R.
It follows that ra is a non-unit because M is a proper ideal.
Hence $ra \in I$.
Therefore the set I is an ideal of R.

$(\Longleftarrow)$: If the set of non-units is an ideal, then R is a local ring

Suppose that the set I of non-units elements in R is an ideal of R.
Since $1 \in R$ is a unit, I is a proper ideal.

Let M be an arbitrary maximal ideal of R.
Note that every element of M is a non-unit element of R since M is a proper ideal.
Thus we have $M \subset I$.
Since M is a maximal ideal, it yields that $M=I$.
Therefore I is the unique maximal ideal of R, and hence R is a local ring.

Proof of (b).

We prove that the maximal ideal M is the set of non-units elements in R.
Then the result follows from part (a).

Take any $a \in R \setminus M$.
Then the ideal $(a)+M$ generated by a and M is strictly larger than M.
Hence

$$(a)+M=R$$

by the maximality of M.

Then there exists $r \in R$ and $m \in M$ such that

$$ra + m = 1.$$

Since $ra = 1 - m \in 1 + M$, it follows from the assumption that ra is a unit.
It yield that a is a unit.

Since M contains no unit elements, we see that M consists of non-unit elements of R.
Thus, by part (a) we conclude that R is a local ring.

The Quotient Ring by an Ideal of a Ring of Some Matrices is Isomorphic to $\mathbb{Q}$.

Problem 525

Let

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{Q} \right\}.$$

Then the usual matrix addition and multiplication make R an ring.
Let

$$J = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \;\middle|\; b \in \mathbb{Q} \right\}$$

be a subset of the ring R.
(a) Prove that the subset J is an ideal of the ring R.
(b) Prove that the quotient ring R/J is isomorphic to $\mathbb{Q}$.

Proof.

(a) Prove that the subset J is an ideal of the ring R.

Let

$$\alpha = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$$

be arbitrary elements in J with $a, b \in \mathbb{Q}$.
Then since we have

$$\alpha - \beta = \begin{bmatrix} 0 & a-b \\ 0 & 0 \end{bmatrix} \in J,$$

the subset J is an additive group.

Now consider any elements

$$\rho = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in R \text{ and } \gamma = \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} \in J.$$

Then we have

$$\rho\gamma = \begin{bmatrix} 0 & ac \\ 0 & 0 \end{bmatrix} \in J \text{ and}$$

$$\gamma\rho = \begin{bmatrix} 0 & ca \\ 0 & 0 \end{bmatrix} \in J.$$

Thus, each element of J multiplied by an element of R is still in J.

Hence J is an ideal of the ring R.

(b) Prove that the quotient ring R/J is isomorphic to $\mathbb{Q}$.

Consider the map $\phi : R \to \mathbb{Q}$ defined by

$$\phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\right) = a,$$

for $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in R$.

We first show that the map ϕ is a ring homomorphism.

First of all, we have

$$\phi\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 1.$$

Thus ϕ maps the unity element of R to the unity element of $\mathbb{Q}$.

Take

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}, \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \in R.$$

Then we have

$$\begin{aligned} \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} + \begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right) &= \phi\left(\begin{bmatrix} a+c & b+d \\ 0 & a+c \end{bmatrix}\right) = a + c \\ &= \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\right) + \phi\left(\begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right) \end{aligned}$$

and

$$\begin{aligned} \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right) &= \phi\left(\begin{bmatrix} ac & ad+bc \\ 0 & ac \end{bmatrix}\right) = ac \\ &= \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\right)\phi\left(\begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right). \end{aligned}$$

It follows from these computations that $\phi : R \to \mathbb{Q}$ is a ring homomorphism.

Next, we determine the kernel of ϕ.

We claim that $\ker(\phi) = J$.

If $\rho = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in \ker(\phi)$, then we have

$$0 = \phi(\rho) = \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \right) = a.$$

So $\rho = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in J$, and hence $\ker(\phi) \subset J$.

On the other hand, if $\rho = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in J$, then it follows from the definition of ϕ that $\phi(\rho) = 0$.

Thus, $J \subset \ker(\phi)$.

Putting these two inclusions together yields $J = \ker(\phi)$.

Observe that the homomorphism ϕ is surjective.

In fact, for any $a \in \mathbb{Q}$, we take $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in R$. Then we have

$$\phi\left(\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \right) = a.$$

In summary, $\phi : R \to \mathbb{Q}$ is a surjective homomorphism with kernel J.

It follows from the isomorphism theorem that

$$R/J \cong \mathbb{Q},$$

as required.

Remark.

Recall that the kernel of a ring homomorphism $\phi : R \to S$ is always an ideal of R.

Thus, the proof of (b) shows that J is an ideal of R. This gives an alternative proof of part (a).

Is the Given Subset of The Ring of Integer Matrices an Ideal?

Problem 524

Let R be the ring of all 2×2 matrices with integer coefficients:

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z} \right\}.$$

Let S be the subset of R given by

$$S = \left\{ \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} \;\middle|\; s \in \mathbb{Z} \right\}.$$

(a) True or False: S is a subring of R.

(b) True or False: S is an ideal of R.

Solution.

(a) True or False: S is a subring of R.

True.

In fact, let

$$A = \begin{bmatrix} t & 0 \\ 0 & t \end{bmatrix} \text{ and } B = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}$$

be arbitrary elements in S with $t, s \in \mathbb{Z}$.

Then we have

$$A + B = \begin{bmatrix} t+s & 0 \\ 0 & t+s \end{bmatrix} \in S$$

and

$$AB = \begin{bmatrix} ts & 0 \\ 0 & ts \end{bmatrix} \in S.$$

Hence S is closed under addition and multiplication.

Note that the 2×2 identity matrix is the unity element of R as well as the unity element of S.

Thus, the subset S is a subring of R.

(b) True or False: S is an ideal of R.

False.

To see that S is not an ideal of R, consider the element

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in R$$

and the element

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S.$$

Then we have

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

which is **not in** S.

This implies that S is not an ideal of R.

(If S were an ideal of R, then an element of S multiplied by an element of R would stay in S.)

Examples of Prime Ideals in Commutative Rings that are Not Maximal Ideals

Problem 520

Give an example of a commutative ring R and a prime ideal I of R that is not a maximal ideal of R.

Solution.

We give several examples. The key facts are:

1. An ideal I of R is prime if and only if R/I is an integral domain.
2. An ideal I of R is maximal if and only if R/I is a field.

Example 1: $\mathbb{Z}$ and (0)

The first example is the ring of integers $R = \mathbb{Z}$ and the zero ideal $I = (0)$.
Note that the quotient ring is $\mathbb{Z}/(0) \cong \mathbb{Z}$ and it is integral domain but not a field.
Thus the ideal (0) is a prime ideal by Fact 1 but not a maximal ideal by Fact 2.

Remark

Note that (0) is the only prime ideal of $\mathbb{Z}$ that is not a maximal ideal.
Nonzero ideals of $\mathbb{Z}$ are (p) for some prime number p.

Example 2: $\mathbb{Z}[x]$ and (x)

The second example is the ring of polynomials $R = \mathbb{Z}[x]$ over $\mathbb{Z}$ and the principal ideal $I = (x)$ generated by $x \in \mathbb{Z}[x]$.
The quotient ring is $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, which is an integral domain but not a field.
Thus the ideal (x) is prime but not maximal by Fact 1, 2.

Example 3: $\mathbb{Q}[x, y]$ and (x)

The third example is the ring of polynomials in two variables $R = \mathbb{Q}[x, y]$ over $\mathbb{Q}$ and the principal ideal $I = (x)$ generated by x.
The quotient ring $\mathbb{Q}[x, y]/(x)$ is isomorphic to $\mathbb{Q}[y]$.
(The proof of this isomorphism is given in the post Prove the Ring Isomorphism $R[x, y]/(x) \cong R[y]$.)
Note that $\mathbb{Q}[y]$ is an integral domain but it is not a field since, for instance, the element $y \in \mathbb{Q}[y]$ is not a unit.
Hence Fact 1, 2 implies that the ideal (x) is prime but not maximal in the ring $\mathbb{Q}[x, y]$.

The Quadratic Integer Ring $\mathbb{Z}[\sqrt{5}]$ is not a Unique Factorization Domain (UFD)

Problem 519

Prove that the quadratic integer ring $\mathbb{Z}[\sqrt{5}]$ is not a Unique Factorization Domain (UFD).

Proof.

Any element of the ring $\mathbb{Z}[\sqrt{-5}]$ is of the form $a + b\sqrt{-5}$ for some integers a, b.
The associated (field) norm N is given by

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Consider the case when $a = 2, b = 1$.
Then we have

$$(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3. \qquad (*)$$

We claim that the numbers $3, 2 \pm \sqrt{-5}$ are irreducible elements in the ring $\mathbb{Z}[\sqrt{-5}]$.
To prove the claim at once, **we show that any element in $\mathbb{Z}[\sqrt{-5}]$ of norm 9 is irreducible**.

Let α be an element in $\mathbb{Z}[\sqrt{-5}]$ such that $N(\alpha) = 9$.
Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$.
Out goal is to show that either β or γ is a unit.
We have

$$9 = N(\alpha) = N(\beta)N(\gamma).$$

Since the norms are nonnegative integers, $N(\beta)$ is one of $1, 3, 9$.
If $N(\beta) = 1$, then it yields that β is a unit.
If $N(\beta) = 3$, then we write $\beta = a + b\sqrt{-5}$ for some integers a, b, and we obtain

$$3 = N(\beta) = a^2 + 5b^2.$$

A quick inspection yields that there are no integers a, b satisfying this equality.
Thus $N(\beta) = 3$ is impossible.
If $N(\beta) = 9$, then $N(\gamma) = 1$ and thus γ is a unit.
Therefore, we have shown that either β or γ is a unit.
Note that the elements $3, 2 \pm \sqrt{-5}$ have norm 9, and hence they are irreducible by what we have just proved.

It follows from the equalities in (*) that the factorization of the element 9 into irreducible elements are not unique.
Thus, the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Related Question.

Problem.
Prove that the quadratic integer ring $\mathbb{Z}[\sqrt{5}]$ is not a Unique Factorization Domain (UFD).

Note that -5 is replaced by 5.
See the proof of this problem ↴
The Quadratic Integer Ring $\mathbb{Z}[\sqrt{5}]$ is not a Unique Factorization Domain (UFD)

The Quadratic Integer Ring $\mathbb{Z}[\sqrt{-5}]$ is not a Unique Factorization Domain (UFD)

Problem 518

Prove that the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a Unique Factorization Domain (UFD).

Proof.

Any element of the ring $\mathbb{Z}[\sqrt{-5}]$ is of the form $a + b\sqrt{-5}$ for some integers a, b.
The associated (field) norm N is given by

$$N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2.$$

Consider the case when $a=2, b=1$.

Then we have

$$(2+\sqrt{-5})(2-\sqrt{-5}) = 9 = 3\cdot 3. \tag{*}$$

We claim that the numbers $3, 2\pm\sqrt{-5}$ are irreducible elements in the ring $\mathbb{Z}[\sqrt{-5}]$.

To prove the claim at once, **we show that any element in $\mathbb{Z}[\sqrt{-5}]$ of norm 9 is irreducible**.

Let α be an element in $\mathbb{Z}[\sqrt{-5}]$ such that $N(\alpha)=9$.

Suppose that $\alpha=\beta\gamma$ for some $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$.

Out goal is to show that either β or γ is a unit.

We have

$$9 = N(\alpha) = N(\beta)N(\gamma).$$

Since the norms are nonnegative integers, $N(\beta)$ is one of $1, 3, 9$.

If $N(\beta)=1$, then it yields that β is a unit.

If $N(\beta)=3$, then we write $\beta=a+b\sqrt{-5}$ for some integers a, b, and we obtain

$$3 = N(\beta) = a^2+5b^2.$$

A quick inspection yields that there are no integers a, b satisfying this equality.

Thus $N(\beta)=3$ is impossible.

If $N(\beta)=9$, then $N(\gamma)=1$ and thus γ is a unit.

Therefore, we have shown that either β or γ is a unit.

Note that the elements $3, 2\pm\sqrt{-5}$ have norm 9, and hence they are irreducible by what we have just proved.

It follows from the equalities in (*) that the factorization of the element 9 into irreducible elements are not unique.

Thus, the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Related Question.

Problem.

Prove that the quadratic integer ring $\mathbb{Z}[\sqrt{5}]$ is not a Unique Factorization Domain (UFD).

Note that -5 is replaced by 5.

See the proof of this problem ↴

The Quadratic Integer Ring $\mathbb{Z}[\sqrt{5}]$ is not a Unique Factorization Domain (UFD)

Prove the Ring Isomorphism $R[x,y]/(x) \cong R[y]$

Problem 517

Let R be a commutative ring. Consider the polynomial ring $R[x,y]$ in two variables x, y.

Let (x) be the principal ideal of $R[x,y]$ generated by x.

Prove that $R[x,y]/(x)$ is isomorphic to $R[y]$ as a ring.

Proof.

Define the map $\psi : R[x,y] \to R[y]$ by sending $f(x,y) \in R[x,y]$ to $f(0,y)$.
Namely, the map ψ is the substitution $x = 0$.
It is straightforward to check that ψ is a ring homomorphism.

For any polynomial $g(y) \in R[y]$, let $G(x,y) = g(y) \in R[x,y]$.
Then we have $\psi(G(x,y)) = G(0,y) = g(y)$.
This proves that ψ is surjective.

We claim that the kernel of ψ is the ideal (x).
Suppose that $f(x,y) \in \ker(\psi)$.
We write

$$f(x,y) = f_0(y) + f_1(y)x + \cdots + f_n(y)x^n,$$

where $f_i \in R[y]$ for $i = 1, \ldots, n$.
Since $f(x,y) \in \ker(\psi)$, it yields that

$$0 = \psi(f(x,y)) = f(0,y) = f_0(y).$$

Hence

$$\begin{aligned} f(x,y) &= f_1(y)x + \cdots + f_n(y)x^n \\ &= x\left(f_1(y) + \cdots + f_n(y)x^{n-1}\right) \in (x). \end{aligned}$$

Thus, $\ker(\psi) \subset (x)$.
On the other hand, suppose $f(x,y) \in (x)$.
Then there exists $g(x,y) \in R[x,y]$ such that

$$f(x,y) = xg(x,y).$$

It follows that

$$\psi\left(\, f(x,y)\,\right) = \psi\left(\, xg(x,y)\,\right) = 0g(0,y) = 0.$$

It implies that $f(x,y) \in \ker(\psi)$, hence $\ker(\psi) \subset (x)$.
Putting two inclusions together gives $(x) = \ker(\psi)$.

In summary, the map $\psi : R[x,y] \to R[y]$ is a surjective ring homomorphism with kernel (x).
Hence by the isomorphism theorem, we obtain the isomorphism

$$R[x,y]/(x) \cong R[y].$$

Idempotent Elements and Zero Divisors in a Ring and in an Integral Domain

Problem 516

Prove the following statements.

(a) If $a \neq 1$ is an idempotent element of R, then a is a zero divisor.

(b) Suppose that R is an integral domain. Determine all the idempotent elements of R.

Definitions (Idempotent, Zero Divisor, Integral Domain)

Let R be a ring with 1.

- An element a of R is called **idempotent** if $a^2 = a$.
- An element a of R is called **zero divisor** if there exists a nonzero element x of R such that $ax = 0$ or $xa = 0$.
- A commutative ring that does not have a nonzero zero divisor is called an **integral domain**

Proof.

(a) If $a \neq 1$ is an idempotent element of R, then a is a zero divisor.

By definition of an idempotent element, we have $a^2 = a$.

It yields that

$$a(a-1) = a^2 - a = 0.$$

Since $a \neq 1$, the element $a - 1$ is a nonzero element in the ring R.

Thus a is a zero divisor.

(b) Suppose that R is an integral domain. Determine all the idempotent elements of R.

Suppose that a is an idempotent element in the integral domain R.

Thus, we have $a^2 = a$.

It follows that we have

$$a(a-1) = a^2 - a = 0. \tag{*}$$

Since R is an integral domain, there is no nonzero zero divisor.

Hence (*) yields that $a = 0$ or $a - 1 = 0$.

Clearly, the elements 0 and 1 are idempotent.

Thus, the idempotent elements in the integral domain R must be 0 and 1.

The Ring $\mathbb{Z}[\sqrt{2}]$ is a Euclidean Domain

Problem 503

Prove that the ring of integers

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

of the field $\mathbb{Q}(\sqrt{2})$ is a Euclidean Domain.

Proof.

First of all, it is clear that $\mathbb{Z}[\sqrt{2}]$ is an integral domain since it is contained in $\mathbb{R}$.

We use the norm given by the absolute value of field norm.
Namely, for each element $a+\sqrt{2}b \in \mathbb{Z}[\sqrt{2}]$, define

$$N(a+\sqrt{2}b) = |a^2 - 2b^2|.$$

Then the map $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_{\geq 0}$ is a norm on $\mathbb{Z}[\sqrt{2}]$.
Also, it is multiplicative:

$$N(xy) = N(x)N(y).$$

Remark that since this norm comes from the field norm of $\mathbb{Q}(\sqrt{2})$, the multiplicativity of N holds for $x, y \in \mathbb{Q}(\sqrt{2})$ as well.
We show the existence of a Division Algorithm as follows.
Let

$$x = a + b\sqrt{2} \text{ and } y = c + d\sqrt{2}$$

be arbitrary elements in $\mathbb{Z}[\sqrt{2}]$, where $a, b, c, d \in \mathbb{Z}$.
We have

$$\frac{x}{y} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2} = r + s\sqrt{2},$$

where we put

$$r = \frac{ac-2bd}{c^2-2d^2} \text{ and } s = \frac{bc-ad}{c^2-2d^2}.$$

Let n be an integer closest to the rational number r and let m be an integer closest to the rational number s, so that

$$|r-n| \leq \frac{1}{2} \text{ and } |s-m| \leq \frac{1}{2}.$$

Let

$$t := r - n + (s-m)\sqrt{2}.$$

Then we have

$$\begin{aligned} t &= r + s\sqrt{2} - (n + m\sqrt{2}) \\ &= \frac{x}{y} - (n+m\sqrt{2})y. \end{aligned}$$

It follows that

$$yt = x - (n+m\sqrt{2}) \in \mathbb{Z}[\sqrt{2}].$$

Thus we have

$$x = (n+m\sqrt{2})y + yt \qquad (*)$$

with $n+m\sqrt{2}, yt \in \mathbb{Z}[\sqrt{2}]$.
We have

$$\begin{aligned} N(t) &= |(r-n)^2 - 2(s-m)^2| \\ &\leq |r-n|^2 + 2|s-m|^2 \\ &\leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4}. \end{aligned}$$

It follows from the multiplicativity of the norm N that

$$N(yt) = N(y)N(t) \leq \frac{3}{4}N(y) < N(y).$$

Thus the expression (*) gives a Division Algorithm with quotient $n + m\sqrt{2}$ and remainder yt.

Related Question.

Problem. In the ring $\mathbb{Z}[\sqrt{2}]$, prove that 5 is a prime element but 7 is not a prime element.

For a proof of this problem, see the post "5 is prime but 7 is not prime in the ring $\mathbb{Z}[\sqrt{2}]$".

Every Ring of Order p^2 is Commutative

Problem 501

Let R be a ring with unit 1. Suppose that the order of R is $|R| = p^2$ for some prime number p.
Then prove that R is a commutative ring.

Proof.

Let us consider the subset

$$Z := \{z \in R \mid zr = rz \text{ for any } r \in R\}.$$

(This is called the **center** of the ring R.)

This is a subgroup of the additive group R.

In fact, if $z, z' \in Z$, then we have for any $r \in R$,

$$(z-z')r = zr - z'r = rz - rz' = r(z-z').$$

It follows that $z - z' \in Z$, and thus Z is a subgroup of R.

Note that $0, 1 \in Z$, hence Z is not a trivial subgroup.

Thus, we have either $|Z| = p, p^2$ since R is a group of order p^2.

If $|Z| = p^2$, then we have $Z = R$.

By definition of Z, this implies that R is commutative.

It remains to show that $|Z| \neq p$.

Assume that $|Z| = p$.

Then R/Z is a cyclic group of order p.

Let α be a generator of R/Z.

Since $Z \neq R$, there exist $r, s \in R$ such that $rs \neq sr$.

Write

$$r = m\alpha + z \text{ and } s = n\alpha + z'$$

for some $m, n \in \mathbb{Z}$, $z, z' \in Z$.

Then we have

$$\begin{aligned} rs &= (m\alpha + z)(n\alpha + z') \\ &= (m\alpha)(n\alpha) + m\alpha z' + nz\alpha + zz' \\ &= (n\alpha)(m\alpha) + mz'\alpha + n\alpha z + z'z \\ &= (n\alpha + z')(m\alpha + z) \\ &= sr. \end{aligned}$$

This contradicts $rs \neq sr$, and we conclude that $|Z| \neq p$.

The Polynomial Rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are Not Isomorphic

Problem 494

Prove that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomoprhic.

Proof.

We give three proofs.

The first two proofs use only the properties of ring homomorphism.

The third proof resort to the units of rings.

If you are familiar with units of $\mathbb{Z}[x]$, then the third proof might be concise and easy to follow.

The First Proof

Assume on the contrary that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are isomorphic.

Let

$$\phi : \mathbb{Q}[x] \to \mathbb{Z}[x]$$

be an isomorphism.

The polynomial x in $\mathbb{Q}[x]$ is mapped to the polynomial $\phi(x) \in \mathbb{Z}[x]$.

Note that $\frac{x}{2^n}$ is an element in $\mathbb{Q}[x]$ for any positive integer n .

Thus we have

$$\begin{aligned} \phi(x) &= \phi(2^n \cdot \frac{x}{2^n}) \\ &= 2^n \phi\left(\frac{x}{2^n}\right) \end{aligned}$$

since ϕ is a homomorphism.

As ϕ is injective, the polynomial $\phi(\frac{x}{2^n}) \neq 0$.

Since $\phi(\frac{x}{2^n})$ is a nonzero polynomial with integer coefficients, the absolute values of the nonzero coefficients of $2^n \phi(\frac{x}{2^n})$ is at least 2^n .

However, since this is true for any positive integer, the coefficients of the polynomial $\phi(x) = 2^n \phi(\frac{x}{2^n})$ is arbitrarily large, which is impossible.

Thus, there is no isomorphism between $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$.

The Second Proof

Seeking a contradiction, assume that we have an isomorphism

$$\phi : \mathbb{Q}[x] \to \mathbb{Z}[x].$$

Since ϕ is a ring homomorphism, we have $\phi(1)=1$.

Then we have

$$\begin{aligned} 1=\phi(1)&=\phi\left(2\cdot\frac{1}{2}\right)\\ &=2\phi\left(\frac{1}{2}\right) \end{aligned}$$

since ϕ is a homomorphism.

Since $\phi\left(\frac{1}{2}\right)\in\mathbb{Z}[x]$, we write

$$\phi\left(\frac{1}{2}\right)=a_nx^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0,$$

for some integers $a_0,\dots,a_n$.

Since $2\phi\left(\frac{1}{2}\right)=1$, it follows that

$$2a_n=0,\dots,2a_1=0,2a_0=1.$$

Since a_0 is an integer, this is a contradiction.

Thus, such an isomorphism does not exists.

Hence $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ are not isomorphic.

The Third Proof

Note that in general the units of the polynomial ring $R[x]$ over an integral domain R is the units $R^\times$ of R.

Since $\mathbb{Z}$ and $\mathbb{Q}$ are both integral domain, the units are

$$\mathbb{Z}[x]^\times=\mathbb{Z}^\times=\{\pm1\} \text{ and } \mathbb{Q}[x]^\times=\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}.$$

Since every ring isomorphism maps units to units, if two rings are isomorphic then the number of units must be the same.

As seen above, $\mathbb{Z}[x]$ contains only two units although $\mathbb{Q}[x]$ contains infinitely many units.

Thus, they cannot be isomorphic.

Determine the Quotient Ring $\mathbb{Z}[\sqrt{10}]/(2,\sqrt{10})$

Problem 487

Let

$$P=(2,\sqrt{10})=\{a+b\sqrt{10}\mid a,b\in\mathbb{Z}, 2|a\}$$

be an ideal of the ring

$$\mathbb{Z}[\sqrt{10}]=\{a+b\sqrt{10}\mid a,b\in\mathbb{Z}\}.$$

Then determine the quotient ring $\mathbb{Z}[\sqrt{10}]/P$.

Is P a prime ideal? Is P a maximal ideal?

Solution.

We prove that the ring $\mathbb{Z}[\sqrt{10}]/P$ is isomorphic to the ring $\mathbb{Z}/2\mathbb{Z}$.

We define the map $\Psi:\mathbb{Z}[\sqrt{10}]\to\mathbb{Z}/2\mathbb{Z}$ by sending $a+b\sqrt{10}$ to $\bar{a}=a \pmod 2\in\mathbb{Z}/2\mathbb{Z}$.

The map Ψ is a ring homomorphism. To see this,

let $a+b\sqrt{10}, c+d\sqrt{10}\in\mathbb{Z}[\sqrt{10}]$.

We have

$$\begin{aligned}\Psi\left((a+b\sqrt{10})(c+d\sqrt{10})\right) &= \Psi\left(ac+10bd+(ad+bc)\sqrt{10}\right)\\ &= ac+10bd \pmod 2 = ac \pmod 2\\ &= \Psi(a+b\sqrt{10})\Psi(c+d\sqrt{10}).\end{aligned}$$

We also have

$$\begin{aligned}\Psi\left((a+b\sqrt{10})+(c+d\sqrt{10})\right) &= \Psi\left(a+c+(b+d)\sqrt{10}\right)\\ &= a+c \pmod 2\\ &= \Psi(a+b\sqrt{10})+\Psi(c+d\sqrt{10}).\end{aligned}$$

Therefore the map Ψ is a ring homomorphism.

Since $\Psi(0)=\bar{0}$ and $\Psi(1)=\bar{1}$, the map $\Psi : \mathbb{Z}[\sqrt{10}] \to \mathbb{Z}/2\mathbb{Z}$ is surjective.

We have $\Psi(a+b\sqrt{10})=\bar{0}$ if and only if a is even.

Thus, the kernel of the homomorphism Ψ is

$$\ker(\Psi) = \{a+b\sqrt{10} \mid a,b\in\mathbb{Z}, 2|a\} = P.$$

In summary the map $\Psi : \mathbb{Z}[\sqrt{10}] \to \mathbb{Z}/2\mathbb{Z}$ is a surjective ring homomorphism with the kernel P. Hence by the first isomorphism theorem, we have

$$\mathbb{Z}[\sqrt{10}]/P \cong \mathbb{Z}/2\mathbb{Z}$$

as we claimed.

Since $\mathbb{Z}/2\mathbb{Z}$ is a field, the ideal P is a maximal ideal, and in particular P is a prime ideal.

Related Question.

A direct proof that the ideal $P=(2,\sqrt{10})$ is prime in the ring $\mathbb{Z}[\sqrt{10}]$ is given in the post "A prime ideal in the ring $\mathbb{Z}[\sqrt{10}]$".

Every Integral Domain Artinian Ring is a Field

Problem 437

Let R be a ring with 1. Suppose that R is an integral domain and an Artinian ring.

Prove that R is a field.

Definition (Artinian ring).

A ring R is called **Artinian** if it satisfies the defending chain condition on ideals.

That is, whenever we have ideals I_n of R satisfying

$$I_1 \supset I_2 \supset \cdots \supset I_n \supset \cdots,$$

there is an integer N such that

$$I_N = I_{N+1} = I_{N+2} = \cdots.$$

Proof.

Let $x\in R$ be a nonzero element. To prove R is a field, we show that the inverse of x exists in R.

Consider the ideal $(x)=xR$ generated by the element x. Then we have a descending chain of ideals of R:

$$(x) \supset (x^2) \supset \cdots \supset (x^i) \supset (x^{i+1}) \supset \cdots.$$

In fact, if $r \in (x^{i+1})$, then we write it as $r = x^{i+1}s$ for some $s \in R$.

Then we have

$$r = x^i \cdot xs \in (x^i)$$

since (x^i) is an ideal and $xs \in R$.

Hence $(x^{i+1}) \subset (x^i)$ for any positive integer i.

Since R is an Artinian ring by assumption, the descending chain of ideals terminates.

That is, there is an integer N such that we have

$$(x^N) = (x^{N+1}) = \cdots.$$

It follows from the equality $(x^N) = (x^{N+1})$ that there is $y \in R$ such that

$$x^N = x^{N+1}y.$$

It yields that

$$x^N(1 - xy) = 0.$$

Since R is an integral domain, we have either $x^N = 0$ or $1 - xy = 0$.

Since x is a nonzero element and R is an integral domain, we know that $x^N \neq 0$.

Thus, we must have $1 - xy = 0$, or equivalently $xy = 1$.

This means that y is the inverse of x, and hence R is a field.

Three Equivalent Conditions for a Ring to be a Field

Problem 436

Let R be a ring with 1. Prove that the following three statements are equivalent.

1. The ring R is a field.
2. The only ideals of R are (0) and R.
3. Let S be any ring with 1. Then any ring homomorphism $f : R \to S$ is injective.

Proof.

We prove the equivalences $(1) \Leftrightarrow (2)$ and $(2) \Leftrightarrow (3)$.

$(1) \implies (2)$

Suppose that R is a field. Let I be an ideal of R.

If $I = (0)$, then there is nothing to prove.

So assume that $I \neq (0)$.

Then there is a nonzero element x in I.

Since R is a field, we have $x^{-1} \in R$.

Since I is an ideal, we have

$$1 = x^{-1} \cdot x \in I.$$

This yields that $I = R$.

$(2) \implies (1)$

Suppose now that the only ideals of R are (0) and R.

Let x be a nonzero element of R. We show the existence of the inverse of x.

Consider the ideal $(x) = xR$ generated by x.

Since x is nonzero, the ideal $(x) \neq 0$, and thus we have $(x) = R$ by assumption.

Thus, there exists $y \in R$ such that

$$xy = 1.$$

So y is the inverse element of x.

Hence R is a field.

$(2) \implies (3)$

Suppose that the only ideals of R are (0) and R.

Let S be any ring with 1 and $f : R \to S$ be any ring homomorphism.

Consider the kernel $\ker(f)$. The kernel $\ker(f)$ is an ideal of R, and thus $\ker(f)$ is either (0) or R by assumption.

If $\ker(f) = R$, then the homomorphism f sends $1 \in R$ to $0 \in S$, which is a contradiction since any ring homomorphism between rings with 1 sends 1 to 1.

Thus, we must have $\ker(f) = 0$, and this yields that the homomorphism f is injective.

$(3) \implies (2)$

Suppose that statement 3 is true. That is, any ring homomorphism $f : R \to S$, where S is any ring with 1, is injective.

Let I be a proper ideal of R: an ideal $I \neq R$.

Then the quotient R/I is a ring with 1 and the natural projection

$$f : R \to R/I$$

is a ring homomorphism.

By assumption, the ring homomorphism f is injective, and hence we have

$$(0) = \ker(f) = I.$$

This proves that the only ideals of R are (0) and R.

If R is a Noetherian Ring and $f : R \to R'$ is a Surjective Homomorphism, then R' is Noetherian

Problem 413

Suppose that $f : R \to R'$ is a surjective ring homomorphism.
Prove that if R is a Noetherian ring, then so is R'.

Definition.

A ring S is Noetherian if for every ascending chain of ideals of S

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$$

there exists an integer N such that we have

$$I_N = I_{N+1} = I_{N+2} = \cdots.$$

Proof.

To prove the ascending chain condition for R', let

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$$

be an ascending chain of ideals of R'.

Note that the preimage $f^{-1}(I_k)$ of the ideal I_k by a ring homomorphism is an ideal of R.

(See the post "The inverse image of an ideal by a ring homomorphism is an ideal" for a proof.)

Thus we obtain the ascending chain of ideals of R

$$f^{-1}(I_1) \subset f^{-1}(I_2) \subset \cdots \subset f^{-1}(I_k) \subset \cdots.$$

By assumption R is Noetherian, and hence this ascending chain of ideals terminates. That is, there is an integer N such that

$$f^{-1}(I_N) = f^{-1}(I_{N+1}) = f^{-1}(I_{N+2}) = \dots.$$

Since f is surjective, we have

$$f\big(f^{-1}(I_k)\big) = I_k$$

for any k. Hence it follows that we have

$$I_N = I_{N+1} = I_{N+2} = \dots.$$

So each ascending chain of ideals of R' terminates, and thus R' is a Noetherian ring.

The Preimage of Prime ideals are Prime Ideals

Problem 412

Let $f : R \to R'$ be a ring homomorphism. Let P be a prime ideal of the ring R'.

Prove that the preimage $f^{-1}(P)$ is a prime ideal of R.

Proof.

The preimage of an ideal by a ring homomorphism is an ideal.

(See the post "The inverse image of an ideal by a ring homomorphism is an ideal" for a proof.)

Thus, $f^{-1}(P)$ is an ideal of R.

We prove that the ideal $f^{-1}(P)$ is prime.

Suppose that we have $ab \in f^{-1}(P)$ for $a, b \in R$. Then we have $f(ab) \in P$.

Since f is a ring homomorphism, we obtain

$$f(a)f(b) = f(ab) \in P.$$

Since P is a prime ideal, it follows that either $f(a) \in P$ or $f(b) \in P$.

Hence we have either $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$.

This proves that the ideal $f^{-1}(P)$ is prime.

The Inverse Image of an Ideal by a Ring Homomorphism is an Ideal

Problem 411

Let $f : R \to R'$ be a ring homomorphism. Let I' be an ideal of R' and let $I = f^{-1}(I)$ be the preimage of I by f. Prove that I is an ideal of the ring R.

Proof.

To prove $I = f^{-1}(I')$ is an ideal of R, we need to check the following two conditions:

1. For any $a, b \in I$, we have $a - b \in I$.
2. For any $a \in I$ and $r \in R$, we have $ra \in I$.

Let us first prove condition 1. Let $a, b \in I$. Then it follows from the definition of I that $f(a), f(b) \in I'$.
Since I' is an ideal (and hence an additive abelian group) we have $f(a) - f(b) \in I'$.
Since f is a ring homomorphism, it yields that

$$f(a - b) = f(a) - f(b) \in I'.$$

Thus we have $a - b \in I$, and condition 1 is met.
This implies that I is an additive abelian group of R.
Next, we check condition 2. Let $a \in I$ and $r \in R$. Since $a \in I$, we have $f(a) \in I'$.
Since I' is an ideal of R' and $f(r) \in R'$, we have $f(r)f(a) \in I'$.
Since f is a ring homomorphism, it follows that

$$f(ra) = f(r)f(a) \in I',$$

and hence $ra \in I$. So condition 2 is also met and we conclude that I is an ideal of R.

Comment.

Instead of condition 1, we could have used
Condition 1′: For any $a, b \in I$, we have $a + b \in I$.
The reason is that condition 2 guarantee the existence of the additive inverses, and hence condition 1 and 2 are equivalent to condition 1′ and 2.

Polynomial $(x - 1)(x - 2) \cdots (x - n) - 1$ is Irreducible Over the Ring of Integers $\mathbb{Z}$

Problem 372

For each positive integer n, prove that the polynomial

$$(x - 1)(x - 2) \cdots (x - n) - 1$$

is irreducible over the ring of integers $\mathbb{Z}$.

Proof.

Note that the given polynomial has degree n.
Suppose that the polynomial is reducible over $\mathbb{Z}$ and it decomposes as

$$(x - 1)(x - 2) \cdots (x - n) - 1 = f(x)g(x) \qquad (*)$$

for some polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ of degree less than n.
Evaluating at $x = 1, 2, \dots, n$, we obtain

$$f(k)g(k) = -1$$

for $k = 1, 2, \dots, n$.

Since $f(x)$ and $g(x)$ have integer coefficients, both $f(k)$ and $g(k)$ are integers for $k = 1, 2, \dots, n$.

It follows that

$$f(k) = 1 = -g(k) \text{ or } f(k) = -1 = -g(k). \qquad (**)$$

Consider the polynomial $h(x) := f(x) + g(x) \in \mathbb{Z}[x]$.

Then we have

$$h(k) = f(k) + g(k) = 0$$

for $k = 1, 2, \dots, n$ by (**).

Thus, the polynomial $h(x)$ has at least n roots.

However, the degree of $h(x)$ is less than n as so are the degrees of $f(x)$ and $g(x)$.

This forces that $h(x) = 0$ for all x, and hence $f(x) = -g(x)$.

Then (*) becomes

$$(x-1)(x-2)\cdots(x-n) - 1 = -g(x)^2.$$

The leading coefficient of the left hand side is 1 but the leading coefficient of the right hand side is a negative number, hence it is a contradiction.

Therefore, the polynomial $(x-1)(x-2)\cdots(x-n) - 1$ must be irreducible over $\mathbb{Z}$.

If Two Ideals Are Comaximal in a Commutative Ring, then Their Powers Are Comaximal Ideals

Problem 360

Let R be a commutative ring and let I_1 and I_2 be **comaximal ideals**. That is, we have

$$I_1 + I_2 = R.$$

Then show that for any positive integers m and n, the ideals I_1^m and I_2^n are comaximal.

Proof.

Since $I_1 + I_2 = R$, there exists $a \in I_1$ and $b \in I_2$ such that

$$a + b = 1.$$

Then we have

$$\begin{aligned} 1 = 1^{m+n-1} &= (a+b)^{m+n-1} \\ &= \sum_{k=1}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} \\ &= \sum_{k=1}^{m-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} + \sum_{k=m}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k}. \end{aligned}$$

In the third equality, we used the binomial expansion.

Note that the first sum is in I_2^n since it is divisible by $b^n \in I_2^n$.

The second sum is in I_1^n since it is divisible by $a^m \in I_1^n$.

Thus the sum is in $I_1^m + I_2^n$, and hence we have $1 \in I_1^m + I_2^n$, which implies that $I_1^m + I_2^n = R$.

Every Maximal Ideal of a Commutative Ring is a Prime Ideal

Problem 351

Let R be a commutative ring with unity.
Then show that every maximal ideal of R is a prime ideal.

Proof 1.

The first proof uses the following facts.

- Fact 1. An ideal I of R is a prime ideal if and only if R/I is an integral domain.
- Fact 2. An ideal I of R is a maximal ideal if and only if R/I is a field.

Let M be a maximal ideal of R. Then by Fact 2, R/M is a field.
Since a field is an integral domain, R/M is an integral domain. Thus by Fact 1, M is a prime ideal.

Proof 2.

In this proof, we solve the problem without using Fact 1, 2.
Let M be a maximal ideal of R.
Seeking a contradiction, let us assume that M is not a prime ideal.
Then there exists $a, b \in R$ such that the product ab is in M but $a \notin M$ and $b \notin M$.
Consider the ideal $(a) + M$ generated by a and M.
Since the ideal $(a) + M$ is strictly larger than M, we must have $R = (a) + M$ by the maximality of M.
Since $1 \in R = (a) + M$, we have

$$1 = ra + m,$$

where $r \in R$ and $m \in M$.
Similarly, we have $R = (b) + M$ and

$$1 = sb + n,$$

where $s \in R$ and $n \in M$.
From these equalities, we obtain

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (ra + m)(sb + n) \\ &= rsab + ran + msb + mn. \end{aligned}$$

Since ab, m, n are elements in the ideal M, the last expression is in M.
This yields that $1 \in M$, and hence $M = R$. Since a maximal ideal is a proper ideal by definition, this is a contradiction.
Thus, R must be a prime ideal.

Prime ideals are Not Necessarily Maximal

We just have shown that every maximal ideal is a prime ideal.
The converse, however, is not true.
That is, some prime ideals are not maximal ideals.
See the post ↴

Examples of Prime Ideals in Commutative Rings that are Not Maximal Ideals

for examples of rings and prime ideals that are not maximal ideals.

A Maximal Ideal in the Ring of Continuous Functions and a Quotient Ring

Problem 345

Let R be the ring of all continuous functions on the interval $[0, 2]$.
Let I be the subset of R defined by

$$I := \{f(x) \in R \mid f(1) = 0\}.$$

Then prove that I is an ideal of the ring R.
Moreover, show that I is maximal and determine R/I.

Hint.

Consider the map $\phi : R \to \mathbb{R}$ defined by

$$\phi(f) = f(1),$$

for every $f(x) \in R$.

Proof.

Let us consider the map ϕ from R to the field of real numbers $\mathbb{R}$ defined by

$$\phi(f) = f(1),$$

for each $f(x) \in R$. Namely, the map ϕ is the evaluation at $x = 1$.

We claim that $\phi : R \to \mathbb{R}$ is a ring homomorphism. In fact we have for any $f(x), g(x) \in R$,

$$\begin{aligned} \phi(fg) &= (fg)(1) = f(1)g(1) = \phi(f)\phi(g) \\ \phi(f+g) &= (f+g)(1) = f(1) + g(1) = \phi(f) + \phi(g), \end{aligned}$$

hence ϕ is a ring homomorphism.

Next, consider the kernel of ϕ. We have

$$\begin{aligned} \ker(\phi) &= \{f(x) \in R \mid \phi(f) = 0\} \\ &= \{f(x) \in R \mid f(1) = 0\} = I. \end{aligned}$$

Since the kernel of a ring homomorphism is an ideal, it follows that $I = \ker(\phi)$ is an ideal of R.

Next, we claim that ϕ is surjective. To see this, let $r \in \mathbb{R}$ be an arbitrary real number.
Define the constant function $f(x) = r$. Then $f(x)$ is an element in R as it is continuous function on $[0, 2]$.
We have

$$\phi(f) = f(1) = r,$$

and this proves that ϕ is surjective.

Since $\phi : R \to \mathbb{R}$ is a surjective ring homomorphism, the first isomorphism theorem yields that

$$R/\ker(\phi) \cong \mathbb{R}.$$

Since $\ker(\phi) = I$ as we saw above, we have

$$R/I \cong \mathbb{R}.$$

Thus, the quotient ring R/I is isomorphic to the field $\mathbb{R}$.

It follows from this that I is a maximal ideal of R.

(Recall the fact that an ideal I of a commutative ring R is maximal if and only if R/I is a field.)

Related Question.

Problem.

Let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients.

Prove that

$$I = \{f(x) \in \mathbb{Z}[x] \mid f(-2) = 0\}$$

is a prime ideal of $\mathbb{Z}[x]$. Is I a maximal ideal of $\mathbb{Z}[x]$?

For a proof, see the post ↴

Polynomial Ring with Integer Coefficients and the Prime Ideal $I = \{f(x) \in \mathbb{Z}[x] \mid f(-2) = 0\}$

Irreducible Polynomial Over the Ring of Polynomials Over Integral Domain

Problem 333

Let R be an integral domain and let $S = R[t]$ be the polynomial ring in t over R. Let n be a positive integer.
Prove that the polynomial

$$f(x) = x^n - t$$

in the ring $S[x]$ is irreducible in $S[x]$.

Proof.

Consider the principal ideal (t) generated by t in S.

Then the ideal (t) is a prime ideal in S since the quotient

$$S/(t) = R[t]/(t) \cong R$$

is an integral domain.

The only non-leading coefficient of $f(x) = x^n - t$ is $-t$, and $-t$ is in the ideal (t) but not in the ideal $(t)^2$.

Then by Eisenstein's criterion, the polynomial $f(x)$ is irreducible in $S[x]$.

(Remark that $S = R[t]$ is an integral domain since R is an integral domain.)

Ring Homomorphisms from the Ring of Rational Numbers are Determined by the Values at Integers

Problem 318

Let R be a ring with unity.
Suppose that f and g are ring homomorphisms from $\mathbb{Q}$ to R such that $f(n) = g(n)$ for any integer n.
Then prove that $f = g$.

Proof.

Let $a/b \in \mathbb{Q}$ be an arbitrary rational number with integers a, b.

Then we have

$$\begin{aligned}
f\left(\frac{a}{b}\right) &= f\left(a \cdot \frac{1}{b}\right) \\
&= f(a)f\left(\frac{1}{b}\right) && (\text{since } f \text{ is a ring homomorphism}) \\
&= g(a)f\left(\frac{1}{b}\right) && (\text{since } a \text{ is an integer}) \\
&= g\left(\frac{a}{b} \cdot b\right)f\left(\frac{1}{b}\right) \\
&= g\left(\frac{a}{b}\right)g(b)f\left(\frac{1}{b}\right) && (\text{since } g \text{ is a ring homomorphism}) \\
&= g\left(\frac{a}{b}\right)f(b)f\left(\frac{1}{b}\right) && (\text{since } b \text{ is an integer}) \\
&= g\left(\frac{a}{b}\right)f\left(b \cdot \frac{1}{b}\right) && (\text{since } f \text{ is a ring homomorphism}) \\
&= g\left(\frac{a}{b}\right)f(1) \\
&= g\left(\frac{a}{b}\right) \cdot 1 \\
&= g\left(\frac{a}{b}\right).
\end{aligned}$$

Therefore, we proved

$$f\left(\frac{a}{b}\right) = g\left(\frac{a}{b}\right),$$

for any rational number $a/b \in \mathbb{Q}$.

Hence we have $f = g$.

Remark.

In the language of category theory, this shows that the inclusion $\mathbb{Z} \to \mathbb{Q}$ is epi in the category of rings.

Also, note that this inclusion is not epi in the category of abelian groups ($\mathbb{Z}$-mod).

Generators of the Augmentation Ideal in a Group Ring

Problem 302

Let R be a commutative ring with 1 and let G be a finite group with identity element e. Let RG be the group ring. Then the map $\epsilon : RG \to R$ defined by

$$\epsilon(\sum_{i=1}^{n} a_i g_i) = \sum_{i=1}^{n} a_i,$$

where $a_i \in R$ and $G = \{g_i\}_{i=1}^n$, is a ring homomorphism, called the **augmentation map** and the kernel of ϵ is called the **augmentation ideal**.

(a) Prove that the augmentation ideal in the group ring RG is generated by $\{g - e \mid g \in G\}$.

(b) Prove that if $G = \langle g \rangle$ is a finite cyclic group generated by g, then the augmentation ideal is generated by $g - e$.

Proof.

(a) The augmentation ideal in RG is generated by $\{g - e \mid g \in G\}$.

Let $I = \ker(\epsilon)$ be the augmentation ideal and let J be the ideal generated by elements of the form $g - e$, $g \in G$.

Since $\epsilon(g - e) = 1 - 1 = 0$, the generator $g - e \in I$. Hence $J \subset I$.

On the other hand, to show that $I \subset J$ let $\sum_{i=1}^n a_i g_i$ be an arbitrary element in the augmentation ideal I.

Then we have

$$\epsilon(\sum_{i=1}^n a_i g_i) = \sum_{i=1}^n a_i = 0. \tag{*}$$

Then we have

$$\begin{aligned} \sum_{i=1}^n a_i g_i &= \sum_{i=1}^n a_i (g_i - e) + \sum_{i=1}^n a_i e \\ &= \sum_{i=1}^n a_i (g_i - e) + (\sum_{i=1}^n a_i) e \\ &\overset{(*)}{=} \sum_{i=1}^n a_i (g_i - e). \end{aligned}$$

Therefore, the element $\sum_{i=1}^n a_i g_i$ is in the ideal J.

Putting the two inclusions together give $I = J$, which completes the proof of (a).

(b) The augmentation ideal is generated by $g - e$ if $G = \langle g \rangle$ is cyclic.

Now suppose $G = \langle g \rangle$ is a finite cyclic group of order n.

By part (a), the augmentation ideal is generated by

$$\{g^i - e \mid i = 0, 1, \dots, n-1\}.$$

Note that we have

$$g^k - e = (g - e)(g^{k-1} + g^{k-2} + \cdots + g + e)$$

for $k \geq 2$.

This implies that $g^k - e$ is contained in the ideal generated by $g - e$ for $k \geq 2$.

Hence the augmentation ideal of the cyclic group G is generated by $g - e$.

There is Exactly One Ring Homomorphism From the Ring of Integers to Any Ring

Problem 264

Let $\mathbb{Z}$ be the ring of integers and let R be a ring with unity.

Determine all the ring homomorphisms from $\mathbb{Z}$ to R.

Definition.

Recall that if A, B are rings with unity then a **ring homomorphism** $f : A \to B$ is a map satisfying

1. $f(x + y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$
3. $f(1_A) = 1_B$

for all $x, y \in A$ and $1_A, 1_B$ are unity elements of A and B, respectively.

Proof.

We claim that there is one and only one ring homomorphism from $\mathbb{Z}$ to R.

Let us first remark that there is at least one ring homomorphism $\mathbb{Z} \to R$.
Define the map $f_0 : \mathbb{Z} \to R$ by

$$f(n) = n.$$

Then it is clear that f_0 is a ring homomorphism from $\mathbb{Z}$ to R.
We want to prove that this is the only ring homomorphism.

Suppose that $f : \mathbb{Z} \to R$ is a ring homomorphism.
By definition, we must have

$$f(1) = 1_R.$$

Using property (1) with $x = y = 0$, we see that

$$f(0) = f(0) + f(0).$$

Thus, we have $f(0) = 0$.
Next, we apply (1) with $x = 1, y = -1$ and obtain

$$0 = f(0) = f(1 + (-1)) = f(1) + f(-1).$$

Thus we have

$$f(-1) = -f(1) = -1_R.$$

We want to determine the value $f(n)$ for any $n \in \mathbb{Z}$.
If n is a positive integer, then we can write it as

$$n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$$

By property (a) applied repeatedly, we have

$$\begin{aligned} f(n) &= \underbrace{f(1)+\cdots+f(1)}_{n \text{ times}} \\ &= \underbrace{1_R+\cdots+1_R}_{n \text{ times}} = n. \end{aligned}$$

If n is a negative integer, we express it as

$$n = \underbrace{(-1)+(-1)+\cdots+(-1)}_{n \text{ times}}$$

and obtain

$$\begin{aligned} f(n) &= \underbrace{f(-1)+f(-1)+\cdots+f(-1)}_{n \text{ times}} \\ &= \underbrace{(-1_R)+(-1_R)+\cdots+(-1_R)}_{n \text{ times}} = n. \end{aligned}$$

Therefore, we have proved that

$$f(n) = n$$

for any $n \in \mathbb{Z}$. Hence any ring homomorphism from $\mathbb{Z}$ to R is the ring homomorphism f_0 that we saw at the beginning of the proof.

In conclusion, there is exactly one ring homomorphism from $\mathbb{Z}$ to R, which is given by

$$f_0(n) = n$$

for any $n \in \mathbb{Z}$.

Comment.

In category theory, we say that the ring of integers $\mathbb{Z}$ is an **initial object** in the category of rings with unity.

Primary Ideals, Prime Ideals, and Radical Ideals

Problem 247

Let R be a commutative ring with unity. A proper ideal I of R is called **primary** if whenever $ab \in I$ for $a, b \in R$, then either $a \in I$ or $b^n \in I$ for some positive integer n.

(a) Prove that a prime ideal P of R is primary.

(b) If P is a prime ideal and $a^n \in P$ for some $a \in R$ and a positive integer n, then show that $a \in P$.

(c) If P is a prime ideal, prove that $\sqrt{P} = P$.

(d) If Q is a primary ideal, prove that the radical ideal $\sqrt{Q}$ is a prime ideal.

Definition.

For an ideal I of R, the **radical ideal** $\sqrt{I}$ is defined to be

$$\sqrt{Q} = \{a \in R \mid a^n \in Q \text{ for some positive integer } n\}.$$

Proof.

(a) A prime ideal is primary

To show that P is primary, suppose that $ab \in P$ for $a, b \in R$. Since P is a prime ideal, we have either $a \in P$ or $b \in P$.

This implies that P is a primary ideal. (We can always take $n = 1$ for a prime ideal.)

(b) If a^n is in the prime ideal P, then $a \in P$

Suppose that we have $a^n \in P$ for some $a \in R$ and a positive integer n. We prove that $a \in P$ by induction.

The base case $n = 1$ is trivial.

So assume that $a^k \in P$ implies $a \in P$ for some $k > 1$.

When $n = k + 1$, we want to show that $a^{k+1} \in P$ implies $a \in P$.

Since the product $a^{k+1} = a \cdot a^k$ of a and a^k is in the prime ideal P, we have either $a \in P$ or $a^k \in P$.

If the former is the case, we are done. If the latter is the case, then by the induction hypothesis, we also have $a \in P$.

Hence the induction step is completed, and the statement (b) is true for any positive integer n.

(c) If P is prime, then $\sqrt{P} = P$

Suppose that P is a prime ideal. By definition, it is clear that $P \subset \sqrt{P}$. We prove that the other inclusion $\sqrt{P} \subset P$.

Take an arbitrary element $a \in \sqrt{P}$.

Then there exists a positive integer n such that $a^n \in P$.

It follows from part (b) that this implies that $a \in P$ since P is a prime ideal. Thus we have proved $\sqrt{P} \subset P$, and hence $\sqrt{P} = P$.

(d) If Q is primary, then $\sqrt{Q}$ is prime

Suppose that Q is a primary ideal of R. To show that the radical ideal $\sqrt{Q}$ is prime, suppose that $ab \in \sqrt{Q}$. Our goal is to show that either $a \in \sqrt{Q}$ or $b \in \sqrt{Q}$.

Since $ab \in \sqrt{Q}$, there exists a positive integer n such that

$$(ab)^n \in Q.$$

Since R is commutative, this implies that we have

$$a^n \cdot b^n \in Q.$$

Since Q is primary, this yields by definition that either

$$a^n \in Q \quad \text{or} \quad (b^n)^m \in Q$$

for some positive integer m.

By definition of the radical ideal, it follows that

$$a \in \sqrt{Q} \quad \text{or} \quad b \in \sqrt{Q},$$

and thus $\sqrt{Q}$ is a prime ideal.

$(x^3 - y^2)$ is a Prime Ideal in the Ring $R[x, y]$, R is an Integral Domain.

Problem 239

Let R be an integral domain. Then prove that the ideal $(x^3 - y^2)$ is a prime ideal in the ring $R[x, y]$.

Proof.

Consider the ring $R[t]$, where t is a variable. Since R is an integral domain, so is $R[t]$.

Define the function $\Psi : R[x,y] \to R[t]$ sending x to t^2 and y to t^3, and extend it to for any $f(x,y) \in R[x,y]$ by linearity.

Then the map Ψ is a ring homomorphism.

Our goal is to show that the kernel of Ψ is the ideal $(x^3 - y^2)$. If this is proved, then the first isomorphism theorem implies that $R[x,y]/(x^3-y^2)$ is a subring of the integral domain $R[t]$, and thus (x^3-y^2) is a prime ideal.

Therefore it suffices to show that $\ker(\Psi) = (x^3 - y^2)$.

Since we have

$$\Psi(x^3 - y^2) = (t^2)^3 - (t^3)^2 = t^6 - t^6 = 0,$$

one inclusion $(x^3 - y^2) \subset \ker(\Psi)$ is clear.

To show that the other inclusion $\ker(\Psi) \subset (x^3 - y^2)$, note that for any $f(x,y) \in R[x,y]$ we can write

$$f(x,y) = f_0(x) + f_1(x)y + (x^3 - y^2)g(x,y), \tag{*}$$

where $f_0(x), f_1(x) \in R[x]$ and $g(x,y) \in R[x,y]$.

To obtain this expression, note that we have

$$x^m y^n = -(x^3 - y^2)x^m y^{n-2} + x^{m+3}y^{n-2}$$

for integers m and $n \geq 2$.

Use this relation recursively (to the second term), we can express

$$x^m y^n = (x^3 - y^2)p(x,y) + q_0(x) + q_1(x)y$$

for some $p(x,y) \in R[x,y]$ and $q_0, q_1 \in R[x]$.

Hence we obtain the expression (*).

Suppose that $f(x,y) \in \ker(\Psi)$ and $f(x,y)$ can be written as in (*).

Then we have

$$\begin{aligned} 0 = \Psi(f(x,y)) &= f(t^2, t^3) \\ &= f_0(t^2) + f_1(t^2)t^3 + ((t^2)^3 - (t^3)^2)g(t^2,t^3) \\ &= f_0(t^2) + f_1(t^2)t^3. \end{aligned}$$

Note that the even terms of the polynomial $f_0(t^2) + f_1(t^2)t^3$ are $f_0(t^2)$, and the odd terms are $f_1(t^2)t^3$.

Thus, we have $f_0(t^2) = 0$, and $f_1(t^2) = 0$.

Equivalently, we have $f_0(x) = 0$ and $f_1(x) = 0$.

It follows that

$$f(x,y) = (x^3 - y^2)g(x,y)$$

and it is in the ideal $(x^3 - y^2)$.

Thus we prove that $\ker(\Psi) = (x^3 - y^2)$ as required.

Polynomial $x^4 - 2x - 1$ is Irreducible Over the Field of Rational Numbers $\mathbb{Q}$

Problem 234

Show that the polynomial

$$f(x) = x^4 - 2x - 1$$

is irreducible over the field of rational numbers $\mathbb{Q}$.

Proof.

We use the fact that $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $f(x+a)$ is irreducible for any $a \in \mathbb{Q}$.

We prove that the polynomial $f(x+1)$ is irreducible.

We have

$$\begin{aligned} f(x+1) &= (x+1)^4 - 2(x+1) - 1 \\ &= (x^4 + 4x^3 + 6x^2 + 4x + 1) - 2(x+1) - 1 \\ &= x^4 + 4x^3 + 6x^2 + 2x - 2. \end{aligned}$$

Then the polynomial $f(x+1)$ is monic and all the non-leading coefficients are divisible by the prime number 2.

Since the constant term is not divisible by 2^2, Eisenstein's criterion implies that the polynomial $f(x+1)$ is irreducible over $\mathbb{Q}$.

Therefore by the fact stated above, the polynomial $f(x)$ is also irreducible over $\mathbb{Q}$.

Characteristic of an Integral Domain is 0 or a Prime Number

Problem 228

Let R be a commutative ring with 1. Show that if R is an integral domain, then the characteristic of R is either 0 or a prime number p.

Definition of the characteristic of a ring.

The characteristic of a commutative ring R with 1 is defined as follows.

Let us define the map $\phi : \mathbb{Z} \to R$ by sending $n \in \mathbb{Z}$ to

$$\phi(n) = \begin{cases} \underbrace{1 + \cdots + 1}_{n \text{ times}} \text{ if } n > 0 \\ 0 \text{ if } n = 0 \\ -(\underbrace{1 + \cdots + 1}_{-n \text{ times}}) \text{ if } n < 0. \end{cases}$$

Then this map ϕ is a ring homomorphism and we define the **characteristic** c of R to be the integer c such that

$$\ker(\phi) = (c).$$

(Note that the kernel of ϕ is an ideal in $\mathbb{Z}$, and Z is a principal ideal domain (PID), thus such an integer c exists.)

Proof.

Let us now prove the problem.

Let c be the characteristic of an integral domain R.

Then by the first isomorphism theorem with the ring homomorphism $\phi : \mathbb{Z} \to R$ as above, we have an injective homomorphism

$$\mathbb{Z}/c\mathbb{Z} = \mathbb{Z}/\ker(\phi) \to R.$$

Since R is an integral domain, $\mathbb{Z}/c\mathbb{Z}$ is also an integral domain.

This yields that $c\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

Therefore $c = 0$ or c is a prime number.

5 is Prime But 7 is Not Prime in the Ring $\mathbb{Z}[\sqrt{2}]$

Problem 224

In the ring

$$\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\},$$

show that 5 is a prime element but 7 is not a prime element.

Hint.

An element p in a ring R is **prime** if p is non zero, non unit element and whenever p divide ab for $a, b \in R$, then p divides a or b.

Equivalently, an element p in the ring R is prime if the principal ideal (p) generated by p is a nonzero prime ideal of R.

Proof.

5 is a prime element in the ring $\mathbb{Z}[\sqrt{2}]$.

We first show that 5 is prime in the ring $\mathbb{Z}[\sqrt{2}]$.

Suppose that

$$5|(a + \sqrt{2}b)(c + \sqrt{2}d)$$

for $a + \sqrt{2}b, c + \sqrt{2}d \in \mathbb{Z}[\sqrt{2}]$.

By taking the norm, we obtain

$$25|(a^2 - 2b^2)(c^2 - 2d^2)$$

in $\mathbb{Z}$.

From this, we may assume that $5|a^2 - 2b^2$.

Now look at the following table.

a, b	$a^2, b^2 \pmod 5$	$2b^2 \pmod 5$
0	0	0
1	1	2
2	4	3
3	4	3
4	1	2

From this table, we see that $a^2 - 2b^2 = 0 \pmod 5$ if and only if a, b are both divisible by 5.

Therefore $5|a + \sqrt{2}b$, and 5 is a prime element in $\mathbb{Z}[\sqrt{2}]$.

7 is not a prime element in the ring $\mathbb{Z}[\sqrt{2}]$.

Next, we show that 7 is not a prime element in $\mathbb{Z}[\sqrt{2}]$.

To see this, note that we have

$$7 = (3 + \sqrt{2})(3 - \sqrt{2})$$

and 7 does not divide $3 + \sqrt{2}$ and $3 - \sqrt{2}$.

Hence 7 is not a prime element in the ring $\mathbb{Z}[\sqrt{2}]$.

Related Question.

Problem. Prove that the ring $\mathbb{Z}[\sqrt{2}]$ is a Euclidean Domain.

For a proof of this fact, see that post "The Ring $\mathbb{Z}[\sqrt{2}]$ is a Euclidean Domain".

A Prime Ideal in the Ring $\mathbb{Z}[\sqrt{10}]$

Problem 223

Consider the ring

$$\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$$

and its ideal

$$P = (2, \sqrt{10}) = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}, 2|a\}.$$

Show that p is a prime ideal of the ring $\mathbb{Z}[\sqrt{10}]$.

Definition of a prime ideal.

An ideal P of a ring R is a **prime ideal** if whenever we have $ab \in P$ for elements $a, b \in R$, then either $a \in P$ or $b \in P$.

Proof.

Suppose that $a + b\sqrt{10}, c + d\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ and the product

$$(a + b\sqrt{10})(c + d\sqrt{10}) \in P.$$

Then expanding the product, we have

$$ac + 10bd + (ad + bc)\sqrt{10} \in P.$$

Since $ac + 10bd$ must be even number, we have either a or c is even.
Hence either

$$a + b\sqrt{10} \in P \text{ or } c + d\sqrt{10} \in P,$$

and we conclude that P is a prime ideal.

Further Question.

In fact, it can be proved that P is a maximal ideal in the ring $\mathbb{Z}[\sqrt{10}]$.
For a proof, see the post "Determine the Quotient Ring $\mathbb{Z}[\sqrt{10}]/(2, \sqrt{10})$".

If a Prime Ideal Contains No Nonzero Zero Divisors, then the Ring is an Integral Domain

Problem 220

Let R be a commutative ring. Suppose that P is a prime ideal of R containing no nonzero zero divisor. Then show that the ring R is an integral domain.

Definitions: zero divisor, integral domain

An element a of a commutative ring R is called a **zero divisor** if there is $b \neq 0$ in R such that $ab = 0$.

If a ring R contains no nonzero zero divisors, then we call R an **integral domain**.

Proof.

Suppose that we have

$$ab = 0$$

for $a, b \in R$. To show that R has no nonzero zero divisors, we need to prove that a or b is the zero element.
Since $ab = 0 \in P$ and P is a prime ideal, either $a \in P$ or $b \in P$.
Without loss of generality, we may assume $a \in P$.
If $a = 0$, then we are done.
So assume that $a \neq 0$. Then since P does not contain any nonzero zero divisor, we must have $b = 0$, otherwise $ab = 0, b \neq 0$ means that a is a nonzero zero divisor in P.
Therefore, in any case we have either $a = 0$ or $b = 0$, and thus the ring R contains no nonzero zero divisors.
Hence R is an integral domain.

How Many Solutions for $x + x = 1$ in a Ring?

Problem 204

Is there a (not necessarily commutative) ring R with 1 such that the equation

$$x + x = 1$$

has more than one solutions $x \in R$?

Solution.

We claim that there is at most one solution x in the ring R.
Suppose that we have two solutions $r, s \in R$. That is, we have

$$r + r = 1 \text{ and } s + s = 1.$$

Then we have $r + r = s + s$. Putting $a = r - s \in R$, we have

$$a + a = 0.$$

Now we compute

$$\begin{aligned} 0 &= 1 \cdot 0 = (r + r)(a + a) \\ &= ra + ra + ra + ra \\ &= (r + r)a + r(a + a) \\ &= 1 \cdot a + r \cdot 0 \\ &= a. \end{aligned}$$

Therefore we obtain $a = 0$ and thus $r = s$.
It follows that the equation $x + x = 1$ has only one solution (at most).

Ideal Quotient (Colon Ideal) is an Ideal

Problem 203

Let R be a commutative ring. Let S be a subset of R and let I be an ideal of I.
We define the subset

$$(I : S) := \{a \in R \mid aS \subset I\}.$$

Prove that $(I : S)$ is an ideal of R. This ideal is called the ***ideal quotient***, or ***colon ideal***.

Proof.

Let $a, b \in (I : S)$ and let $r \in R$. To show that $(I : S)$ is an ideal of the ring R, it suffices to show that the element $a + rb \in (I : S)$.

Thus we show that

$$(a + br)S \subset I.$$

Let $s \in S$ be an arbitrary element. Then since $a, b \in (I : S)$, we have $as, bs \in I$.

Since I is an ideal of R, we have $r(bs) \in I$ as well.

Thus

$$(a + rb)s = as + r(bs) \in I$$

for any $s \in S$, and hence we obtain $(a + br)S \subset I$.

By the definition of the ideal quotient, we have $a + br \in (I : S)$, and hence $(I : S)$ is an ideal of the ring R.

Non-Prime Ideal of Continuous Functions

Problem 199

Let R be the ring of all continuous functions on the interval $[0, 1]$.

Let I be the set of functions $f(x)$ in R such that $f(1/2) = f(1/3) = 0$.

Show that the set I is an ideal of R but is not a prime ideal.

Proof.

We first show that I is an ideal of R.

Let $f(x), g(x) \in R$ and $r \in R$.

Then the function $f(x) + rg(x)$ is a continuous function on $[0, 1]$ and we have

$$(f(x) + rg(x))(1/2) = f(1/2) + rg(1/2) = 0 + r \cdot 0 = 0$$

since $f(1/2) = g(1/2) = 0$.

Similarly, we have $(f(x) + rg(x))(1/3) = 0$.

Hence $f(x) + rg(x) \in I$, and thus I is an ideal of R.

Next, we show that the ideal I is not a prime ideal.

Let us define

$$f(x) = x - \frac{1}{3} \text{ and } g(x) = x - \frac{1}{2}.$$

Then the functions $f(x), g(x)$ are continuous on $[0, 1]$, hence they are elements in R.

Since we have

$$f\left(\frac{1}{2}\right) = \frac{1}{2} - \frac{1}{3} = \frac{1}{6} \neq 0 \text{ and } g\left(\frac{1}{3}\right) = \frac{1}{3} - \frac{1}{2} = -\frac{1}{6} \neq 0,$$

the functions $f(x), g(x)$ are not in the ideal I.

However, the product $f(x)g(x)$ is in I since we have

$$f\left(\frac{1}{2}\right)g\left(\frac{1}{2}\right)=\left(\frac{1}{2}-\frac{1}{3}\right)\left(\frac{1}{2}-\frac{1}{2}\right)=0$$
$$f\left(\frac{1}{3}\right)g\left(\frac{1}{3}\right)=\left(\frac{1}{3}-\frac{1}{3}\right)\left(\frac{1}{3}-\frac{1}{2}\right)=0.$$

In summary, the functions $f(x)$ and $g(x)$ are not in I but the product $f(x)(g)$ is in I. Thus the ideal I is not a prime ideal.

The Ideal (x) is Prime in the Polynomial Ring $R[x]$ if and only if the Ring R is an Integral Domain

Problem 198

Let R be a commutative ring with 1. Prove that the principal ideal (x) generated by the element x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain.
Prove also that the ideal (x) is a maximal ideal if and only if R is a field.

Proof.

We claim that we have a ring isomorphism

$$R[x]/(x)\cong R.$$

Let us for the moment assume that this claim is true and prove the problem.
If the ideal (x) is a prime ideal of $R[x]$, then $R[x]/(x)$ is an integral domain.
Hence, by the claim $R\cong R[x]/(x)$ is also an integral domain.
On the other hand, if R is an integral domain, then $R[x]/(x)$ is also an integral domain.
This yields that the ideal (x) is a prime ideal.
Similarly, we see that the ideal (x) is a maximal ideal if and only if $R\cong R[x]/(x)$ is a field.
Thus it remains to prove the claimed isomorphism of rings.

Proof of the claim

Define

$$\Psi : R[x]\to R$$

by mapping $f(x)\in R[x]$ to $f(0)\in R$. (Evaluating the polynomial $f(x)$ at $x=0$.)
Then the map Ψ is a ring homomorphism since we have for $f,g\in R[x]$ and $r\in R$

$$\begin{aligned}\Psi(f+g)&=(f+g)(0)=f(0)+g(0)=\Psi(f)+\Psi(g)\\ \Psi(rf)&=(rf)(0)=rf(0)=r\Psi(f).\end{aligned}$$

The homomorphism Ψ is surjective since for any $r\in R$, letting $f(x)=r$ we see that $\Psi(f)=r$.
Therefore by the isomorphism theorem for rings, we have

$$R[x]/\ker(\Psi)\cong R. \qquad (*)$$

It remains to show that

$$\ker(\Psi)=(x).$$

($\implies$) Let $f \in \ker(\Psi)$. Then we have $\Psi(f) = f(0) = 0$.
Let us write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Then since $f(0) = 0$, we have $a_0 = 0$ and thus we have

$$f(x) = x(a_n x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in (x).$$

Thus $\ker(\Psi) \subset R$.

($\impliedby$) Let $f \in (x)$. Then we can write f as $f = xg$ for some $g \in R[x]$.
It follows that we have

$$\Psi(f) = f(0) = 0 \cdot g(0) = 0$$

and $f \in \ker(\Psi)$.
Hence $R \subset \ker(\Psi)$.

Thus putting the two inclusions together gives $\ker(\Psi) = (x)$, and combining this with the isomorphism (*) we obtain

$$R[x]/(x) \cong R$$

as claimed.

If the Quotient Ring is a Field, then the Ideal is Maximal

Problem 197

Let R be a ring with unit $1 \neq 0$.
Prove that if M is an ideal of R such that R/M is a field, then M is a maximal ideal of R.
(Do not assume that the ring R is commutative.)

Proof.

Let I be an ideal of R such that

$$M \subset I \subset R.$$

Then I/M is an ideal of R/M.
Since R/M is a field by assumption, the only ideals of the field R/M is $\bar{0} = M/M$ or R/M itself.
So the ideal I/M is either $\bar{0}$ or R/M.
By the fourth (or lattice) isomorphism theorem for rings, there is a one-to-one correspondence between the set of ideals of R containing M and the set of ideals of R/M. Hence I must be either M or R.
(Since the fourth isomorphism theorem gives the correspondence $M \leftrightarrow M/M = \bar{0}$ and $R \leftrightarrow R/M$, and there is no ideal of R/M between $\bar{0}$ and R/M.)
Therefore the ideal M is maximal.

Finite Integral Domain is a Field

Problem 192

Show that any finite integral domain R is a field.

Definition.

A commutative ring R with $1 \neq 0$ is called an **integral domain** if it has no zero divisors.
That is, if $ab = 0$ for $a, b \in R$, then either $a = 0$ or $b = 0$.

Proof.

We give two proofs.

Proof 1.

Let $r \in R$ be a nonzero element in R.
We show that r is a unit.
Consider the map $f : R \to R$ sending $x \in R$ to $f(x) = rx$.
We claim that the map f is injective.
Suppose that we have $f(x) = f(y)$ for $x, y \in R$. Then we have

$$rx = ry$$

or equivalently, we have

$$r(x - y) = 0.$$

Since R is an integral domain and $r \neq 0$, we must have $x - y = 0$, and thus $x = y$.
Hence f is injective. Since R is a finite set, the map is also surjective.
Then it follows that there exists $s \in R$ such that $rs = f(s) = 1$, and thus r is a unit.
Since any nonzero element of a commutative ring R is a unit, R is a field.

Proof 2.

Let $r \in R$ be a nonzero element.
We show that the inverse element of r exists in R as follows.
Consider the powers of r:

$$r, r^2, r^3, \dots.$$

Since R is a finite ring, not all of the powers cannot be distinct.
Thus, there exist positive integers $m > n$ such that

$$r^m = r^n.$$

Equivalently we have

$$r^n(r^{m-n} - 1) = 0.$$

Since R is an integral domain, this yields either $r^n = 0$ or $r^{m-n} - 1 = 0$.
But the former gives $r = 0$, and this is a contradiction since $r \neq 0$.
Hence we have $r^{m-n} = 1$, and thus

$$r \cdot r^{m-n-1} = 1.$$

Since $r-m-1 \geq 0$, we have $r^{m-n-1} \in R$ and it is the inverse element of r.

Therefore, any nonzero element of R has the inverse element in R, hence R is a field.

Ring of Gaussian Integers and Determine its Unit Elements

Problem 188

Denote by i the square root of -1.

Let

$$R=\mathbb{Z}[i]=\{a+ib \mid a,b \in \mathbb{Z}\}$$

be the ring of Gaussian integers.

We define the norm $N : \mathbb{Z}[i] \to \mathbb{Z}$ by sending $\alpha=a+ib$ to

$$N(\alpha)=\alpha\bar{\alpha}=a^2+b^2.$$

Here $\bar{\alpha}$ is the complex conjugate of α.

Then show that an element $\alpha \in R$ is a unit if and only if the norm $N(\alpha)=\pm 1$.

Also, determine all the units of the ring $R=\mathbb{Z}[i]$ of Gaussian integers.

Proof.

Suppose that an element α is a unit of R.

Then there exists $\beta \in R$ such that $\alpha\beta=1$.

Then the norm of $\alpha\beta$ is

$$\begin{aligned} N(\alpha\beta)&=(\alpha\beta)(\overline{\alpha\beta}) \\ &=\alpha\bar{\alpha}\beta\bar{\beta} \\ &=N(\alpha)N(\beta). \end{aligned}$$

Since the norm $N(1)=1$, we obtain

$$1=N(\alpha)N(\beta)$$

in the ring $\mathbb{Z}$. Since $N(\alpha)$ and $N(\beta)$ are both integers, it follows that we have

$$N(\alpha)=\pm 1 \text{ and } N(\beta)=\pm 1.$$

On the other hand, suppose that $N(\alpha)=\pm 1$ for an element $\alpha \in R$.

Then let $\beta:=N(\alpha)^{-1}\bar{\alpha}$.

Since $N(\alpha)^{-1}=\pm 1$, the element $\beta \in R$. We have

$$\begin{aligned} \beta\alpha&=N(\alpha)^{-1}\bar{\alpha}\cdot\alpha \\ &=N(\alpha)^{-1}N(\alpha)=1. \end{aligned}$$

Thus the element α is a unit in R.

Using this result, let us determine all units of the ring R of Gaussian integers.

An element $\alpha=a+ib \in R$ is a unit if and only if

$$N(\alpha)=a^2+b^2=1,$$

where $a,b \in \mathbb{Z}$. Thus only solutions are

$$(a,b)=(\pm 1,0),(0,\pm 1).$$

Therefore the units of $R = \mathbb{Z}[i]$ are

$$\pm 1, \pm i.$$

$\sqrt[m]{2}$ is an Irrational Number

Problem 179

Prove that $\sqrt[m]{2}$ is an irrational number for any integer $m \geq 2$.

Hint.

Use ring theory:

1. Consider the polynomial $f(x) = x^m - 2$.
2. Apply Eisenstein's criterion, show that $f(x)$ is irreducible over $\mathbb{Q}$.

Proof.

Consider the monic polynomial $f(x) = x^m - 2$ in $\mathbb{Z}[x]$.
The constant term is divisible by the prime 2 and not divisible by 2^2.
Thus, by Eisenstein's criterion, the polynomial $f(x)$ is irreducible over the rational numbers $\mathbb{Q}$.
In particular, it does not have a degree 1 factor.
If $\sqrt[m]{2}$ is rational, then $x - \sqrt[m]{2} \in Q[x]$ is a degree 1 factor of $f(x)$ and this cannot happen.
Therefore, $\sqrt[m]{2}$ is an irrational number for any integer $m \geq 2$.

The Ideal Generated by a Non-Unit Irreducible Element in a PID is Maximal

Problem 177

Let R be a principal ideal domain (PID). Let $a \in R$ be a non-unit irreducible element.
Then show that the ideal (a) generated by the element a is a maximal ideal.

Proof.

Suppose that we have an ideal I of R such that

$$(a) \subset I \subset R.$$

Since R is a PID, there exists $b \in R$ such that $I = (b)$. As $a \in (a) \subset I = (b)$, we can write

$$a = bc$$

for some $c \in R$.
The irreducibility of the element a yields that either b or c is a unit element of R .
If b is a unit, then $I = (b) = R$. If c is a unit then we have $c' \in R$ such that $cc' = 1$.
Then $b = b \cdot 1 = bcc' = ac'$, and we have $I = (b) = (a)$.
Therefore, in either case, we see that we have $I = (a)$ or $I = R$.
Thus, (a) is a maximal ideal.

In a Principal Ideal Domain (PID), a Prime Ideal is a Maximal Ideal

Problem 175

Let R be a principal ideal domain (PID) and let P be a nonzero prime ideal in R.
Show that P is a maximal ideal in R.

Definition

A commutative ring R is a **principal ideal domain** (**PID**) if R is a domain and any ideal I is generated by a single element $a \in I$, that is $I = (a)$.

Proof.

Since R is a PID, we can write $P = (a)$, an ideal generated by an element $a \in R$.
Since P is a nonzero ideal, the element $a \neq 0$.
Now suppose that we have

$$P \subset I \subset R$$

for some ideal I of R.
We can write $I = (b)$ for some $b \in R$ since R is a PID.
The element $a \in (a) \subset (b)$ and so there is an element $c \in R$ such that $a = bc$.
Since $a = bc$ is in the prime ideal P, we have either $b \in P$ or $c \in P$.
If $b \in P$, then it follows that $I = (b) \subset P$, and hence $P = I$.
If $c \in P = (a)$, then we have $d \in R$ such that $c = ad$.
Then we have

$$a = bc = bad$$

and since R is a domain and $a \neq 0$, we have

$$1 = bd.$$

This yields that b is a unit and hence $I = (b) = R$.
In summary, we observe that whenever we have $P \subset I \subset R$, we have either $I = P$ or $I = R$. Thus P is a maximal ideal.

Equivalent Conditions For a Prime Ideal in a Commutative Ring

Problem 174

Let R be a commutative ring and let P be an ideal of R. Prove that the following statements are equivalent:
(a) The ideal P is a prime ideal.
(b) For any two ideals I and J, if $IJ \subset P$ then we have either $I \subset P$ or $J \subset P$.

Proof.

(a) $\Longrightarrow$ (b)

Suppose that P is a prime ideal. Let I and J be ideals such that $IJ \subset P$. Assume that

$$I \not\subset P \text{ and } J \not\subset P.$$

Then there exist

$$a \in I \setminus P \text{ and } b \in J \setminus P.$$

Then the element ab is in both I and J since I, J are ideals. Then we have

$$ab \in IJ \subset P$$

and this implies either $a \in P$ or $b \in P$ since P is a prime ideal.

However, this contradicts the choice of the elements a, b.

Therefore, we must have

$$I \subset P \text{ or } J \subset P.$$

(b) $\implies$ (a)

Now we assume statement (b) is true.

Suppose that $ab \in P$, where $a, b \in R$.

Let $I = (a), J = (b)$ be ideals generated by a and b, respectively.

Then we have

$$IJ = (ab) \subset P$$

since $ab \in P$, and statement (b) implies that we have either $(a) = I \subset P$ or $(b) = J \subset P$.

Hence we have either $a \in P$ or $b \in P$.

Thus P is a prime ideal.

Prime Ideal is Irreducible in a Commutative Ring

Problem 173

Let R be a commutative ring. An ideal I of R is said to be **irreducible** if it cannot be written as an intersection of two ideals of R which are strictly larger than I.

Prove that if $\mathfrak{p}$ is a prime ideal of the commutative ring R, then $\mathfrak{p}$ is irreducible.

Proof.

Suppose that the ideal $\mathfrak{p}$ is reducible. Then there exist ideals I_1 and I_2 such that

$$\mathfrak{p} = I_1 \cap I_2, \text{ and } \mathfrak{p} \subsetneq I_1, \mathfrak{p} \subsetneq I_2.$$

Since I_1, I_2 are strictly larger than $\mathfrak{p}$, there exists $a \in I_1 \setminus \mathfrak{p}$ and $b \in I_2 \setminus \mathfrak{p}$.

Then the product $ab \in I_1$ since a is in the ideal I_1. Also $ab \in I_2$ since b is in the ideal I_2.

Therefore $ab \in I_1 \cap I_2 = \mathfrak{p}$.

Since $\mathfrak{p}$ is a prime ideal and $ab \in \mathfrak{p}$, either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ but this contradicts with the choice of elements a and b.

Hence $\mathfrak{p}$ is irreducible.

Ring is a Filed if and only if the Zero Ideal is a Maximal Ideal

Problem 172

Let R be a commutative ring.

Then prove that R is a field if and only if $\{0\}$ is a maximal ideal of R.

Proof.

($\implies$): If R is a field, then $\{0\}$ is a maximal ideal

Suppose that R is a field and let I be a non zero ideal:

$$\{0\} \subsetneq I \subset R.$$

Then the ideal I contains a nonzero element $x \neq 0$. Since R is a field, we have the inverse $x^{-1} \in R$.

Then it follows that $1 = x^{-1}x \in I$ since x is in the ideal I.

Since $1 \in I$, any element $r \in R$ is in I as $r = r \cdot 1 \in I$.

Thus we have $I = R$ and this proves that $\{0\}$ is a maximal ideal of R.

($\Longleftarrow$): If $\{0\}$ is a maximal ideal, then R is a field

Let us now suppose that $\{0\}$ is a maximal ideal of R.

Let x be any nonzero element in R.

Then the ideal (x) generated by the element x properly contains the ideal $\{0\}$.

Since $\{0\}$ is a maximal ideal, we must have $(x) = R$.

Since $1 \in R = (x)$, there exists $y \in R$ such that $1 = xy$.

This implies that the element x is invertible. Therefore any nonzero element of R is invertible, and hence R is a field.

Nilpotent Element a in a Ring and Unit Element $1 - ab$

Problem 171

Let R be a commutative ring with $1 \neq 0$.

An element $a \in R$ is called **nilpotent** if $a^n = 0$ for some positive integer n.

Then prove that if a is a nilpotent element of R, then $1 - ab$ is a unit for all $b \in R$.

Proof 1.

Since a is nilpotent, we have $a^n = 0$ for some positive integer n.

Then for any $b \in R$, we have $(ab)^n = a^n b^n = 0$ since R is commutative.

Then we have the following equality:

$$(1 - ab)(1 + (ab) + (ab)^2 + \cdots + (ab)^{n-1}) = 1.$$

Therefore $1 - ab$ is a unit in R.

Proof 2.

There exists $n \in \mathbb{N}$ such that $a^n = 0$ since a is nilpotent.

Assume that $1 - ab$ is not a unit for some $b \in R$.

Then there exists a prime ideal $\mathfrak{p}$ of R such that $\mathfrak{p} \ni 1 - ab$.

Since $a^n = 0 \in \mathfrak{p}$, we have $a \in \mathfrak{p}$ since $\mathfrak{p}$ is an prime ideal.

Then $ab \in \mathfrak{p}$ and we have

$$1 = (1 - ab) + ab \in \mathfrak{p}.$$

However, this implies that $\mathfrak{p} = R$ and this is a contradiction. Thus $1 - ab$ is a unit of the ring R for all $b \in R$.

Rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are Not Isomorphic

Problem 170

Prove that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Definition of a ring homomorphism.

Let R and S be rings.

- A homomorphism is a map $f : R \to S$ satisfying
  1. $f(a+b) = f(a) + f(b)$ for all $a, b \in R$, and
  2. $f(ab) = f(a)f(b)$ for all $a, b \in R$.
- A bijective ring homomorphism is called an isomorphism.
- If there is an isomorphism from R to S, then we say that rings R and S are isomorphic (as rings).

Proof.

Suppose that the rings are isomorphic. Then we have a ring isomorphism

$$f : 2\mathbb{Z} \to 3\mathbb{Z}.$$

Let us put $f(2) = 3a$ for some integer a. Then we compute $f(4)$ in two ways.
First we have

$$f(4) = f(2+2) = f(2) + f(2) = 3a + 3a = 6a.$$

Next we have

$$f(4) = f(2 \cdot 2) = f(2) \cdot f(2) = 3a \cdot 3a = 9a^2.$$

These are equal and hence we have

$$6a = 9a^2.$$

The only integer solution is $a = 0$.
But then we have $f(0) = 0 = f(2)$, which contradicts that f is an isomorphism (hence in particular injective).
Therefore, there is no such isomorphism f, thus the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Problems in Module Theory

A Module M is Irreducible if and only if M is isomorphic to R/I for a Maximal Ideal I.

Problem 449

Let R be a commutative ring with 1 and let M be an R-module.
Prove that the R-module M is irreducible if and only if M is isomorphic to R/I, where I is a maximal ideal of R, as an R-module.

Definition (Irreducible module).

An R-module M is called **irreducible** if M is not the zero module and 0 and M are the only submodules of M.
An irreducible module

is also called a **simple** module.

Proof.

$(\implies)$ Suppose that M is an irreducible R-module.
Then by definition of an irreducible module, M is not the zero module.

Take any nonzero element $m \in M$, and consider the cyclic submodule $(m) = Rm$ generated by m.
Since M is irreducible, we must have $M = Rm$.
Now we define a map $f : R \to M$ by sending $r \in R$ to $f(r) = rm$.
Then the map f is an R-module homomorphism regarding R is an R-module.
In fact, we have

$$f(r+s) = (r+s)m = rm + sm = f(r) + f(s)$$
$$f(rs) = (rs)m = r(sm) = rf(s)$$

for any $r, s \in R$.
Since $M = Rm$, the homomorphism f is surjective.
Thus, by the first isomorphism theorem, we obtain

$$R/I \cong M,$$

where $I = \ker(f)$.
It remains to show that I is a maximal ideal of R.
Suppose that J is an ideal such that $I \subset J \subset R$.
Then by the third isomorphism theorem for rings, we know that J/I is an ideal of the ring $R/I \cong M$, hence J/I is a submodule.
Since M is irreducible, we must have either $J/I = 0$ or $J/I = M$.
This implies that $J = I$ or $J = M$.
Hence I is a maximal ideal.

($\Longleftarrow$) Suppose now that $M \cong R/I$ for some maximal ideal I of R.
Let N be any submodule of R/I. (We identified M and R/I by the above isomorphism.)
Then N is an ideal of R/I since N is an abelian group and closed under the action of R, hence that of R/I.
Since R is a commutative ring and I is a maximal ideal of R, we know that R/I is a field.
Thus, only the ideals of R/I are 0 or R/I.
Hence we have $N = 0$ or $N = R/I = M$.
This proves that M is irreducible.

Related Question.

A similar technique in the proof above can be used to solve the following problem.

Problem. Let R be a ring with 1.
Prove that a nonzero R-module M is irreducible if and only if M is a cyclic module with any nonzero element as its generator.

See the post "A module is irreducible if and only if it is a cyclic module with any nonzero element as generator" for a proof.

A Module is Irreducible if and only if It is a Cyclic Module With Any Nonzero Element as Generator

Problem 434

Let R be a ring with 1.
A nonzero R-module M is called **irreducible** if 0 and M are the only submodules of M.
(It is also called a **simple** module.)
(a) Prove that a nonzero R-module M is irreducible if and only if M is a cyclic module with any nonzero element as its generator.
(b) Determine all the irreducible $\mathbb{Z}$-modules.

Proof.

(a) Prove that a nonzero R-module M is irreducible if and only if M is a cyclic module with any nonzero element as its generator.

$(\implies)$ Suppose that M is an irreducible module.
Let $a \in M$ be any nonzero element and consider the submodule (a) generated by the element a.
Since a is a nonzero element, the submodule (a) is non-zero. Since M is irreducible, this yields that

$$M = (a).$$

Hence M is a cyclic module generated by a. Since a is any nonzero element, we conclude that the module M is a cyclic module with any nonzero element as its generator.

$(\impliedby)$ Suppose that M is a cyclic module with any nonzero element as its generator.
Let N be a nonzero submodule of M. Since N is non-zero, we can pick a nonzero element $a \in N$. By assumption, the non-zero element a generates the module M.
Thus we have

$$(a) \subset N \subset M = (a).$$

It follows that $N = M$, and hence M is irreducible.

(b) Determine all the irreducible $\mathbb{Z}$-modules.

By the result of part (a), any irreducible $\mathbb{Z}$-module is generated by any nonzero element.
We first claim that M cannot contain an element of infinite order. Suppose on the contrary $a \in M$ has infinite order.
Then since M is irreducible, we have

$$M = (a) \cong \mathbb{Z}.$$

Since $\mathbb{Z}$-module $\mathbb{Z}$ has, for example, a proper submodule $2\mathbb{Z}$, it is not irreducible. Thus, the module M is not irreducible, a contradiction.
It follows that any irreducible $\mathbb{Z}$-module is a finite cyclic group.
(Recall that any $\mathbb{Z}$-module is an abelian group.)
We claim that its order must be a prime number.
Suppose that $M = \mathbb{Z}/n\mathbb{Z}$, where $n = ml$ with $m, l > 1$.
Then

$$(\bar{l}\,) = \{l + n\mathbb{Z}, 2l + n\mathbb{Z}, \dots, (m-1)l + n\mathbb{Z}\}$$

is a proper submodule of M, and it is a contradiction.
Thus, n must be prime.

We conclude that any irreducible $\mathbb{Z}$-module is a cyclic group of prime order.

Related Question.

Here is another problem about irreducible modules.

Problem. Let R be a commutative ring with 1 and let M be an R-module.
Prove that the R-module M is irreducible if and only if M is isomorphic to R/I, where I is a maximal ideal of R, as an R-module.

For a proof of this problem, see the post "A Module M is Irreducible if and only if M is isomorphic to R/I for a Maximal Ideal I.".

Finitely Generated Torsion Module Over an Integral Domain Has a Nonzero Annihilator

Problem 432

(a) Let R be an integral domain and let M be a finitely generated torsion R-module.
Prove that the module M has a nonzero annihilator.
In other words, show that there is a nonzero element $r \in R$ such that $rm = 0$ for all $m \in M$.
Here r does not depend on m.
(b) Find an example of an integral domain R and a torsion R-module M whose annihilator is the zero ideal.

Proof.

(a) Prove that the module M has a nonzero annihilator.

Since M is a finitely generated R-module, there is a finite set

$$A := \{a_1, a_2, \dots, a_n\} \subset M$$

such that $M = RA$
As M is a torsion R-module, for each $a_i \in A \subset M$ there is a nonzero element $r_i \in R$ such that

$$r_i a_i = 0.$$

Let us put $r \in R$ to be the product of these r_i:

$$r := r_1 r_2 \cdots r_n.$$

Note that r is a nonzero element of R since each r_i is nonzero and R is an integral domain.
We claim that the element r annihilates the module M.
Let m be an arbitrary element in M. Since M is generated by the set A, we can write

$$m = s_1 a_1 + s_2 a_2 + \cdots + s_n a_n$$

for some elements $s_1, s_2, \dots, s_n \in R$.

Note that since R is an integral domain, it is commutative by definition.
Hence we can change the order of the product in r freely. Thus for each i we can write

$$r = p_i r_i,$$

where p_i is the product of all r_j except r_i.

Then it follows that we have

$$ra_i = p_i r_i a_i = p_i 0 = 0 \tag{*}$$

for each i.

Using this, we obtain

$$\begin{aligned} rm &= r(s_1a_1 + s_2a_2 + \cdots + s_na_n) \\ &= rs_1a_1 + rs_2a_2 + \cdots + rs_na_n \\ &= s_1ra_1 + s_2ra_2 + \cdots + s_nra_n && \text{as } R \text{ is commutative} \\ &= s_10 + s_20 + \cdots + s_n0 && \text{by (*)} \\ &= 0. \end{aligned}$$

Therefore, for any element $m \in M$ we have proved that $rm = 0$.

Thus the nonzero element r annihilates the module M.

(b) Find an example of an integral domain R and a torsion R-module M whose annihilator is the zero ideal.

Let $R = \mathbb{Z}$ be the ring of integers. Then $R = \mathbb{Z}$ is an integral domain.

Consider the $\mathbb{Z}$-module

$$M = \oplus_{i=1}^{\infty} \mathbb{Z}/2^i\mathbb{Z}.$$

Then each element $a \in M$ can be written as

$$a = (a_1 + \mathbb{Z}/2\mathbb{Z}, a_2 + \mathbb{Z}/2^2\mathbb{Z}, \dots, a_k + \mathbb{Z}/2^k\mathbb{Z}, 0, 0, \dots)$$

for some $a_1, a_2, \dots, a_k \in \mathbb{Z}$.

(Here k depends on a.)

It follows that we have

$$2^k a = 0,$$

and thus M is a torsion $\mathbb{Z}$-module.

We now prove that any annihilator of M must be the zero element of $R = \mathbb{Z}$.

Let $r \in \mathbb{Z}$ be an annihilator of M.

Choose an integer k so that $r < 2^k$. Consider the element

$$a = (0, 0, \dots, 1 + \mathbb{Z}/2^k\mathbb{Z}, 0, 0, \dots)$$

in M. The only nonzero entry of a is at the k-th place. Since r is an annihilator, we have

$$0 = ra = (0, 0, \dots, r + \mathbb{Z}/2^k\mathbb{Z}, 0, 0, \dots)$$

and this implies that $r = 0$ because $r < 2^k$. We conclude that the annihilator is the zero ideal.

Nilpotent Ideal and Surjective Module Homomorphisms

Problem 431

Let R be a commutative ring and let I be a nilpotent ideal of R.
Let M and N be R-modules and let $\phi : M \to N$ be an R-module homomorphism.
Prove that if the induced homomorphism $\bar{\phi} : M/IM \to N/IN$ is surjective, then ϕ is surjective.

Proof.

Since the homomorphism $\bar{\phi} : M/IM \to N/IN$ is surjective, for any $b \in N$ there exists $a \in M$ such that

$$\bar{\phi}(\bar{a}) = \bar{b}, \tag{*}$$

where $\bar{a} = a + IM$ and $\bar{b} = b + IN$.
By definition of $\bar{\phi} : M/IM \to N/IN$, we have

$$\bar{\phi}(\bar{a}) = \overline{\phi(a)} = \phi(a) + IN.$$

Thus, it follows from (*) that

$$\phi(a) + IN = b + IN,$$

or equivalently

$$b - \phi(a) \in IN.$$

Thus we have

$$b \in \phi(M) + IN.$$

Now we claim that for any $b \in N$ and any positive integer k, we have

$$b \in \phi(M) + I^k N.$$

We prove this claim by induction on k.
The base case $k = 1$ is proved above.
Suppose that $b \in \phi(M) + I^n N$. Then we prove that $b \in \phi(M) + I^{n+1} N$.
Since $b \in \phi(M) + I^n N$, we have

$$b = \phi(a) + \sum_i \alpha_i c_i,$$

where the sum is finite and $\alpha_i \in I^n$ and $c_i \in N$.
Since each $c_i \in N$, we have $c_i \in \phi(M) + IN$ by the base case.
Hence we have

$$c_i = \phi(a_i) + \sum_{j_i} \beta_{j_i} d_{j_i}$$

for some finite pairs $(\beta_{j_i}, d_{j_i}) \in (I, N)$.
It follows that we have

$$\begin{aligned} b &= \phi(a) + \sum_i \alpha_i c_i \\ &= \phi(a) + \sum_i \alpha_i \left(\phi(a_i) + \sum_{j_i} \beta_{j_i} d_{j_i} \right) \\ &= \phi(a) + \sum_i \alpha_i \phi(a_i) + \sum_i \sum_{j_i} \alpha_i \beta_{j_i} d_{j_i} \\ &= \phi(a) + \sum_i \phi(\alpha_i a_i) + \sum_{i,j_i} (\alpha_i \beta_{j_i}) d_{j_i} \\ &= \phi \left(a + \sum_i \alpha_i a_i \right) + \sum_{i,j_i} (\alpha_i \beta_{j_i}) d_{j_i}, \end{aligned}$$

where the last two equalities follows since ϕ is an R-module homomorphism.
Since $\alpha_i \in I^n$ and $\beta_{j_i} \in I$, the product $\alpha_i \beta_{j_i} \in I^{n+1}$.
Hence the above expression of b yields that

$$b \in \phi(M) + I^{n+1} N,$$

and this completes the induction step and the claim is proved.

Now, since I is a nilpotent ideal by assumption, there is a positive integer n such that I^n is the zero ideal of R.
Thus, it follows from the claim that for any $b \in N$ we have

$$b \in \phi(M) + I^n N = \phi(M).$$

This implies that $\phi : M \to N$ is surjective as required.

Difference Between Ring Homomorphisms and Module Homomorphisms

Problem 422

Let R be a ring with 1 and consider R as a module over itself.
(a) Determine whether every module homomorphism $\phi : R \to R$ is a ring homomorphism.
(b) Determine whether every ring homomorphism $\phi : R \to R$ is a module homomorphism.
(c) If $\phi : R \to R$ is both a module homomorphism and a ring homomorphism, what can we say about ϕ?

Solution.

(a) Determine whether every module homomorphism $\phi : R \to R$ is a ring homomorphism.

Consider the ring of integers $R = \mathbb{Z}$. Then the map

$$\phi : \mathbb{Z} \to \mathbb{Z}$$

defined by

$$\phi(x) = 2x$$

is a $\mathbb{Z}$-module homomorphism.
In fact, we have for $x, y, r \in R$

$$\phi(x+y) = 2(x+y) = 2x + 2y = \phi(x) + \phi(y)$$

and

$$\phi(rx) = 2(rx) = r(2x) = r\phi(x).$$

However, the map ϕ is not a ring homomorphism since $\phi(1) = 2 \neq 1$.

(Every ring homomorphism sends 1 to itself.)

Thus, we conclude that not every module homomorphism $\phi : R \to R$ is a ring homomorphism.

(b) Determine whether every ring homomorphism $\phi : R \to R$ is a module homomorphism.

Let us consider the polynomial ring $R = \mathbb{Z}[x]$.

Consider the map

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$$

defined by

$$\phi\left(f(x) \right) = f(x^2)$$

for $f(x) \in \mathbb{Z}[x]$.

Then ϕ is a ring homomorphism because we have

$$\begin{aligned}
&\phi\left(f(x) + g(x) \right) = f(x^2) + g(x^2) = \phi\left(f(x) \right) + \phi\left(g(x) \right), \text{ and} \\
&\phi\left(f(x)g(x) \right) = f(x^2)g(x^2) = \phi\left(f(x) \right)\phi\left(g(x) \right).
\end{aligned}$$

However, the map ϕ is not a $\mathbb{Z}[x]$-module homomorphism. If it were a $\mathbb{Z}[x]$-module, then we would have

$$\begin{aligned}
x^2 &= \phi(x) \\
&= x\phi(1) && \text{since } \phi \text{ is a } \mathbb{Z}[x]\text{-module homomorphism} \\
&= x \cdot 1 && \text{since } \phi \text{ is a ring homomorphism} \\
&= x,
\end{aligned}$$

and thus we have $x = x^2$, which is a contradiction.

Thus, the conclusion is that not every ring homomorphism $\phi : R \to R$ is a module homomorphism.

(c) If $\phi : R \to R$ is both a module homomorphism and a ring homomorphism, what can we say about ϕ?

Suppose that $\phi : R \to R$ is both a ring homomorphism and an R-module homomorphism.

Then for any $x \in R$, we have

$$\begin{aligned}
\phi(x) &= x\phi(1) && \text{since } \phi \text{ is an } R\text{-module homomorphism} \\
&= x \cdot 1 && \text{since } \phi \text{ is a ring homomorphism} \\
&= x,
\end{aligned}$$

and it follows that ϕ must be the identity map.

Can $\mathbb{Z}$-Module Structure of Abelian Group Extend to $\mathbb{Q}$-Module Structure?

Problem 418

If M is a finite abelian group, then M is naturally a $\mathbb{Z}$-module.
Can this action be extended to make M into a $\mathbb{Q}$-module?

Proof.

In general, we cannot extend a $\mathbb{Z}$-module into a $\mathbb{Q}$-module.

We give a counterexample. Let $M = \mathbb{Z}/2\mathbb{Z}$ be the order 2 cyclic abelian group.

Hence it is a naturally $\mathbb{Z}$-module. We prove that this action cannot be extended to a $\mathbb{Q}$-action.

Let us assume the contrary.

Then for any $x \in M$, let

$$M \ni y := \frac{1}{2} \cdot x.$$

Then we have

$$x = 1 \cdot x = 2 \cdot \frac{1}{2} \cdot x = 2y = 0$$

in $M = \mathbb{Z}/2\mathbb{Z}$.

This is a contradiction since M contains a non-zero element.

Therefore, the $\mathbb{Z}$-action cannot be extended to a $\mathbb{Q}$-action.

Submodule Consists of Elements Annihilated by Some Power of an Ideal

Problem 417

Let R be a ring with 1 and let M be an R-module. Let I be an ideal of R.
Let M' be the subset of elements a of M that are annihilated by some power I^k of the ideal I, where the power k may depend on a.
Prove that M' is a submodule of M.

Proof.

Let us define the subset of M by

$$N_i =: \{a \in M \mid sa = 0 \text{ for all } s \in I^i\}.$$

That is, N_i consists of elements of M that are annihilated by the power I^i.

We claim that:

1. the subset N_i is a submodule of M for each integer i, and
2. we have the ascending chain

$$N_1 \subset N_2 \subset \cdots,$$

and

3. $M' = \cup_{i=1}^{\infty} N_i$.

Once we prove these claims, the result follows from the previous problem.

Let us prove claim 1. Let $a, b \in N_i$ and let $r \in R$.
For any $s \in I^i$ we have

$$s(a+b) = sa + sb = 0$$

because a, b are annihilated by $s \in I^i$.
Also, we have

$$s(ra) = (sr)a = 0$$

since $sr \in I$ as I is an ideal.
Thus, N_i is a submodule of M.

To prove claim 2, we note the inclusion

$$I^{i+1} = I^i \cdot I \subset I^i.$$

Thus each $a \in N_i$ is annihilated by elements in I^{i+1}.
Hence $N_i \subset N_{i+1}$ for any i, and this proves claim 2.

The claim 3 follows from the definition of the subset M'.

Since the union of submodules in an ascending chain of submodules is a submodule, we conclude that M' is a submodule of M.
(For a proof of this fact, see the post "Ascending chain of submodules and union of its submodules".)

Ascending Chain of Submodules and Union of its Submodules

Problem 416

Let R be a ring with 1. Let M be an R-module. Consider an ascending chain

$$N_1 \subset N_2 \subset \cdots$$

of submodules of M.
Prove that the union

$$\cup_{i=1}^{\infty} N_i$$

is a submodule of M.

Proof.

To simplify the notation, let us put

$$U = \cup_{i=1}^{\infty} N_i.$$

Prove that U is a submodule of M, it suffices to show the following two conditions:

1. For any $x, y \in U$, we have $x + y \in U$, and

2. For any $x \in U$ and $r \in R$, we have $rx \in U$.

To check condition 1, let $x, y \in U$.
Since x lies in the union $U = \cup_{i=1}^{\infty} N_i$, there is an integer n such that

$$x \in N_n.$$

Similarly, we have

$$y \in N_m$$

for some integer m.
Since $N_n \subset N_{\max(n,m)}$ and $N_m \subset N_{\max(n,m)}$, we have

$$x, y \in N_{\max(n,m)}.$$

As $N_{\max(n,m)}$ is a submodule of M, it is closed under addition.
It follows that

$$x + y \in N_{\max(n,m)} \subset U.$$

Hence condition 1 is met.

Next, we consider condition 2.

Let $x \in U$ and $r \in R$.

Since x is in the union U, there exists an integer n such that $x \in N_n$.

Since N_n is a submodule of M, it is closed under scalar multiplication.

Thus we have

$$rx \in N_n \subset U.$$

Therefore, condition 2 is satisfied, and so U is a submodule of M.

Linearly Dependent Module Elements / Module Homomorphism and Linearly Independency

Problem 415

(a) Let R be a commutative ring. If we regard R as a left R-module, then prove that any two distinct elements of the module R are linearly dependent.
(b) Let $f : M \to M'$ be a left R-module homomorphism. Let $\{x_1, \dots, x_n\}$ be a subset in M. Prove that if the set $\{f(x_1), \dots, f(x_n)\}$ is linearly independent, then the set $\{x_1, \dots, x_n\}$ is also linearly independent.

Definition.

Let R be a ring and M be a left R-module.
A finite subset $\{v_1, \dots, v_n\}$ of M is said to be **linearly independent** if whenever

$$r_1 v_1 + \cdots r_n v_n = 0$$

holds, then we have

$$r_1 = \cdots = r_n = 0.$$

Proof (a) any two distinct elements of the module R are linearly dependent.

Let x, y be distinct elements of the module R.

As R is a commutative ring, we have

$$(-y) \cdot x + x \cdot y = 0$$

This equality should be read as a linear combination of elements x and y in the module R with coefficients $-y$ and x in R.

Since x and y are distinct, at least one of them is non-zero.

Hence this equality yields that x, y are linearly dependent.

Proof (b) the set $\{x_1, \dots, x_n\}$ is linearly independent.

Suppose that we have a linear combination

$$r_1 x_1 + \cdots r_n x_n = 0$$

for $r_1, \dots, r_n \in R$.

Then we have

$$\begin{aligned} 0 &= f(0) \\ &= f(r_1 x_1 + \cdots r_n x_n) \\ &= r_1 f(x_1) + \cdots r_n f(x_n). \end{aligned}$$

since f is a R-module homomorphism.

It follows from the linearly independence of elements $f(x_1), \dots, f(x_n)$ that we obtain

$$r_1 = \cdots r_n = 0.$$

Hence the elements $x_1, \dots, x_n$ are linearly independent.

Short Exact Sequence and Finitely Generated Modules

Problem 414

Let R be a ring with 1. Let

$$0 \to M \xrightarrow{f} M' \xrightarrow{g} M'' \to 0 \tag{*}$$

be an exact sequence of left R-modules.

Prove that if M and M'' are finitely generated, then M' is also finitely generated.

Proof.

Since M is finitely generated, let $x_1, \dots, x_n$ be generators of M.

Similarly, let $z_1, \dots, z_m$ be generators of M''.

The exactness of the sequence (*) yields that the homomorphism $g : M' \to M''$ is surjective.

Thus, there exist $y_1, \dots, y_m \in M'$ such that

$$g(y_i) = z_i$$

for $i = 1, \dots, m$.

We claim that the elements

$$f(x_1), \ldots, f(x_n), y_1, \ldots, y_m$$

generate the module M.

Let w be an arbitrary element of M'. Then $g(w) \in M''$ and we can write

$$g(w) = \sum_{i=1}^{m} r_i z_i$$

for some $r_i \in R$ as z_i generate M''.

Then we have

$$\begin{aligned} g(w) &= \sum_{i=1}^{m} r_i z_i \\ &= \sum_{i=1}^{m} r_i g(y_i) \\ &= g\left(\sum_{i=1}^{m} r_i y_i \right) \end{aligned}$$

since g is a module homomorphism.

It follows that we have

$$g\left(w - \sum_{i=1}^{m} r_i y_i \right) = g(w) - g\left(\sum_{i=1}^{m} r_i y_i \right) = 0,$$

and thus

$$w - \sum_{i=1}^{m} r_i y_i \in \ker(g).$$

Since the sequence (*) is exact, we have $\ker(g) = \operatorname{im}(f)$.

Hence there exists $x \in M$ such that

$$f(x) = w - \sum_{i=1}^{m} r_i y_i.$$

Since x_i generate M, we can write

$$x = \sum_{i=1}^{n} s_i x_i$$

for some $s_i \in R$.

Thus, we have

$$\begin{aligned} w &= f(x) + \sum_{i=1}^{m} r_i y_i \\ &= f\left(\sum_{i=1}^{n} s_i x_i \right) + \sum_{i=1}^{m} r_i y_i \\ &= \sum_{i=1}^{n} s_i f(x_i) + \sum_{i=1}^{m} r_i y_i. \end{aligned}$$

This proves that any element $w \in M'$ can be written as a linear combination of

$$f(x_1), \dots, f(x_n), y_1, \dots, y_m,$$

and we conclude that M' is generated by these elements and thus finitely generated.

Annihilator of a Submodule is a 2-Sided Ideal of a Ring

Problem 410

Let R be a ring with 1 and let M be a left R-module.
Let S be a subset of M. The **annihilator** of S in R is the subset of the ring R defined to be

$$\mathrm{Ann}_R(S) = \{r \in R \mid rx = 0 \text{ for all } x \in S\}.$$

(If $rx = 0, r \in R, x \in S$, then we say r **annihilates** x.)
Suppose that N is a submodule of M. Then prove that the annihilator

$$\mathrm{Ann}_R(N) = \{r \in R \mid rn = 0 \text{ for all } n \in N\}$$

of M in R is a 2-sided ideal of R.

Proof.

To prove $\mathrm{Ann}_R(N)$ is a 2-sided ideal of R, it suffices to prove the following conditions:

1. For any $r, s \in \mathrm{Ann}_R(N)$, we have $r + s \in \mathrm{Ann}_R(N)$.
2. For any $r \in R$ and $s \in \mathrm{Ann}_R(N)$, we have $rs \in \mathrm{Ann}_R(N)$.
3. For any $r \in R$ and $s \in \mathrm{Ann}_R(N)$, we have $sr \in \mathrm{Ann}_R(N)$.

Let $r, s \in \mathrm{Ann}_R(N)$. Then for any $n \in N$, we have

$$rn = 0 \text{ and } sn = 0.$$

It follows from these identities that

$$(r + s)n = rn + sn = 0 + 0 = 0$$

for any $n \in N$.
Hence $r + s \in \mathrm{Ann}_R(N)$, and condition 1 is met.

To prove condition 2, let $r \in R$ and $s \in \mathrm{Ann}_R(N)$.
For any $n \in N$, we have

$$\begin{aligned}(rs)n &= r(sn)\\ &= r(0) && (\text{since } s \in \mathrm{Ann}_R(N))\\ &= 0.\end{aligned}$$

Thus, the element rs annihilates all elements n in N.

So $rs \in \mathrm{Ann}_R(N)$ and condition 2 is satisfied.

(At this point, we have proved that $\mathrm{Ann}_R(N)$ is a left ideal of R.)

To check condition 3, let $r \in R$ and $s \in \mathrm{Ann}_R(N)$.

We need to prove that $(sr)n = 0$ for any $n \in N$.

Since N is a submodule of M, the element rn is in N.

Since $s \in \mathrm{Ann}_R(N)$, we have $s(rn) = 0$.

It follows from the associativity that

$$(sr)n = s(rn) = 0$$

for any $n \in N$.

Hence $sr \in \mathrm{Ann}_R(N)$ and condition 3 is proved.

Therefore, $\mathrm{Ann}_R(N)$ is a 2-sided ideal of R.

This completes the proof.

Remark.

Note that the proof of condition 1 and 2 shows that $\mathrm{Ann}_R(S)$ is a left ideal of R for any subset S of M.

We needed the assumption that N is a submodule of M when we proved condition 3.

Torsion Submodule, Integral Domain, and Zero Divisors

Problem 409

Let R be a ring with 1. An element of the R-module M is called a **torsion element** if $rm = 0$ for some nonzero element $r \in R$.

The set of torsion elements is denoted

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero} r \in R\}.$$

(a) Prove that if R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M.

(Remark: an integral domain is a commutative ring by definition.) In this case the submodule $\mathrm{Tor}(M)$ is called **torsion submodule** of M.

(b) Find an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule.

(c) If R has nonzero zero divisors, then show that every nonzero R-module has nonzero torsion element.

Proof.

(a) Prove that if R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M.

To prove $\mathrm{Tor}(M)$ is a submodule of M, we check the following submodule criteria:

1. $\mathrm{Tor}(M)$ is not empty.
2. For any $m, n \in \mathrm{Tor}(M)$ and $t \in R$, we have $m + tn \in M$.

It is clear that the zero element 0 in M is in $\mathrm{Tor}(M)$, hence condition 1 is met.

To prove condition 2, let $m, n \in \mathrm{Tor}(M)$ and $t \in R$.

Since m, n are torsion elements, there exist nonzero elements $r, s \in R$ such that $rm = 0, sn = 0$.

Since R is an integral domain, the product rs of nonzero elements is nonzero.

We have

$$\begin{aligned} rs(m+tn) &= rsm + rstn \\ &= s(rm) + rt(sn) \qquad (R \text{ is commutative}) \\ &= s0 + rt0 = 0. \end{aligned}$$

This yields that $m + tn$ is a torsion elements, hence $m + tn \in \mathrm{Tor}(M)$.

This condition 2 is met as well, and we conclude that $\mathrm{Tor}(M)$ is a submodule of M.

(b) Find an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule.

Let us consider $R = \mathbb{Z}/6\mathbb{Z}$ and let M be the R-module R.

We just simply write n for the element $n + 6\mathbb{Z}$ in $R = \mathbb{Z}/6\mathbb{Z}$.

Then we have

$$3 \cdot 2 = 0 \text{ and } 2 \cdot 3 = 0.$$

This implies that 2 and 3 are torsion elements of the module M.

However, the sum $5 = 2 + 3$ is not a torsion element in M since if $r \cdot 5 = 0$ in $\mathbb{Z}/6\mathbb{Z}$, then $r = 0$.

Thus, $\mathrm{Tor}(M)$ is not closed under addition. Hence it is not a submodule of M.

(c) If R has nonzero zero divisors, then show that every nonzero R-module has nonzero torsion element.

Let r be nonzero zero divisors of R. That is, there exists a nonzero element $s \in R$ such that $rs = 0$. Let M be a nonzero R-module and let m be a nonzero element in M.

Put $n = sm$.

If $n = 0$, then this implies m is a nonzero torsion element of M, and we are done.

If $n \neq 0$, then we have

$$rn = r(sm) = (rs)m = 0m = 0.$$

This yields that n is a nonzero torsion element of M.

Hence, in either case, we obtain a nonzero torsion element of M. This completes the proof.

Basic Exercise Problems in Module Theory

Problem 408

Let R be a ring with 1 and M be a left R-module.

(a) Prove that $0_R m = 0_M$ for all $m \in M$.

Here 0_R is the zero element in the ring R and 0_M is the zero element in the module M, that is, the identity element of the additive group M.

To simplify the notations, we ignore the subscripts and simply write

$$0m = 0.$$

You must be able to and must judge which zero elements are used from the context.

(b) Prove that $r0 = 0$ for all $s \in R$. Here both zeros are 0_M.

(c) Prove that $(-1)m = -m$ for all $m \in M$.

(d) Assume that $rm = 0$ for some $r \in R$ and some nonzero element $m \in M$. Prove that r does not have a left inverse.

Definition of a module.

Let R be a ring with 1.

A set M is a left R-module if it has a binary operation $+$ on M under which M is an abelian group, and it has a map $R \times M \to M$ (called an action of R on M) denoted by rm, for all $r \in R$ and $m \in M$ satisfying the following axioms

1. $(r+s)m = rm + sm$
2. $(rs)m = r(sm)$
3. $r(m+n) = rm + rn$

for all $r, s \in R$ and $m, n \in M$.

If the ring R has a 1, we also impose the axiom:

4. $1m = m$

for all $m \in M$.

Proof.

(a) Prove that $0_R m = 0_M$ for all $m \in M$.

We have

$$\begin{aligned} 0m &= (0+0)m \\ &= 0m + 0m \qquad \text{by axiom 1.} \end{aligned}$$

Subtracting $0m$, we obtain $0m = 0$ as required.

(b) Prove that $r0 = 0$ for all $s \in R$.

We have

$$\begin{aligned} r0 &= r(0+0) \\ &= r0 + r0 \qquad \text{by axiom 3.} \end{aligned}$$

Subtracting $r0$ from both sides, we obtain

$$r0 = 0.$$

(c) Prove that $(-1)m = -m$ for all $m \in M$.

We compute

$$\begin{aligned} m + (-1)m &= 1m + (-1)m \qquad \text{by axiom 4} \\ &= (1 + (-1))m \qquad \text{by axiom 1} \\ &= 0m \\ &= 0 \qquad \text{by part (a).} \end{aligned}$$

This shows that $(-1)m$ is the additive inverse of m, which must be $-m$ by the uniqueness of the additive

inverse of an abelian group.

Hence we obtain $(-1)m = -m$.

Prove that r does not have a left inverse.

Seeking a contradiction, assume that r has a left inverse s. That is, we have $sr = 1$.

Multiplying $rm = 0$ by s on the left, we have

$$s(rm) = s0 = 0$$

by part (b).

The left hand side is

$$\begin{aligned} s(rm) &= (sr)m && \text{by axiom 2} \\ &= 1m \\ &= m && \text{by axiom 4.} \end{aligned}$$

It follows that $m = 0$ but by assumption m is a nonzero element of M.

Thus this is a contradiction, and we conclude that r does not have a left inverse.

Problems in Field Theory

Prove that $\mathbb{F}_3[x]/(x^2+1)$ is a Field and Find the Inverse Elements

Problem 529

Let $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ be the finite field of order 3.

Consider the ring $\mathbb{F}_3[x]$ of polynomial over $\mathbb{F}_3$ and its ideal $I = (x^2+1)$ generated by $x^2+1 \in \mathbb{F}_3[x]$.

(a) Prove that the quotient ring $\mathbb{F}_3[x]/(x^2+1)$ is a field. How many elements does the field have?

(b) Let $ax+b+I$ be a nonzero element of the field $\mathbb{F}_3[x]/(x^2+1)$, where $a, b \in \mathbb{F}_3$. Find the inverse of $ax+b+I$.

(c) Recall that the multiplicative group of nonzero elements of a field is a cyclic group.

Confirm that the element x is not a generator of $E^\times$, where $E = \mathbb{F}_3[x]/(x^2+1)$ but $x+1$ is a generator.

Proof.

(a) Prove that the quotient ring $\mathbb{F}_3[x]/(x^2+1)$ is a field

Let $f(x) = x^2 + 1$. We claim that the polynomial $f(x)$ is irreducible over $\mathbb{F}_3$.

To see this, note that $f(x)$ is a quadratic polynomial.

So $f(x)$ is irreducible over $\mathbb{F}_3$ if it does not have a root in $\mathbb{F}_3$.

We have

$$f(0) = 1, \quad f(1) = 2, \quad f(2) = 2^2 + 1 = 2 \text{ in } \mathbb{F}_3.$$

Hence $f(x)$ does not have a root in $\mathbb{F}_3$ and it is irreducible over $\mathbb{F}_3$.

It follows that the quotient $\mathbb{F}_3[x]/(x^2+1)$ is a field.

Since x^2+1 is quadratic, the extension degree of $\mathbb{F}_3[x]/(x^2+1)$ over $\mathbb{F}_3$ is 2.

Hence the number of elements in the field is $3^2 = 9$.

(b) Find the inverse of $ax+b+I$

Let $ax+b$ be a representative of a nonzero element of the field $\mathbb{F}_3[x]/(x^2+1)$.

Let $cx+d$ be its inverse. Then we have

$$\begin{aligned} 1 &= (ax+b)(cx+d) = acx^2 + (ad+bc)x + bd \\ &= (ad+bc)x + bd - ac \end{aligned}$$

since $x^2 = -1$ in $\mathbb{F}_3[x]/(x^2+1)$.

Hence we obtain two equations

$$ad+bc = 0 \text{ and } bd-ac = 1.$$

Since $ax+b$ is a nonzero element, at least one of a, b is not zero.

If $a \neq 0$, then the first equation gives

$$d = -\frac{bc}{a}. \qquad (*)$$

Substituting this to the second equation, we obtain

$$\left(\frac{-b^2-a^2}{a}\right)c = 1.$$

Observe that a^2+b^2 is not zero in $\mathbb{F}_3$.

(Since $a \neq 0$, we have $a^2 = 1$. Also $b^2 = 0, 1$.)

Hence we have

$$c = -\frac{a}{a^2+b^2}.$$

It follows from (*) that

$$d = \frac{b}{a^2+b^2}$$

Thus, if $a \neq 0$, then the inverse element is

$$(ax+b)^{-1} = \frac{1}{a^2+b^2}(-ax+b). \qquad (**)$$

If $a = 0$, then $b \neq 0$ and it is clear that the inverse element of $ax+b = b$ is $1/b$.

Note that the formula (**) is still true in this case.

In summary, we have

$$(ax+b)^{-1}=\frac{1}{a^2+b^2}(-ax+b)$$

for any nonzero element $ax+b$ in the field $\mathbb{F}_3[x]/(x^2+1)$.

(c) x is not a generator but $x+1$ is a generator

Note that the order of $E^\times$ is 8 since E is a finite field of order 9 by part (a).

We compute the powers of x and obtain

$$x,\quad x^2=-1,\quad x^3=-x,\quad x^4=-x^2=1.$$

Thus, the order of the element x is 4, hence x is not a generator of the cyclic group $E^\times$.

Next, let us check that $x+1$ is a generator.

We compute the powers of $x+1$ as follows.

$$\begin{aligned}&x+1,\quad (x+1)^2=x^2+2x+1=2x,\\ &(x+1)^3=2x(x+1)=2x^2+2x=2x-2=2x+1\\ &(x+1)^4=(2x+1)(x+1)=2x^2+3x+1=2.\end{aligned}$$

Observe that at this post the order of $x+1$ must be larger than 4.

Since the order of $E^\times$ is 8, the order of $x+1$ must be 8 by Lagrange's theorem.

Just for a reference we give the complete list of powers of $x+1$.

n	$(x+1)^n$
1	$x+1$
2	$2x$
3	$2x+1$
4	2
5	$2x+2$
6	x
7	$x+2$
8	1

Each Element in a Finite Field is the Sum of Two Squares

Problem 511

Let F be a finite field.

Prove that each element in the field F is the sum of two squares in F.

Proof.

Let x be an element in F. We want to show that there exists $a,b\in F$ such that

$$x = a^2 + b^2.$$

Since F is a finite field, the characteristic p of the field F is a prime number.

If $p = 2$, then the map $\phi : F \to F$ defined by $\phi(a) = a^2$ is a field homomorphism, hence it is an endomorphism since F is finite.(The map ϕ is called the Frobenius endomorphism).
Thus, for any element $x \in F$, there exists $a \in F$ such that $\phi(a) = x$.
Hence x can be written as the sum of two squares $x = a^2 + 0^2$.

Now consider the case $p > 2$.
We consider the map $\phi : F^\times \to F^\times$ defined by $\phi(a) = a^2$. The image of ϕ is the subset of F that can be written as a^2 for some $a \in F$.
If $\phi(a) = \phi(b)$, then we have

$$0 = a^2 - b^2 = (a - b)(a + b).$$

Hence we have $a = b$ or $a = -b$.
Since $b \neq 0$ and $p > 2$, we know that $b \neq -b$.
Thus the map ϕ is a two-to-one map.
Thus, there are $\frac{|F^\times|}{2} = \frac{|F|-1}{2}$ square elements in $F^\times$.
Since 0 is also a square in F, there are

$$\frac{|F| - 1}{2} + 1 = \frac{|F| + 1}{2}$$

square elements in the field F.
Put

$$A := \{a^2 \mid a \in F\}.$$

We just observed that $|A| = \frac{|F|+1}{2}$.
Fix an element $x \in F$ and consider the subset

$$B := \{x - b^2 \mid b \in F\}.$$

Clearly $|B| = |A| = \frac{|F|+1}{2}$.
Observe that both A and B are subsets in F and

$$|A| + |B| = |F| + 1 > |F|,$$

and hence A and B cannot be disjoint.
Therefore, there exists $a, b \in F$ such that $a^2 = x - b^2$, or equivalently,

$$x = a^2 + b^2.$$

Hence each element $x \in F$ is the sum of two squares.

Any Automorphism of the Field of Real Numbers Must be the Identity Map

Problem 507

Prove that any field automorphism of the field of real numbers $\mathbb{R}$ must be the identity automorphism.

Proof.

We prove the problem by proving the following sequence of claims.

Let $\phi : \mathbb{R} \to \mathbb{R}$ be an automorphism of the field of real numbers $\mathbb{R}$.

1. **Claim 1**. For any positive real number x, we have $\phi(x) > 0$.
2. **Claim 2**. For any $x, y \in \mathbb{R}$ such that $x > y$, we have $\phi(x) > \phi(y)$.
3. **Claim 3**. The automorphism ϕ is the identity on positive integers.
4. **Claim 4**. The automorphism ϕ is the identity on rational numbers.
5. **Claim 5**. The automorphism ϕ is the identity on real numbers.

Let us now start proving the claims.

Let $\phi : \mathbb{R} \to \mathbb{R}$ be an automorphism of the field of real numbers $\mathbb{R}$.

Claim 1. For any positive real number x, we have $\phi(x) > 0$.

Since x is a positive real number, we have $\sqrt{x} \in \mathbb{R}$ and

$$\phi(x) = \phi\left(\sqrt{x}^2\right) = \phi(\sqrt{x})^2 \geq 0.$$

Note that since $\phi(0) = 0$ and ϕ is bijective, $\phi(x) \neq 0$ for any $x \neq 0$.

Thus, it follows that $\phi(x) > 0$ for each positive real number x.

Claim 1 is proved.

Claim 2. For any $x, y \in \mathbb{R}$ such that $x > y$, we have $\phi(x) > \phi(y)$.

Since $x > y$, we have $x - y > 0$ and it follows from Claim 1 that

$$0 < \phi(x - y) = \phi(x) - \phi(y).$$

Hence, $\phi(x) > \phi(y)$.

Claim 3. The automorphism ϕ is the identity on positive integers.

Let n be a positive integer. Then we have

$$\phi(n) = \phi(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\phi(1) + \phi(1) + \cdots + \phi(1)}_{n \text{ times}} = n$$

since $\phi(1) = 1$.

Claim 4. The automorphism ϕ is the identity on rational numbers.

Any rational number q can be written as $q = \pm m/n$, where m, n are positive integers.

Then we have

$$\phi(q) = \phi\left(\pm\frac{m}{n}\right) = \pm\frac{\phi(m)}{\phi(n)} = \pm\frac{m}{n} = q,$$

where the third equality follows from Claim 3.

Claim 5. The automorphism ϕ is the identity on real numbers.

In this claim, we finish the proof of the problem.

Let x be any real number.

Seeking a contradiction, assume that $\phi(x) \neq x$.

There are two cases to consider:

$$x < \phi(x) \text{ or } x > \phi(x).$$

First, suppose that $x < \phi(x)$. Then there exists a rational number q such that

$$x < q < \phi(x).$$

Then we have

$$\begin{aligned} \phi(x) &< \phi(q) && \text{by Claim 2 since } x < q \\ &= q && \text{by Claim 4 since } q \text{ is rational} \\ &< \phi(x) && \text{by the choice of } q, \end{aligned}$$

and this is a contradiction. Next, consider the case when $x > \phi(x)$.

There exists a rational number q such that

$$\phi(x) < q < x.$$

Then by the same argument as above, we have

$$\phi(x) < q = \phi(q) < \phi(x),$$

which is a contradiction. Thus, in either case we reached a contradiction, and hence we must have $\phi(x) = x$ for all real numbers x. This proves that the automorphism $\phi : \mathbb{R} \to \mathbb{R}$ is the identity map.

Example of an Infinite Algebraic Extension

Problem 499

Find an example of an infinite algebraic extension over the field of rational numbers $\mathbb{Q}$ other than the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$.

Definition (Algebraic Element, Algebraic Extension).

Let F be a field and let E be an extension of F .

- The element $\alpha \in E$ is said to be **algebraic** over F is α is a root of some nonzero polynomial with coefficients in F .
- The extension E/F is said to be **algebraic** if every element of E is algebraic over F .

Proof.

Consider the field

$$K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{2}, \dots, \sqrt[2n+1]{2}, \dots).$$

That is, K is the field extension obtained by adjoining all numbers of the form $\sqrt[2n+1]{2}$ for any positive integers n.

Note that $\sqrt[2n+1]{2}$ is a root of the monic polynomial $x^{2n+1}-2$, hence $\sqrt[2n+1]{2}$ is algebraic over $\mathbb{Q}$.

By Eisenstein's criterion with prime 2, we know that the polynomial $x^{2n+1}-2$ is irreducible over $\mathbb{Q}$.

Thus the extension degree is $[\mathbb{Q}(\sqrt[2n+1]{2}):\mathbb{Q}]=2n+1$.

Since the field K contains the subfield $\mathbb{Q}(\sqrt[2n+1]{2})$, we have

$$2n+1=[\mathbb{Q}(\sqrt[2n+1]{2}):\mathbb{Q}]\leq[K:\mathbb{Q}]$$

for any positive integer n.

Therefore, the extension degree of K over $\mathbb{Q}$ is infinite.

Observe that any element α of K belongs to a subfield $\mathbb{Q}(\sqrt[3]{2},\sqrt[5]{2},\dots,\sqrt[2n+1]{2})$ for some $n\in\mathbb{Z}$.

Since each number $\sqrt[2k+1]{2}$ is algebraic over $\mathbb{Q}$, we know that this subfield is algebraic, hence α is algebraic.

Thus, the field K is algebraic over $\mathbb{Q}$.

Is K different from $\bar{\mathbb{Q}}$?

It remains to show that $K\neq\bar{\mathbb{Q}}$.

Consider $\sqrt{2}$.

Since $\sqrt{2}$ is a root of x^2-2, it is algebraic, hence $\sqrt{2}\in\bar{\mathbb{Q}}$.

We claim that $\sqrt{2}\notin K$.

Assume on the contrary that $\sqrt{2}\in K$.

Then $\sqrt{2}\in F:=\mathbb{Q}(\sqrt[3]{2},\sqrt[5]{2},\dots,\sqrt[2n+1]{2})\subset K$ for some $n\in\mathbb{Z}$.

Note that the extension degree of this subfield F is odd since each extension degree of $\mathbb{Q}(\sqrt[2k+1]{2})/\mathbb{Q}$ is odd.

Since $\sqrt{2}\in F$, we must have

$$[F:\mathbb{Q}]=[F:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2[F:\mathbb{Q}(\sqrt{2})],$$

which is even.

This is a contradiction, and hence $\sqrt{2}\notin K$.

Thus, $K\neq\bar{\mathbb{Q}}$.

Comment.

With the same argument, we can prove that the field

$$K=\mathbb{Q}(\sqrt[2]{2},\sqrt[3]{2},\dots,\sqrt[n]{2},\dots)$$

is infinite algebraic extension over $\mathbb{Q}$.

However, it is not trivial to show that this field is different from $\bar{\mathbb{Q}}$.

That's why we used only $\sqrt[2k+1]{2}$ in K.

We can also use $\sqrt[p]{2}$ for odd prime p.

The Cyclotomic Field of 8-th Roots of Unity is $\mathbb{Q}(\zeta_8)=\mathbb{Q}(i,\sqrt{2})$

Problem 491

Let ζ_8 be a primitive 8-th root of unity.

Prove that the cyclotomic field $\mathbb{Q}(\zeta_8)$ of the 8-th root of unity is the field $\mathbb{Q}(i,\sqrt{2})$.

Proof.

Recall that the extension degree of the cyclotomic field of n-th roots of unity is given by $\phi(n)$, the Euler totient function.

Thus we have

$$[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \phi(8) = 4.$$

Without loss of generality, we may assume that

$$\zeta_8 = e^{2\pi i/8} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i.$$

Then $i = \zeta_8^2 \in \mathbb{Q}(\zeta_8)$ and $\zeta_8 + \zeta_8^7 = \sqrt{2} \in \mathbb{Q}(\zeta_8)$.

Thus, we have

$$\mathbb{Q}(i, \sqrt{2}) \subset \mathbb{Q}(\zeta_8).$$

It suffices now to prove that $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$.

Note that we have $[\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, we know that $i \notin \mathbb{Q}(\sqrt{2})$.

Thus, we have

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

It follows that

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2}).$$

A Rational Root of a Monic Polynomial with Integer Coefficients is an Integer

Problem 489

Suppose that α is a rational root of a monic polynomial $f(x)$ in $\mathbb{Z}[x]$.

Prove that α is an integer.

Proof.

Suppose that $\alpha = \frac{p}{q}$ is a rational number in lowest terms, that is, p and q are relatively prime integers.

Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be a monic polynomial in $\mathbb{Z}[x]$ and α is a root of $f(x)$.

Since α is a root of $f(x)$, we have

$$\begin{aligned} 0 &= f(\alpha) \\ &= \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \\ &= \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1\frac{p}{q} + a_0. \end{aligned}$$

Multiplying by q^n, we obtain

$$\begin{aligned} 0 &= q^n f(\alpha) \\ &= p^n + a_{n-1}qp^{n-1} + \cdots + a_1 q^{n-1}p + a_0 q^n \\ &= p^n + q\left(a_{n-1}p^{n-1} + \cdots + a_1 q^{n-2}p + a_0 q^{n-1}\right). \end{aligned}$$

Hence we have

$$q\left(a_{n-1}p^{n-1}+\cdots+a_1q^{n-2}p+a_0q^{n-1}\right)=-p^n,$$

and this implies that q divides p^n, and so q divides p.

Since p and q are relatively primes, it yields that $q=1$.

Therefore, $\alpha=p/1=p$ is an integer.

Cubic Polynomial x^3-2 is Irreducible Over the Field $\mathbb{Q}(i)$

Problem 399

Prove that the cubic polynomial x^3-2 is irreducible over the field $\mathbb{Q}(i)$.

Proof.

Note that the polynomial x^3-2 is irreducible over $\mathbb{Q}$ by Eisenstein's criterion (with prime $p=2$).

This implies that if α is any root of x^3-2, then the degree of the field extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 3:

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=3. \tag{*}$$

Seeking a contradiction, assume that x^3-2 is reducible over $\mathbb{Q}(i)$.

Then x^3-2 has a root in $\mathbb{Q}(i)$ as it is a reducible degree 3 polynomial. So let us call the root $\alpha\in\mathbb{Q}(i)$.

Then $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{Q}(i)$ and thus we have

$$2=[\mathbb{Q}(i):\mathbb{Q}]=[\mathbb{Q}(i):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]\geq 3$$

by (*). Hence we have reached a contradiction.

As a result, x^3-2 is irreducible over $\mathbb{Q}(i)$.

Prove that any Algebraic Closed Field is Infinite

Problem 398

Prove that any algebraic closed field is infinite.

Definition.

A field F is said to be **algebraically closed** if each non-constant polynomial in $F[x]$ has a root in F.

Proof.

Let F be a finite field and consider the polynomial

$$f(x)=1+\prod_{a\in F}(x-a).$$

The coefficients of $f(x)$ lie in the field F, and thus $f(x)\in F[x]$. Of course, $f(x)$ is a non-constant polynomial.

Note that for each $a\in F$, we have

$$f(a)=1\neq 0.$$

So the polynomial $f(x)$ has no root in F.

Hence the finite field F is not algebraic closed.

It follows that every algebraically closed field must be infinite.

Extension Degree of Maximal Real Subfield of Cyclotomic Field

Problem 362

Let n be an integer greater than 2 and let $\zeta = e^{2\pi i/n}$ be a primitive n-th root of unity. Determine the degree of the extension of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta + \zeta^{-1})$.
The subfield $\mathbb{Q}(\zeta + \zeta^{-1})$ is called **maximal real subfield**.

Proof.

Note that since $n > 2$, the primitive n-th root ζ is not a real number.

Also, we have

$$\zeta + \zeta^{-1} = 2\cos(2\pi/n),$$

which is a real number.

Thus the field $\mathbb{Q}(\zeta + \zeta^{-1})$ is real.

Therefore the degree of the extension satisfies

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \geq 2.$$

We actually prove that the degree is 2.

To see this, consider the polynomial

$$f(x) = x^2 - (\zeta + \zeta^{-1})x + 1$$

in $\mathbb{Q}(\zeta + \zeta^{-1})[x]$.

The polynomial factos as

$$f(x) = x^2 - (\zeta + \zeta^{-1})x + 1 = (x - \zeta)(x - \zeta^{-1}).$$

Hence ζ is a root of this polynomial.

It follows from $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \geq 2$ that $f(x)$ is the minimal polynomial of ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$, and hence the extension degree is

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2.$$

Comment.

The subfield $\mathbb{Q}(\zeta + \zeta^{-1})$ is called **the maximal real subfield**.

The reason why it is called as such should be clear from the proof.

Equation $x_1^2 + \cdots + x_k^2 = -1$ Doesn't Have a Solution in Number Field $\mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3})$

Problem 358

Let $\alpha = \sqrt[3]{2}e^{2\pi i/3}$. Prove that $x_1^2 + \cdots + x_k^2 = -1$ has no solutions with all $x_i \in \mathbb{Q}(\alpha)$ and $k \geq 1$.

Proof.

Note that $\alpha = \sqrt[3]{2}e^{2\pi i/3}$ is a root of the polynomial $x^3 - 2$.

The polynomial $x^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with prime $p = 2$.

The roots of this polynomial are

$$\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3}.$$

Then it follows that we have an isomorphism

$$\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3})\cong\mathbb{Q}[x]/(x^3-2)\cong\mathbb{Q}(\sqrt[3]{2}).$$

Let us denote this isomorphism by $\phi:\mathbb{Q}(\alpha)\to\mathbb{Q}(\sqrt[3]{2})$, which sends α to $\sqrt[3]{2}$ and fixed $\mathbb{Q}$ elementwise.

Seeking a contradiction, we assume that there exist $x_1,\dots,x_k\in\mathbb{Q}(\alpha)$ such that

$$x_1^2+\cdots+x_k^2=-1.$$

Then we apply the isomorphism ϕ and obtain

$$\begin{aligned}-1&=\phi(-1)=\phi(x_1^2+\cdots+x_k^2)\\&=\phi(x_1)^2+\cdots+\phi(x_k)^2.\end{aligned}$$

However, this equality does not hold since $\phi(x_i)\in\mathbb{Q}(\sqrt[3]{2})$ and the field $\mathbb{Q}(\sqrt[3]{2})$ consists of real numbers.
Thus, we have reached a contradiction, hence there is no solution of $x_1^2+\cdots+x_k^2=-1$ in the field $\mathbb{Q}(\alpha)$.

Application of Field Extension to Linear Combination

Problem 335

Consider the cubic polynomial $f(x)=x^3-x+1$ in $\mathbb{Q}[x]$.
Let α be any real root of $f(x)$.
Then prove that $\sqrt{2}$ can not be written as a linear combination of $1,\alpha,\alpha^2$ with coefficients in $\mathbb{Q}$.

Proof.

We first prove that the polynomial $f(x)=x^3-x+1$ is irreducible over $\mathbb{Q}$.
Since $f(x)$ is a monic cubic polynomial, the only possible roots are the divisors of the constant term 1. As we have $f(1)=f(-1)=1\neq 0$, the polynomial has no rational roots. Hence $f(x)$ is irreducible over $\mathbb{Q}$.
Then $f(x)$ is the minimal polynomial of α over $\mathbb{Q}$, and hence the field extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ has degree 3.
If $\sqrt{2}$ is a linear combination of $1,\alpha,\alpha^2$, then it follows that $\sqrt{2}\in\mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{Q}(\alpha)$.
Then the degree of the field extension is

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

Since $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, this is impossible.
Thus, $\sqrt{2}$ is not a linear combination of $1,\alpha,\alpha^2$.

Irreducible Polynomial x^3+9x+6 and Inverse Element in Field Extension

Problem 334

Prove that the polynomial

$$f(x)=x^3+9x+6$$

is irreducible over the field of rational numbers $\mathbb{Q}$.
Let θ be a root of $f(x)$.
Then find the inverse of $1+\theta$ in the field $\mathbb{Q}(\theta)$.

Proof.

Note that $f(x)$ is a monic polynomial and the prime number 3 divides all non-leading coefficients of $f(x)$. Also the constant term 6 of $f(x)$ is not divisible by 3^2. Hence by Eisenstein's criterion, the polynomial $f(x)$ is irreducible over $\mathbb{Q}$.

We divide the polynomial $f(x)$ by $x+1$ and obtain

$$x^3+9x+6=(x+1)(x^2-x+10)-4$$

by long division.

Then it follows that in the field $\mathbb{Q}(\theta)\cong \mathbb{Q}[x]/(f(x))$ (note that $f(x)$ is the minimal polynomial of θ), we have

$$0=(\theta+1)(\theta^2-\theta+10)-4,$$

and hence this yields that we have the inverse

$$(1+\theta)^{-1}=\frac{1}{4}(\theta^2-\theta+10).$$

Explicit Field Isomorphism of Finite Fields

Problem 233

(a) Let $f_1(x)$ and $f_2(x)$ be irreducible polynomials over a finite field $\mathbb{F}_p$, where p is a prime number. Suppose that $f_1(x)$ and $f_2(x)$ have the same degrees. Then show that fields $\mathbb{F}_p[x]/(f_1(x))$ and $\mathbb{F}_p[x]/(f_2(x))$ are isomorphic.

(b) Show that the polynomials x^3-x+1 and x^3-x-1 are both irreducible polynomials over the finite field $\mathbb{F}_3$.

(c) Exhibit an explicit isomorphism between the splitting fields of x^3-x+1 and x^3-x-1 over $\mathbb{F}_3$.

Proof.

(a) Fields $\mathbb{F}_p[x]/(f_1(x))$ and $\mathbb{F}_p[x]/(f_2(x))$ are isomorphic

Let n be the degree of f_1 and f_2.

Since f_1 is irreducible over $\mathbb{F}_p$, the quotient field $\mathbb{F}_p[x]/(f_1(x))$ is the finite field of p^n elements.

Similarly, so is $\mathbb{F}_p[x]/(f_2(x))$.

Since a finite field of p^n elements are unique up to isomorphism, these two quotient fields are isomorphic.

Here, we give an explicit isomorphism. The polynomial $f_1(x)$ splits completely in the field $F_{p^n}\cong \mathbb{F}_p[x]/(f_2(x))$, so let θ be a root of $f_1(x)$ in $\mathbb{F}_p[x]/(f_2(x))$. (Note that θ is a polynomial.)

Define a map

$$\Phi : \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_2(x))$$

sending $g(x)\in \mathbb{F}_p[x]$ to $g(\theta)$. The map Φ is a ring homomorphism.

We want to show that the kernel $\ker(\Phi)=(f_1(x))$.

Since $\Phi(f_1(x))=f_1(\theta)=0$, we have $(f_1(x))\subset \ker(\Phi)$.

On the other hand, if $g(x)\in \ker(\Phi)$, then we have $g(\theta)=0$.

Since $f_1(x)$ is the minimal polynomial of θ, it follows that f_1 divides $g(x)$, and hence $g(x)\in (f_1(x))$.

Therefore we proved $\ker(\Phi)=(f_1(x))$.

By the first isomorphism theorem, we obtain an isomorphism

$$\tilde{\Phi} : \mathbb{F}_p[x]/(f_1(x)) \xrightarrow{\cong} \mathbb{F}_p[x]/(f_2(x)),$$

where $\tilde{\Phi}$ maps x to θ.

(b) The polynomials $x^3 - x + 1$ and $x^3 - x - 1$ are irreducible over $\mathbb{F}_3$

Since these polynomial are of degree 3, if they are reducible, then it has a root in $\mathbb{F}_3$. Evaluating these polynomials at $x = 0, 1, 2$ shows that they have no roots in $\mathbb{F}_3$. Thus these two polynomial are irreducible over $\mathbb{F}_3$.

(c) Explicit isomorphism between the splitting fields of $x^3 - x + 1$ and $x^3 - x - 1$ over $\mathbb{F}_3$

By part (a), the splitting fields

$$\mathbb{F}_3[x]/(x^3 - x + 1) \text{ and } \mathbb{F}_3[x]/(x^3 - x - 1)$$

are isomorphic. In the proof of part (a), we gave an explicit isomorphism.
That is, if θ is a root of $x^3 - x + 1$ in the field $\mathbb{F}_3[x]/(x^3 - x - 1)$, then the map sending
$x \in \mathbb{F}_3[x]/(x^3 - x + 1)$ to $\theta \in \mathbb{F}_3[x]/(x^3 - x - 1)$ gives an isomorphism.
So we want to find a root θ of $f_1(x) := x^3 - x + 1$.
Let $\theta = a + bx + cx^2 \in \mathbb{F}_3[x]/(x^3 - x - 1)$.

Then we have

$$\begin{aligned}
f_1(\theta) &= f_1(a + bx + cx^2) \\
&= (a + bx + cx^2)^3 - (a + bx + cx^2) + 1 \\
&= a + bx^3 + cx^6 - (a + bx + cx^2) + 1 \\
&\text{(Note that } a^3 = a \text{ in } \mathbb{F}_3 \text{ and similarly for } b \text{ and } c.) \\
&= a + b(x + 1) + c(x^2 + 2x + 1) - (a + bx + cx^2) + 1 \\
&\text{(Note that } x^3 = x + 1 \text{ in } \mathbb{F}_3[x]/(x^3 - x - 1), \text{ and thus } x^6 = x^2 + 2x + 1.) \\
&= 2cx + b + c + 1 \overset{\text{set}}{=} 0.
\end{aligned}$$

From this we deduce that $c = 0, b = 2$ gives a root θ.
For example, choosing $a = 0$, we have a root $\theta = 2x$ of $f_1(x)$.
Therefore the explicit isomorphism is

$$\Phi : \mathbb{F}_3[x]/(x^3 - x + 1) \xrightarrow{\cong} \mathbb{F}_3[x]/(x^3 - x - 1),$$

which sends x to $\theta = 2x$.

Galois Extension $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ of Degree 4 with Cyclic Group

Problem 231

Show that $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is a cyclic quartic field, that is, it is a Galois extension of degree 4 with cyclic Galois group.

Proof.

Put $\alpha = \sqrt{2 + \sqrt{2}}$. Then we have $\alpha^2 = 2 + \sqrt{2}$. Taking square of $\alpha^2 - 2 = \sqrt{2}$, we obtain
$\alpha^4 - 4\alpha^2 + 4 = 2$. Hence α is a root of the polynomial

$$f(x) = x^4 - 4x + 2.$$

By the Eisenstein's criteria, $f(x)$ is an irreducible polynomial over $\mathbb{Q}$.
There are four roots of $f(x)$:

$$\pm\sqrt{2 \pm \sqrt{2}}.$$

Note that we have a relation

$$(\sqrt{2+\sqrt{2}})(\sqrt{2-\sqrt{2}}) = \sqrt{2}.$$

Thus we have

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in \mathbb{Q}(\sqrt{2+\sqrt{2}}).$$

Hence all the roots of $f(x)$ are in the field $\mathbb{Q}(\sqrt{2+\sqrt{2}})$, hence $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is the splitting field of the separable polynomial $f(x) = x^4 - 4x + 2$.
Thus the field $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois over $\mathbb{Q}$ of degree 4.
Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})$ be the automorphism sending

$$\sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}.$$

Then we have

$$\begin{aligned} 2 + \sigma(\sqrt{2}) &= \sigma(2+\sqrt{2}) \\ &= \sigma\left((\sqrt{2+\sqrt{2}})^2\right) \\ &= \sigma\left(\sqrt{2+\sqrt{2}}\right)^2 \\ &= \left(\sqrt{2-\sqrt{2}}\right)^2 = 2 - \sqrt{2}. \end{aligned}$$

Thus we obtain $\sigma(\sqrt{2}) = -\sqrt{2}$.
Using this, we have

$$\begin{aligned} \sigma^2(\sqrt{2+\sqrt{2}}) &= \sigma(\sqrt{2-\sqrt{2}}) \\ &= \sigma\left(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\right) \\ &= \frac{\sigma(\sqrt{2})}{\sigma(\sqrt{2+\sqrt{2}})} \\ &= \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} \\ &= -\sqrt{2-\sqrt{2}}. \end{aligned}$$

Therefore σ^2 is not the identity automorphism. This implies the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})$ is generated by σ, that is, the Galois group is a cyclic group of order 4.

Galois Group of the Polynomial $x^2 - 2$

Problem 230

Let $\mathbb{Q}$ be the field of rational numbers.
(a) Is the polynomial $f(x) = x^2 - 2$ separable over $\mathbb{Q}$?
(b) Find the Galois group of $f(x)$ over $\mathbb{Q}$.

Solution.

(a) The polynomial $f(x) = x^2 - 2$ is separable over $\mathbb{Q}$

The roots of the polynomial $f(x)$ are $\pm\sqrt{2}$. Since all the roots of $f(x)$ are distinct, $f(x) = x^2 - 2$ is separable.

(b) The Galois group of $f(x)$ over $\mathbb{Q}$

The Galois group of the separable polynomial $f(x) = x^2 - 2$ is the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$.
Since the roots of $f(x)$ are $\pm\sqrt{2}$, the splitting field of $f(x)$ is $\mathbb{Q}(\sqrt{2})$. Thus, we want to determine the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}).$$

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. Then the automorphism σ permutes the roots of the irreducible polynomial $f(x) = x^2 - 2$.
Thus $\sigma(\sqrt{2})$ is either $\sqrt{2}$ or $-\sqrt{2}$. Since σ fixes the elements of $\mathbb{Q}$, this determines σ completely as we have

$$\sigma(a + b\sqrt{2}) = a + b\sigma(\sqrt{2}) = a \pm \sqrt{2}.$$

The map $\sqrt{2} \mapsto \sqrt{2}$ is the identity automorphism 1 of $\mathbb{Q}\sqrt{2}$.
The other map $\sqrt{2} \mapsto -\sqrt{2}$ gives non identity automorphism τ. Therefore, the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \tau\}$ is a cyclic group of order 2.
In summary, the Galois group of the polynomial $f(x) = x^2 - 2$ is isomorphic to a cyclic group of order 2.

Polynomial $x^p - x + a$ is Irreducible and Separable Over a Finite Field

Problem 229

Let $p \in \mathbb{Z}$ be a prime number and let $\mathbb{F}_p$ be the field of p elements.
For any nonzero element $a \in \mathbb{F}_p$, prove that the polynomial

$$f(x) = x^p - x + a$$

is irreducible and separable over F_p.
(Dummit and Foote “Abstract Algebra” Section 13.5 Exercise #5 on p.551)
(Dummit and Foote “Abstract Algebra” Section 13.5 Exercise #5 on p.551)

Proof.

Separability

The separability can be checked by noting that the derivative of $f(x)$ is

$$f'(x) = px^{p-1} - 1 = -1$$

and is relatively prime to $f(x)$, and thus $f(x)$ is separable.
We give two proofs for the irreducibility of $f(x) = x^p - x + a$. Both proofs use the following lemmas.

Lemma 1

Lemma 1. If α is a root of $f(x) = x^p - x + a$, then $\alpha + j$ is a root of $f(x)$ for any $j \in \mathbb{F}_p$.

Proof of Lemma 1

We have

$$\begin{aligned} f(\alpha + j) &= (\alpha + j)^p - (\alpha + j) + a \\ &= \alpha^p + j^p - \alpha - j + a \\ &= f(\alpha) = 0. \end{aligned}$$

Here, we used Fermat's little theorem that $j^a = j$ in $\mathbb{F}_p$.
Thus, $\alpha + j$ is also a root of $f(x)$ for any $j \in \mathbb{F}_p$.

Lemma 2

Lemma 2. The polynomial $f(x) = x^p - x + a$ does not have a root in $\mathbb{F}_p$.

Proof of Lemma 2

If α is a root of $f(x)$ in $\mathbb{F}_p$, then we have

$$0 = f(\alpha) = \alpha^p - \alpha + a = a$$

since $\alpha^p = \alpha$ in $\mathbb{F}_p$ by Fermat's little theorem.
However, this contradicts that a is a nonzero element of $\mathbb{F}_p$.

Proof 1 of the irreducibility

Suppose that we have

$$f(x) = g(x)h(x)$$

for $g(x), h(x) \in \mathbb{F}_p[x]$.
By Lemma 1, if α is a root of $f(x)$, then $\alpha + j$ is also a root of $f(x)$ for any $j \in \mathbb{F}_p$. Thus, $\alpha + j$ is a root of either $g(x)$ or $h(x)$. From this, we obtain that

$$g(x) = \prod_{j \in I} (x - (\alpha + j)),$$

where I is a subset of $\mathbb{F}_p$.
Expanding the product, we see that

$$g(x) = x^n - \sum_{j \in I} (\alpha + j) x^{n-1} + \text{(lower terms)},$$

where $n = |I|$.
Since $g(x) \in \mathbb{F}_p[x]$, the coefficient of x^{n-1} is in $\mathbb{F}_p$. Thus we have

$$\mathbb{F}_p \ni \sum_{j \in I} (\alpha + j) = n\alpha + \sum_{j \in I} j.$$

Since $\sum_{j\in I} j \in \mathbb{F}_p$, we deduce that $n\alpha \in \mathbb{F}_p$.

Since by Lemma 2, $\alpha \notin \mathbb{F}_p$, we must have $n = 0$ in $\mathbb{F}_p$.

(Otherwise n is invertible in $\mathbb{F}_p$ and we would get $\alpha \in \mathbb{F}_p$.)

Therefore $n = |I|$ is either 0 or p.

If $n = 0$, then $g(x) = 1$. If $n = p$, then $h(x) = 1$. This implies that $f(x)$ is irreducible over $\mathbb{F}_p$.

Proof 2 of the irreducibility

We give another proof that $f(x) = x^p - x + a$ is irreducible over $\mathbb{F}_p$.

Let $m(x) \in \mathbb{F}_p[x]$ be the minimal polynomial of the root α of $f(x)$.

Then we have $f(x) = m(x)f_1(x)$ for some $f_1(x) \in \mathbb{F}_p[x]$.

If $f_1(x) = 1$, then $f(x) = m(x)$ is irreducible as the minimal polynomial is irreducible.

If not, then $f_1(x)$ has some root, and it must be of the form $\alpha + j$ for some $j \in \mathbb{F}_p$ by Lemma 1.

It is straightforward to check that the minimal polynomial of $\alpha + j$ is $m(x - j)$. Thus we can write

$f_1(x) = m(x - j)f_2(x)$.

If $f_2(x) = 1$, we stop here. If not we iterate the same procedure with f_2 as above. Eventually we obtain

$$f(x) = \prod_{j\in I} m(x - j)$$

for some subset I of $\mathbb{F}_p$.

Let n be the degree of $m(x)$. Then comparing the degree of both sides, we have

$$p = n|I|.$$

Since p is prime, we have either $n = 1, |I| = p$, or $n = p$, $|I| = 1$.

The former case implies that the minimal polynomial $m(x)$ of α is degree 1, and hence $\alpha \in \mathbb{F}_p$. However, this cannot happen by Lemma 2.

So we must have $n = p$ and $|I| = 1$, which deduce that $f(x) = m(x)$ and $f(x)$ is irreducible over $\mathbb{F}_p$.

Comment.

The polynomial $f(x) = x^p - x + a$ is studied in Artin–Schreier theory.

Show that Two Fields are Equal: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Problem 215

Show that fields $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are equal.

Proof.

It follows from $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ that we have $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

To show the reverse inclusion, consider

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

This yields that we have

$$\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Now we can express $\sqrt{2}$ in terms of elements of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ as follows. We have

$$\sqrt{6}(\sqrt{2} + \sqrt{3}) - 2(\sqrt{2} + \sqrt{3}) = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

(Note that the numbers on the left hand side are all in the field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.)
Hence we also have

$$(\sqrt{2}+\sqrt{3})-\sqrt{2}=\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Therefore the elements $\sqrt{2},\sqrt{3}$ are in the field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, hence

$$\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Since we showed both inclusions, we have

$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Galois Group of the Polynomial x^p-2.

Problem 110

Let $p\in\mathbb{Z}$ be a prime number.
Then describe the elements of the Galois group of the polynomial x^p-2.

Solution.

The roots of the polynomial x^p-2 are

$$\sqrt[p]{2}\zeta^k, k=0,1,\dots,p-1$$

where $\sqrt[p]{2}$ is a real p-th root of 2 and ζ is a primitive p-th root of unity.
(Explicitly, you may take $\zeta=e^{2\pi i/p}$.)
Thus x^p-2 is a separable polynomial over $\mathbb{Q}$. The Galois group of x^p-2 is the Galois group of the splitting field of x^p-2.
The splitting field of x^p-2 is $K:=\mathbb{Q}(\sqrt[p]{2},\zeta)$ of extension degree $p(p-1)$.
(Check this.)

Let $G=\mathrm{Gal}(K/\mathbb{Q})$ be the Galois group of x^p-2. The order of the Galois group G is $p(p-1)$. Let $\sigma\in G$ be an automorphism.
Then σ sends an element of G to its conjugate (a root of the minimal polynomial of the element.)
The minimal polynomial of $\sqrt[p]{2}$ is x^p-2 since it is irreducible by Eisenstein's criteria.
The minimal polynomial of ζ is the cyclotomic polynomial

$$\Phi(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1.$$

Therefore σ maps

$$\begin{aligned}\sqrt[p]{2}&\mapsto\sqrt[p]{2}\zeta^a\\ \zeta&\mapsto\zeta^b\end{aligned}$$

for some $a=0,1,\dots,p-1$ and $b=1,2,\dots,p-1$.
Thus there are $p(p-1)$ possible maps for σ.
Since the order of G is $p(p-1)$, these are exactly the elements of the Galois group G of the polynomial x^p-2

.

Two Quadratic Fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are Not Isomorphic

Problem 99

Prove that the quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Hint.

Note that any homomorphism between fields over $\mathbb{Q}$ fixes $\mathbb{Q}$ pointwise.

Proof.

Assume that there is an isomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$.
Let $\phi(\sqrt{2}) = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, where $a, b \in \mathbb{Q}$.
Then since ϕ fixes the elements of $\mathbb{Q}$, we have

$$\begin{aligned} 2 = \phi(2) = \phi((\sqrt{2})^2) = \phi(\sqrt{2})^2 \\ = (a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}. \end{aligned}$$

Hence we have $2 = a^2 + 3b^2$ and $2ab = 0$.
From the second equality, we must have $a = 0$ or $b = 0$. If $a = 0$, then $2 = 3b^2$, and $b = \pm\sqrt{2/3}$ but this is not a rational number. Hence $a \neq 0$ and $b = 0$.
But in this case, $2 = a^2$ and this implies that $a = \pm\sqrt{2}$, which is not a rational number.
This is a contradiction, and we conclude that the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Automorphism Group of $\mathbb{Q}(\sqrt[3]{2})$ Over $\mathbb{Q}$.

Problem 97

Determine the automorphism group of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.

Proof.

Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ be an automorphism of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.
Then σ is determined by the value $\sigma(\sqrt[3]{2})$ since any element α of $\mathbb{Q}(\sqrt[3]{2})$ can be written as
$\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ for some $a, b, c \in \mathbb{Q}$ and

$$\begin{aligned} \sigma(\alpha) &= \sigma(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) \\ &= \sigma(a) + \sigma(b)\sigma(\sqrt[3]{2}) + \sigma(c)\sigma(\sqrt[3]{2})^2 \\ &= a + b\sigma(\sqrt[3]{2}) + c\sigma(\sqrt[3]{2})^2 \end{aligned}$$

since σ fixes the elements in $\mathbb{Q}$.
Note that $\sigma(\sqrt[3]{2})$ is a root of the minimal polynomial $x^3 - 2$ of $\sqrt[3]{2}$.
But the roots of $x^3 - 2$ are not real except $\sqrt[3]{2}$, hence not in $\mathbb{Q}(\sqrt[3]{2})$.
Thus we must have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Hence σ is trivial.
In conclusion, we have

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/Q) = \{1\}.$$

Determine the Splitting Field of the Polynomial $x^4 + x^2 + 1$ over $\mathbb{Q}$

Problem 92

Determine the splitting field and its degree over $\mathbb{Q}$ of the polynomial

$$x^4+x^2+1.$$

Hint.

The polynomial x^4+x^2+1 is not irreducible over $\mathbb{Q}$.

Proof.

Note that we can factor the polynomial as follows.

$$\begin{aligned} x^4+x^2+1 &= x^4+2x^2+1-x^2 = (x^2+1)^2-x^2 \\ &= (x^2+x+1)(x^2-x+1). \end{aligned}$$

Thus the roots of the polynomial are

$$x=\frac{\pm 1 \pm \sqrt{-3}}{2}$$

by the quadratic formula.

The field $\mathbb{Q}(\sqrt{-3})$ contains all the roots of x^4+x^2+1.

Hence the splitting field is a subfield of $\mathbb{Q}(\sqrt{-3})$, and it is not $\mathbb{Q}$ since the roots are not real numbers.

Since the polynomial x^2+3 is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, the extension degree $[\mathbb{Q}(\sqrt{-3}):\mathbb{Q}]=2$.

Thus the field $\mathbb{Q}(\sqrt{-3})$ must be the splitting field and its degree over $\mathbb{Q}$ is 2.

In a Field of Positive Characteristic, $A^p=I$ Does Not Imply that A is Diagonalizable.

Problem 91

Show that the matrix $A=\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$, where α is an element of a field F of characteristic $p>0$ satisfies $A^p=I$ and the matrix is not diagonalizable over F if $\alpha \neq 0$.

Comment.

Remark that if A is a square matrix over $\mathbb{C}$ with $A^k=I$, then A is diagonalizable.

For a proof of this fact, see If a power of a matrix is the identity, then the matrix is diagonalizable

Thus, over a field of characteristic $p>0$ the condition $A^p=1$ dose not always imply that A is diagonalizable.

Proof.

By induction, it is straightforward to see that

$$A^m=\begin{bmatrix} 1 & m\alpha \\ 0 & 1 \end{bmatrix}$$

for any positive integer m.

Thus

$$A^p=\begin{bmatrix} 1 & p\alpha \\ 0 & 1 \end{bmatrix}=I$$

since $p\alpha=0$ in the field F.

Since the eigenvalues of A is 1, if A is diagonalizable, then there exists an invertible matrix P such that $P^{-1}AP = I$, or $AP = P$.

Let $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then we have

$$AP = \begin{bmatrix} a+\alpha c & b+\alpha d \\ c & d \end{bmatrix}$$

and this is equal to P, hence

$$a + \alpha c = a \text{ and } b + \alpha d = b$$

Thus

$$\alpha c = 0 \text{ and } \alpha d = 0$$

If $\alpha \neq 0$, then $c = d = 0$ but this implies that the matrix P is non-invertible, a contradiction.

Therefore we must have $\alpha = 0$.

The Polynomial $x^p - 2$ is Irreducible Over the Cyclotomic Field of p-th Root of Unity

Problem 89

Prove that the polynomial $x^p - 2$ for a prime number p is irreducible over the field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity.

Hint.

Consider the field extension $\mathbb{Q}(\sqrt[p]{2}, \zeta)$, where ζ is a primitive p-th root of unity.

Remark

The following proof proves more than enough. You might want to refine the proof for a simpler proof.

Proof.

We first determine the splitting field of $x^p - 2$.

The roots of the polynomial $x^p - 2$ are

$$\sqrt[p]{2}\zeta^i,$$

where ζ is a primitive p-th root of unity and $i = 0, 1, \dots, p-1$.

Let F be the splitting field of $x^p - 2$. Since both $\sqrt[p]{2}$ and $\sqrt[p]{2}\zeta$ is in F, the quotient $\zeta = \sqrt[p]{2}\zeta / \sqrt[p]{2} \in F$.

Therefore we see that $\mathbb{Q}(\sqrt[p]{2}, \zeta) \subset F$. Since the field $\mathbb{Q}(\sqrt[p]{2}, \zeta)$ contains all the roots of $x^p - 2$, we must have $F = \mathbb{Q}(\sqrt[p]{2}, \zeta)$.

Next, we find the degree of the extension $\mathbb{Q}(\sqrt[p]{2}, \zeta)$ over $\mathbb{Q}$.

The field $\mathbb{Q}(\sqrt[p]{2}, \zeta)$ contains the cyclotomic field $\mathbb{Q}(\zeta)$ as a subfield and we obtain $\mathbb{Q}(\sqrt[p]{2}, \zeta)$ by adjoining $\sqrt[p]{2}$ to $\mathbb{Q}(\zeta)$.

Since $\sqrt[p]{2}$ is a root of $x^p - 2$, the degree of the extension $[\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}(\zeta)] \leq p$.

Thus we have

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] \leq p(p-1)$$

since the degree of cyclotomic extension over $\mathbb{Q}$ is $\phi(p) = p - 1$. (Here ϕ is the Euler phi function.)

Note that $\mathbb{Q}(\sqrt[p]{2})$ is also a subfield and $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p$ since $x^p - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion.

Hence both p and $p-1$ divide $[\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}] \leq p(p-1)$. Since p is a prime, the numbers p and $p-1$ are relatively prime. Thus we must have $[\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}] = p(p-1)$.

In particular, the polynomial $x^p - 2$ must be irreducible over $\mathbb{Q}(\zeta)$ otherwise the degree $[\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}]$ is strictly less than $p(p-1)$.

Algebraic Number is an Eigenvalue of Matrix with Rational Entries

Problem 88

A complex number z is called ***algebraic number*** (respectively, ***algebraic integer***) if z is a root of a monic polynomial with rational (respectively, integer) coefficients.

Prove that $z \in \mathbb{C}$ is an algebraic number (resp. algebraic integer) if and only if z is an eigenvalue of a matrix with rational (resp. integer) entries.

Hint.

Use the companion matrix.

Recall that the characteristic polynomial of the companion matrix of a polynomial is the polynomial.

See the post Companion matrix for a polynomial for the definition of the companion matrix and the proof of the above fact.

Proof.

$(\implies)$

Suppose that z is algebraic number (resp. algebraic integer). Then z is a root of a monic polynomial

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where a_i are rational numbers (resp. integers).

Then consider the matrix

$$A = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}.$$

Note that the matrix A has rational (resp. integer) entries. Then the characteristic polynomial $\det(xI - A)$ of A is the polynomial $p(x)$.

Hence z is an eigenvalue of the matrix A.

$(\impliedby)$

Suppose that z is an eigenvalue of a matrix A with rational (resp. integer) entries.

Then z is a root of the characteristic polynomial of A.

The characteristic polynomial of A is a monic polynomial with rational (resp. integer) coefficients. Thus z is an algebraic number (resp. integer).

Degree of an Irreducible Factor of a Composition of Polynomials

Problem 83

Let $f(x)$ be an irreducible polynomial of degree n over a field F. Let $g(x)$ be any polynomial in $F[x]$.
Show that the degree of each irreducible factor of the composite polynomial $f(g(x))$ is divisible by n.

Hint.

Use the following fact.

Let $h(x)$ is an irreducible polynomial over a field F.

Let α be a root of $h(x)$.

(That is, $h(x)$ is the minimal polynomial of α over F.)

Then we have

$$\deg(h(x)) = [F(\alpha) : F].$$

Proof.

Let $h(x)$ be an irreducible factor of $f(g(x))$. Let β be a root of $h(x)$.

Put $\alpha = g(\beta)$. Then α is a root of $f(x)$ since we have

$$f(\alpha) = f(g(\beta)) = 0.$$

Since $f(x)$ is irreducible, $[F(\alpha) : F] = n$.

Since $g(\beta) \in F(\beta)$, the field $F(g(\beta))$ is a subfield of the field $F(\beta)$.

Thus we have

$$\begin{aligned} \deg(h(x)) &= [F(\beta) : F] \text{ (since } h(x) \text{ is irreducible)} \\ &= [F(\beta) : F(g(\beta))][F(g(\beta)) : F] \\ &= [F(\beta) : F(g(\beta))][F(\alpha) : F] \\ &= [F(\beta) : F(g(\beta))] \cdot n. \end{aligned}$$

Hence n divides the degree of the irreducible factor $h(x)$ of the composite $f(g(x))$.

$x^3 - \sqrt{2}$ is Irreducible Over the Field $\mathbb{Q}(\sqrt{2})$

Problem 82

Show that the polynomial $x^3 - \sqrt{2}$ is irreducible over the field $\mathbb{Q}(\sqrt{2})$.

Hint.

Consider the field extensions $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[6]{2})$.

Proof.

Let $\sqrt[6]{2}$ denote the positive real 6-th root of of 2.

Then since $x^6 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, hence it is the minimal polynomial for $\sqrt[6]{2}$ over $\mathbb{Q}$. Therefore, we have $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$.

Similarly, we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Since $\mathbb{Q}(\sqrt[6]{2}) \ni (\sqrt[6]{2})^3 = \sqrt{2}$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we must have

$$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3.$$

Note that $\sqrt[6]{2}$ is a root of the polynomial $x^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$.
Hence it must be the minimal polynomial for $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$.
In particular, the polynomial is irreducible over $\mathbb{Q}(\sqrt{2})$.