

- a) x is nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$.
- b) Let $H \leq G$ be a subgroup. Then $|H|$ divides $|G|$.
- c) $Z(G) = \{zg = gz \mid z \in G \text{ for all } g \in G\}$
- d) $\phi: G \rightarrow H$ is an isomorphism if it is a homomorphism (meaning $\phi(gh) = \phi(g)\phi(h)$) that is both surjective and injective, meaning onto and one-to-one.
- e) Let $N \trianglelefteq G$ be normal. Then $gng \in N$ for all $n \in N, g \in G$.
- f) $(2\ 3\ 6\ 1)(2\ 6)(2\ 1)(1\ 5\ 4\ 2)(3\ 1\ 7)(7\ 8\ 4) = (7\ 8\ 2\ 1)(5\ 4\ 6\ 3)$
- g) $LCM = 4$, order of $(7\ 8\ 2\ 1)(5\ 4\ 6\ 3)$ is 4
- h) Let $\phi: G \rightarrow H$ be a ^{homomorphism} ~~function~~. Then $\ker(\phi) \trianglelefteq G$ and $G/\ker(\phi) \cong \text{im}(\phi)$.
There exists an isomorphism from \ker of that function.
- i) Let T be a subring and I be an ideal.
Then $(T+I)/I \cong T/(T \cap I)$, ~~the number of subrings containing I is one-to-one to the n~~
- j) $\text{degree}(f(x)) = n$, where $n \in \mathbb{N}$ is the exponent of the maximal term in the polynomial $f(x)$.
- k) $r \in R$ is irreducible if there exists no elements $x, y \in R$ such that $xy = r$.

l) The group action is given by $G \times A \rightarrow A$ such that
$$g_1 \cdot (g_2 \cdot a) = (g_1 \cdot g_2) \cdot a \text{ for } g_1, g_2 \in G \text{ and } a \in A$$

and $e \cdot a = a$ for $e \in G$.

m) Sylow p -subgroup is a subgroup of G with order p^a , (a subgroup that is a p -group).

n) _____

o) _____

n) An unique factorization domain is a ring where all elements $r \in R$ are irreducible.

2. Let R be a ring and I and J be left ideals of R .

Then $rI \subseteq I$ and $rJ \subseteq J$ for all $r \in R$.

This also means that for any $r \in R$ and any $i \in I$ and $j \in J$, $r \cdot i \in I$ and $r \cdot j \in J$.

Consider $I \cap J$.

An element $x \in (I \cap J)$ is both $x \in I$ and $x \in J$.

Therefore for any element $y = r \cdot x$, $r \in R$:

$$x \in I \rightarrow y \in I \quad \text{and}$$

$$x \in J \rightarrow y \in J.$$

Therefore $y = r \cdot x$ is both in I and J and hence

$$y \in (I \cap J).$$

So $r(I \cap J) \subseteq (I \cap J)$ is a left ideal.

3. Let $(G, *)$ and (H, \circ) be groups.

Consider $G \times H$ with an operation given by

~~$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$$~~

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

Observe that $G \times H$ is closed under multiplication:

$(g_1, h_1), (g_2, h_2) \in G \times H$ and

$$(g_1 * g_2, h_1 \circ h_2) = (g_3, h_3) \in G \times H \text{ for}$$

$$g_1 * g_2 = g_3 \in G \quad \text{and} \quad h_1 \circ h_2 = h_3 \in H.$$

It is associative: Let $(g, h), (x, y), (a, b) \in G \times H$.

$$\begin{aligned} (g, h) \cdot [(x, y) \cdot (a, b)] &= (g, h) \cdot (x * a, y \circ b) \\ &= (g * x * a, h \circ y \circ b) \\ &= (g * x, h \circ y) \cdot (a, b) \\ &= [(g, h) \cdot (x, y)] \cdot (a, b) \end{aligned}$$

It has identity: $(g, h) \cdot (I_G, I_H) = (g * I_G, h \circ I_H) = (g, h) \in G \times H$

And inverses: For $(g, h) \in G \times H$, consider $g^{-1} \in G$ and $h^{-1} \in H$. Thus $(g^{-1}, h^{-1}) \in G \times H$ and hence

$$(g, h) \cdot (g^{-1}, h^{-1}) = (g * g^{-1}, h \circ h^{-1}) = (I_G, I_H) = 1.$$

So $G \times H$ is a group under its operation.

1. Let R be commutative with identity and $M \subsetneq R$ be an ideal. Therefore $1 \in R$, $xy = yx$ for $\forall x, y \in R$, and $rM \subseteq M$ and $Mr \subseteq M$ for every $r \in R$, too.

Let M be maximal. Then for any $M \subseteq I \subseteq R$, $I = R$ as M is the largest ideal that contains itself but is not R .

Consider $R/M := \{r+M \mid r \in R\}$. R/M is commutative because R is commutative.

Consider a nonzero element $u \in R/M$. Then let $u = x + M$ for some $x \in R$.

Let $v = y + M$ for some $y \in R$ such that

$xy \in M$. Then $uv = (x+M)(y+M) = xy + (x+y)M + M$, which is contained in M as M is maximal and thus $(x+y)M \subseteq M$ since no other ideal $I \neq R$ is greater.

Hence ~~$uv = M$~~ $uv = M$, and u is a unit of R/M , and R/M is a commutative division ring.

Let R/M be a field. Then every nonzero element of R/M is a unit. Thus for $u \in R/M$, there exists some $v \in R/M$ such that $uv = M$.

Assume M wasn't maximal. Then some $M \subsetneq I \subsetneq R$ ideal would contain M , and hence some cosets $a, b, c, \dots \in R/M$ would give as a product I . However every element product is a unit and thus $M = I$ so M is maximal.

6. Let R be a ring with a left identity:

1_L such that $1_L \cdot r = r$, $r \in R$ and

a right identity:

1_R such that $r \cdot 1_R = r$, $r \in R$.

Now consider $e = 1_R \cdot 1_L$.

If $e = 1_R$ or $e = 1_L$, then either 1_L or 1_R are two-sided unique as $r(1_R \cdot 1_L) = r$ and $(1_R \cdot 1_L)r = r$.

If $1_R \cdot 1_L \neq 1_L$ and $1_R \cdot 1_L \neq 1_R$ then consider

$$r \cdot e = (r \cdot 1_R) \cdot 1_L = r \cdot 1_L \quad \text{and}$$

$$e \cdot r = 1_R \cdot (1_L \cdot r) = 1_R \cdot r \quad \text{and}$$

$$r \cdot e \cdot s = (r \cdot 1_R) (1_L \cdot s) = r \cdot s.$$

Then as $r \cdot e \cdot s = r \cdot s$, $e = 1$ and two-sided.

Thus R contains a unique two-sided identity with $1_R \in R$ and $1_L \in R$.

7. Let A be a finite abelian group. Then $|A| \neq \infty$ and for every $x, y \in A$, $xy = yx$.

Let A be cyclic. Then $A = \langle a \rangle$ for some $a \in A$, and $|\langle a \rangle| = |A| \neq \infty$.

Consider any Sylow p -subgroup of A . If $|A| = n$, then the p -subgroups of A are each $H \leq A$ such that $|H| = p^m$, where $p^m \mid n$ and $m \in \mathbb{N}$, p is prime.

But observe for any $b \in H$, $b = a^i$ as A is cyclic.

8. Let us consider factors of 400:

$$400 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 = 2^4 \cdot 5^2$$

Thus G with order $|G| = 400$ can be

$$\mathbb{Z}_{25} \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_{25} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_{25} \oplus \mathbb{Z}_{16},$$

$$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \text{ and}$$

$$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{16}.$$

Hence there are 8 abelian groups of order 400 up to isomorphism.

9. Suppose that R is a commutative ring with 1 and $S \subset R$ is a multiplicatively closed set.

Then for $x, y \in S$, $xy \in S$.

Let $s \in S$ be nilpotent. Then $s^n = 0$ for some $n \in \mathbb{N}$. Consider the ring $S^{-1}R = R_S$.

We have that the set S is multiplicatively closed and each element is nilpotent. We want to know how many elements are in

$$S^{-1}R := \{s^{-1}r \mid r \in R, s^{-1} \text{ is the inverse of } s \in S\}$$

This is the ring of elements that are products of inverses of S and R . There are $|R|$ many elements of R , and each nilpotent element in S has n many inverses (as S is closed under multiplication and therefore $s^1 \cdot s^1 \in S \dots s^{n-1} \in S \dots s^n = 0 \in S$).

Therefore there are, for each m where $s \in S$ has $s^m = 0$, $m \cdot |R|$ many elements in R_S .