Abstract Algebra Select Solutions

MyMathYourMath.com
Solutions by: Sean Zhu & Hossien Sahebjame

2021

Contents

28. In integral domain prime implies irreducible
29. In PID irreducible implies prime.
30. P prime iff R/P integral domain in commutative ring with 1
31. Every maximal ideal in commutative ring with 1 is prime

1. Subgroups closed under (arbitrary) intersections

Let G be a group. If $H \leq G, K \leq G$, then $H \cap K \leq G$.

Proof. First we show this for the case with two subgroups. Let G be a group. Suppose that

$$H \leq G, K \leq G.$$

We must show

$$H \cap K \leq G.$$

First we show non-empty. Note that $e_G \in H$ and $e_G \in K$ as they are subgroups forcing

$$e_G \in H \cap K,$$

and we have that the intersection is non-empty. Next for subgroup criterion, let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$. As H, K are subgroups we have by subgroup criterion that

$$xy^{-1} \in H \wedge xy^{-1} \in K.$$

Forcing

$$xy^{-1} \in H \cap K$$

as needed and thus $H \cap K \leq G$.
Next suppose that $\{H_i\}_{i \in I}$ is a collection of subgroups in G, for I some arbitrary indexing set. We want to show

$$\bigcap_{i \in I} H_i \leq G.$$

As $H_i \leq G$ for each $i \in I$ we have

$$e_G \in \bigcap_{i \in I} H_i$$

thus the intersection of the H_i is non-empty. Let $x, y \in \bigcap_{i \in I} H_i$ then $x, y \in H_i$ for every $i \in I$. Since the H_i are all subgroups, by the subgroup criteria,

$$xy^{-1} \in H_i$$

for every $i \in I$ hence

$$xy^{-1} \in \bigcap_{i \in I} H_i$$

and thus $\bigcap_{i \in I} H_i \leq G$ as needed. □

<back2top>

2. Cyclic Groups

Let G be a finite group.
(a) Prove subgroups of G need be cyclic.

Proof. Let G be a cyclic group and H a nontrivial proper subgroup. As G is cyclic, we have

$$G = \langle x \rangle.$$

Then $x^n \in H$ for some $n \in \mathbb{N}$ and let $m \in \mathbb{Z}^+$ be the smallest such that

$$x^m \in H.$$

I claim that

$$H = \langle x^m \rangle$$

Let $h \in H$, as $H \leq G$ we know there exists some $k \in \mathbb{Z}^+$ such that

$$h = x^k$$

for some n. Then by the Division Algorithm there exists q, r such that

$$k = qm + r$$

with $0 \leq r < m$. Thus we can write

$$\begin{aligned} h &= x^k \\ &= x^{mq+r} \\ &= (x^m)^q x^r. \end{aligned}$$

This gives us that $x^r = (x^m)^{-q} a^n \in H$ by closure of subgroups. Contradicting minimality of m because then $r = 0$ and $h \in H$ is a power of x^m thus

$$H = \langle x^m \rangle$$

is cylic. □

(b) Let $H \trianglelefteq G$. If H is cyclic, then every subgroup of H is normal in G.

Proof. As $H \trianglelefteq G$ we know that for every $h \in H, g \in G$ that

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

Let $K \leq H$. As H is cyclic and subgroups of cyclic need be cyclic, we have that K is cyclic as well. That is,

$$K = \langle h^m \rangle$$

for $h \in H$ and some $m \in \mathbb{Z}^+$. Let $g \in G, k \in K$, then there is an $n \in \mathbb{Z}^+$ such that

$$k = h^{mn}.$$

Then we can compute

$$\begin{aligned} gkg^{-1} &= g(h^{mn})g^{-1} && \text{substitute for } k \\ &= (ghg^{-1})^{mn} && \text{conjugation} \\ &= (h^l)^{mn} && \text{some } l \in \mathbb{Z}^+ \text{ as } H \trianglelefteq G \\ &= k^l && \text{commutivity of exponents, substitute for } k \\ &\in K && K \text{ is cyclic} \end{aligned}$$

as needed and thus $K \trianglelefteq G$. □

(c) Show (b) is false if H is not cyclic.

Proof. Consider the group $G = S_3$ given by

$$\{e, (12), (13), (23), (123), (132)\}.$$

Clearly we have that $G \trianglelefteq G$ however G is not cylic. To see this look at the subgroup

$$\{e, (12)\},$$

Then for the element $g = (123)$ we have that

$$(123)(12)(132) = (23) \notin G$$

as a counterexample. □

<*back2top*>

3. Commutative ring and ideals

Let R be a commutative ring.
(a) Prove the only ideals of R are $\{0\}$ and R itself if and only if R is a field.

Proof. Let R be a commutative ring. First let us assume the only ideals are the zero ideal and R itself. It is enough to show any nonzero element of R has a multiplicative inverse. Let $0 \neq r \in R$. We must show there is some $s \in R$ such that

$$rs = e_R.$$

Consider the ideal (r). So then (r) is either the zero ideal or R itself. But

$$r \neq 0$$

thus (r) cannot be the zero ideal and so (r) must be all of R. That is,

$$R = (r).$$

Thus $e_R \in (r)$ and so there exists some $s \in R$ such that

$$rs = e_R.$$

And therefore R is a field.
On the other hand, suppose R is a field. We must show the only ideals of R are itself and the zero ideal. Let I be a non-zero ideal of R. I claim $I = R$. As I is not the zero ideal there exists some $r \in I$ with $r \neq 0$. As R is a field there exists some $s \in R$ such that

$$rs = e_R.$$

Therefore $e_R \in I$ giving us that

$$I = R$$

as needed. □

(b) Prove that if R has exactly 3 ideals, R is not an integral domain.

Proof. Let R be a ring with exactly 3 ideals I_1, I_2, I_3 where I_1 is the zero ideal, $I_2 = R$ and I_3 is a proper non-trivial ideal. Let us assume now that R is an integral domain and let $a \in I_3$ be non-zero. Then $I_3 = (a)$. Next, consider the ideal generated by a^2. If (a^2) is the zero ideal then $a^2 = 0$ but $a \neq 0$, a contradiction. So it must be that

$$\begin{aligned} I_3 &= (a) \\ &= (a^2). \end{aligned}$$

So there exist some $b \in R$ such that

$$a = a^2 b.$$

This holds if and only if $a(1 - ab) = 0$ and as $a \neq 0$, $ab = e_R$ contradicting the fact that a is a non-unit and thus R is not an integral domain. □

<back2top>

4. Ring Homomorphism

Let R, S be commutative rings with identity and let ϕ be a surjective ring homomorphism between them. Prove $\phi(e_R) = e_S$ and that if M is a maximal ideal in R, then $\phi(M)$ is either all of S is a maximal ideal in S.

Proof. Let R, S be commutative rings and

$$\phi : R \to S$$

be a surjective homomorphism of rings. We must show

$$\phi(e_R) = e_S.$$

But as ϕ is a ring homomorphism we can write

$$\begin{aligned}\phi(e_R) &= \phi(e_R e_R) \\ &= \phi(e_R)\phi(e_R).\end{aligned}$$

And if we hit each side with $\phi(e_R)^{-1}$ then we have

$$\begin{aligned}e_S &= \phi(e_R)\phi(e_R)^{-1} \\ &= \phi(e_R)\end{aligned}$$

as needed.
Now let us assume M is a maximal ideal in R. We must show $\phi(M) = S$ or is a maximal ideal in S. First, we show $\phi(M)$ is an ideal in S. Let $s \in S$, by surjectivity of ϕ there exists some $r \in R$ such that

$$\phi(r) = s.$$

Thus

$$\begin{aligned}s\phi(M) &= \phi(r)\phi(M) && \text{surjectivity of } \phi \\ &= \phi(rM) && \phi \text{ is ring homomorphism} \\ &= \phi(M) && \text{M is an ideal.}\end{aligned}$$

Now let us assume $\phi(M)$ is not all of S. Let I be an ideal of S such that

$$\phi(M) \subsetneq I \subset S.$$

I claim $I = S$ and we would be done. Let $s \in I \setminus \phi(M)$. By surjectivity of ϕ we are guaranteed the existence of some $r \in R$ such that $\phi(r) = s \notin \phi(M)$. Thus $r \in M$ which is maximal thus there is some $x \in R$ and $m \in M$ such that

$$e_R = xr + m.$$

By the earlier part of this problem we can compute out

$$\begin{aligned}e_S &= \phi(e_R) \\ &= \phi(xr + m) \\ &= \phi(x)\phi(r) + \phi(m) \\ &\in (\phi(r), \phi(M)) \\ &= (s, \phi(M)).\end{aligned}$$

Forcing $e_S \in I$ thus $I = S$ hence $\phi(M)$ is a maximal ideal of S.

□

<back2top>

5. Group of order 12 $\cong A_4$

Let G be a group of order 12. Prove if $Z(G)$ contains no element of order 2, then $G \cong A_4$.

Proof. As G has order $|G| = 12 = 2^2 \cdot 3$, By the Sylow Theorem, the number of Sylow 3-subgroups is $n_3 \equiv 1 \mod 3$ where $n_3 \mid 4$. Thus n_3 is either 1 or 4.
Let us first assume $n_3 = 4$ and let $P_1, P_2 \in Syl_3(G)$. Then we have that

$$1 \leq |P_1 \cap P_2| \leq |P_1| = 3.$$

By Lagranges theorem, this forces $|P_1 \cap P_2|$ to be 1 or 3. If P_1, P_2 are distinct, then their intersection is 1. So we can assume they are not distinct then each sylow 3-subgroup has 3 elements and so in the 4 Sylow 3-subgroups there is a total of $2 \cdot 4 = 8$ distinct elements of order 3.

Now we let G act on its 4 Sylow 3-subgroups via conjugation. This action is transitive as the subgroups are conjugates of one another thus there is only one orbit for this group action. Then the permutation representation

$$\phi : G \to S_4$$

is non-trivial. Thus we can define

$$\ker \phi = \{g \in G : gPg^{-1} = P, \forall P \in Syl_3(G)\}.$$

This satisfies the condition of the normalizer of P in G. Thus

$$\ker \phi \leq N_G(P).$$

Let $P \in Syl_3(G)$. Since the only conjugates of P is another element of $Syl_3(G)$ and $|Syl_3(G)| = 4$, then $|G : N_G(P)| = 4$ forcing $|N_P(G)| = 3$. Since P has order 3 it must be that

$$P = N_P(G).$$

Then we have that

$$\ker \phi \leq P.$$

And so by Lagranges theorem either the kernel is trivial or is all of P. As kernel of homomorphisms are normal and P is not normal in G, the kernel is trivial and thus ϕ is 1-1. Since G has 8 elements of order 3, this must also holds for $\phi(G)$ in S_4. As permutations of order 3 are 3 cycles, there are exactly 8 3-cycles all contained in $A_4 \leq S_4$. So we have that

$$8 \leq |\phi(G) \cap A_4| = |A_4| = 12.$$

Thus by Lagranges theorem,

$$\phi(G) = A_4$$

forcing $G \cong A_4$. *Proof almost finished* □

<*back2top*>

6. Abelian Group

Prove a group G is cyclic if and only if $G/Z(G)$ is cylcic.

Proof. First let us suppose that $G/Z(G)$ is cyclic. Then we have that

$$G/Z(G) = \langle xZ(G) \rangle.$$

I claim that any $g \in G$ is of the form

$$x^n z$$

for some $n \in \mathbb{Z}$ and some $z \in Z(G)$. Let $g \in G$. Then

$$gZ(G) = x^n Z(G)$$

Hitting the left with g^{-1} we obtain

$$\begin{aligned} g^{-1}gZ(G) &= Z(G) \\ &= g^{-1}x^n Z(G) \end{aligned}$$

and thus $g^{-1}x^n \in Z(G)$ and so

$$g^{-1}x^n = z.$$

Then hitting both left sides by g we see that

$$x^n = gz$$

And both right sides by z^{-1} we get that

$$g = x^n z^{-1}.$$

Where $z^{-1} \in Z(G)$ and we have proven the claim. Lastly, to show G is abelian, let $a, b \in G$. Then we can write

$$a = x^n z, b = x^m w.$$

As $z, w \in Z(G)$ We have that

$$\begin{aligned} ab &= x^n z x^m w \\ &= x^n x^m z w \\ &= x^m x^n w z \\ &= x^m w x^n z \\ &= ba \end{aligned}$$

hence G is abelian.
On the other hand, suppose G is abelian. Then we have that

$$G = Z(G)$$

thus $G/G = \{e_G\}$ is trivially cyclic as needed. □

<*back2top*>

7. Normal subgroups

If $H \trianglelefteq K$ and $K \trianglelefteq G$, is $H \trianglelefteq G$?

Proof. This is false in general. To see this, take □

8. Normal subgroup intersected with arbitrary subgroup.

Let $G \trianglerighteq N$ and $H \leq G$. Show $H \trianglerighteq N \cap H$

Proof. If $h \in H$, then

$$h^{-1}Hh = H$$

as $H \leq G$. Furthermore for all $g \in G$, and elements of H, one has

$$h^{-1}Nh = N.$$

This is by normality of N. Thus if $x \in N \cap H$ and $h \in H$ we have

$$h^{-1}xh \in H \cap N$$

and we have what we needed, $H \cap N$ is normal in H. □

If $g^2 = e$ for all $g \in G$, G is abelian

If $g^2 = e$ for all $g \in G$, then G is abelian. Let $g, h \in G$, then we have

$$\begin{aligned}
(g \cdot h) \cdot (h \cdot g) &= g \cdot (h \cdot h) \cdot g && \text{by associativity of the group} \\
&= g \cdot e \cdot g && \text{by assumption} \\
&= g \cdot g && \text{definition of identity} \\
&= e && \text{by assumption}
\end{aligned}$$

But $g \cdot h$ has a unique inverse, namely $g \cdot h$ but we just showed

$$(g \cdot h) \cdot (h \cdot g) = e$$

Forcing

$$g \cdot h = h \cdot g$$

for all $h, g \in G$ thus G is abelian.

<back2top>

10. Kernal of group homomorphism is normal in the group

Let

$$\phi : G \to H$$

be a group homomorphism. Prove $\ker \phi \trianglelefteq G$.

Proof. We begin by showing $\ker \phi \leq G$. By the subgroup criteria, it suffices to show $\ker\phi$ is nonempty and for any $k_1, k_2 \in \ker \phi$, we have $k_1 k_2^{-1} \in \ker \phi$. As ϕ is a group homomorphism, it sends identities to identity. Thus we have that

$$\phi(e_G) = e_H$$

forcing $e_G \in \ker \phi$ thus $\ker \phi$ is non empty. Let $k_1, k_2 \in \ker \phi$. We check if $k_1 k_2^{-1} \in \ker \phi$. So we have

$$\begin{aligned}
\phi(k_1 k_2^{-1}) &= \phi(k_1)\phi(k_2^{-1}) && \text{as } \phi \text{ is a homomorphism} \\
&= \phi(k_1)\phi(k_2)^{-1} && \text{as } \phi \text{ is a homomorphism} \\
&= e_H \cdot e_H^{-1} && \text{definition of ker } \phi \\
&= e_H \cdot e_H && \text{identity is it's own inverse} \\
&= e_H && \text{identity times itself is itself}
\end{aligned}$$

thus $k_1 k_2^{-1} \in \ker \phi$ and we have that $\ker \phi \leq G$. Let $k \in \ker \phi$, we must show for every $g \in G$ that

$$gkg^{-1} \in \ker \phi.$$

We have that

$$\begin{aligned}
\phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g)^{-1} \\
&= \phi(g)e_H\phi(g)^{-1} \\
&= \phi(g)\phi(g)^{-1} \\
&= e_H.
\end{aligned}$$

This forces $gkg^{-1} \in \ker \phi$. Thus we have that $\ker \phi \trianglelefteq G$ as needed.
Next we show that if

$$\text{im}\phi = \{h \in H : \phi(g) = h; \quad \text{for some } g \in G\},$$

then $\text{im } \phi \leq H$. Clearly $\text{im } \phi$ is non empty, as the identity gets mapped to the identity, thus $e_H \in \text{im } \phi \neq \emptyset$. Lastly, by the subgroup criteria, we check if given $h_1, h_2 \in \text{im } \phi$, that $h_1 h_2^{-1} \in H$. Let $h_1, h_2 \in \text{im } \phi$ be given. Then there exists g_1, g_2 such that

$$\phi(g_1) = h_1, \phi(g_2) = h_2.$$

Then we have that

$$\begin{aligned}
h_1 h_2^{-1} &= \phi(g_1)\phi(g_2)^{-1} \\
&= \phi(g_1)\phi(g_2^{-1}) \\
&= \phi(g_1 g_2^{-1}),
\end{aligned}$$

however, as $G \leq G$, we have that $g_1 g_2^{-1} \in G$ forcing $h_1 h_2^{-1} \in \text{im } \phi$ thus $\text{im } \phi \leq H$ as desired. □

<back2top>

11. Show infinite cyclic groups are isomorphic to $\mathbb{Z}$.

Let G be an infinite cyclic group. Prove $G \cong \mathbb{Z}$.

Proof. We let $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Define the map

$$\phi : \mathbb{Z} \to G$$

via

$$n \mapsto g^n.$$

We must show ϕ is well-defined. We know that $g^n \neq g^m$ if and only if nm. Thus ϕ is well-defined. To show it is a homomorphism, let $n, m \in \mathbb{Z}$, then calculate $(n + m)$ as follows:

$$\begin{aligned} \phi(n+m) &= g^{n+m} \\ &= g^n g^m \\ &= \phi(n)\phi(m) \end{aligned}$$

Thus ϕ is a homomorphism. To show ϕ is onto, note as G is cyclic, every element of G is g raised to some power, thus for every $x \in G$, there exists some $k \in \mathbb{Z}$ such that

$$x = g^k.$$

And by definition of ϕ,

$$\phi(k) = g^k = x$$

and we have shown ϕ is onto. For 1-1, it follows that for every $m, n \in \mathbb{Z}$ such that $m \neq n$, then

$$g^m \neq g^n$$

and ϕ is 1-1 forcing $G \cong \mathbb{Z}$. □

<back2top>

12. If $G/Z(G)$ is cyclic, then G is abelian.

Let $G/Z(G)$ be cyclic. Prove then that G is abelian.

Proof. As $G/Z(G)$ is cyclic, there exists some $g \in G/Z(G)$ such that

$$G/Z(G) = \langle gZ(G) \rangle.$$

As g is a coset by $Z(G)$, we have that there exists some $h \in G$ with

$$g = hZ(G).$$

Hence every coset of $Z(G)$ by G is of the form

$$(hZ(G))^k; \qquad \text{for some } k \in \mathbb{Z}$$

Now let $g_1, g_1 \in G$ and suppose $g_1 \in h^m Z(G), g_2 \in h^n Z(G)$, then

$$g_1 = h^m z_1, g_2 = h^n z_2; \text{for some } z_1, z_2 \in Z(G).$$

We can now compute

$$\begin{aligned} g_1 g_2 &= h^m z_1 h^n z_2 \\ &= h^m h^n z_1 z_2 \\ &= h^{m+n} z_1 z_2 \\ &= h^{n+m} z_2 z_1 \\ &= h^n h^m z_2 z_1 \\ &= h^n z_2 h^m z_1 \\ &= g_2 g_1 \end{aligned}$$

Thus G is abelian. □

<*back2top*>

13. Finite Subgroups of group G.

Let G be a group and $H \subset G$ a nonempty finite subset. Prove $H \leq G$ if and only if for any $h_1, h_2 \in H$, $h_1 h_2 \in H$.

Proof. First off, if H is a subgroup, then clearly if $h_1, h_2 \in H$, we have that $h_1 h_2 \in H$ by closure. On the other hand, suppose that for any $h_1, h_2 \in H$, that $h_1 h_2 \in H$. We only need to show H has an inverse for each of its elements. Let $h \in H$. Then

$$h, h^2, h^3, ..., h^n, ...$$

all belong to H which is finite and closed under the operation, thus we have by finiteness that

$$h^m = h^n$$

for some integers $0 \leq m < n$. Thus hitting both sides by h^{-m} we have that $e = h^{n-m} \in H$. As $n - m \geq 1$, we have that

$$e = hh^{n-m-1}$$

implies $h^{-1} = h^{n-m-1} \in H$ for each $h \in H$, thus $H \leq G$.
The result does not hold if H is infinite, for counterexample take $G = (\mathbb{Z}, +)$ and $H = \{1, 2, 3, ...\}$, then $a + b \in H$ whenever $a, b \in H$ but H is not a subgroup as $0 \notin H$. □

<back2top>

14. Subgroup is subgroup of normalizer

Let $H \leq G$, prove $H \leq N_G(H)$.

Proof. First a claim. If $K \leq G$ and $H \subset K$, then $H \leq K$. To see why, let $h_1, h_2 \in H$, then are in G thus by the subgroup criteria we have that $h_1 h_2^{-1} \in H$ thus by subgroup crietria for K, $H \leq K$. Now to show $H \subset N_G(H)$, we show $hHh^{-1} = H$. Let $h \in H$, then if $a \in H$, we have that

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

as $H \leq G$, thus $hHh^{-1} \subset H$. Moreover, if $a \in H$, then we have

$$a = h(h^{-1}ah)h^{-1}$$

forcing $H \subset hHh^{-1}$. Thus by our claim we have that $H \leq N_G(H)$. Moreover, we can show $H \leq C_G(H)$ if and only if H is abelian. First suppose H is abelian, then

$$h_1 h_2 = h_2 h_1.$$

Hitting both sides with h_1^{-1} we have

$$h_1 h_2 h_1^{-1} = h_2$$

thus $h_1 \in C_G(H)$. On the other hand, suppose $H \leq C_G(H)$. If $h_1, h_2 \in H$, then we have that

$$h_1 h_2 h_1^{-1} = h_2$$

hitting both sides with h_1 we obtain

$$h_1 h_2 = h_2 h_1$$

forcing H to be abelian. □

<*back2top*>

15. If G has order $n > 2$ then it contains no subgroup of order $n - 1$.

Let G be a finite group of order $n > 2$. Prove it cannot contain a subgroup of order $n - 1$.

Proof. Let $g \in G \setminus H$ and consider gH. I claim that

$$gH \cap H = \emptyset.$$

If not, then there exists some h such that $h \in H$ and $h \in gH$. The latter implies

$$h = gk$$

for some $k \in H$ which forces

$$g = hk^{-1} \in H$$

a contradiction. Forcing

$$gH \cap H = \emptyset.$$

Supposing H has $n-1$ elements, then gH and H both have $n-1$ elements, their union has $2(n-1)$ elements contradicting G having $n > 2$ elements.
Alternatively, let G be a group of order $n > 2$ and let H be a subgroup of order $n - 1$ and let $g \in G \setminus H$. Let $h \in H$ be a non-identity element. If $gh \in H$, then $(gh)h^{-1} \in H$ a contradiction forcing $gh \in G \setminus H$. Thus

$$gh = g$$

for every $h \in H$. I.e,

$$h = e$$

for every $h \in H$ thus $H = \{e\}$ contradicting G having order $n > 2$ and H having order $n - 1$. Therefore no such subgroup exists. □

<back2top>

16. Show the commutator subgroup is normal in the group.

Let G be a group and let G' denote the group generated by all commutators. That is, elements of the form $[x, y]$ where

$$[x, y] := x^{-1}y^{-1}xy.$$

Show $G' \trianglelefteq G$.

Proof. Note if $h \in G'$ and if $g \in G$, then $[h, g] = h^{-1}g^{-1}hg \in G'$ as G' is closed under the group operation and inverses. However,

$$h(h^{-1}g^{-1}hg) = g^{-1}hg \in G'$$

This forces

$$ghg^{-1} \in G'$$

and $G' \trianglelefteq G$ as needed.
Moreover, we prove G/G' is abelian. Let $xG', yG' \in G/G'$. Then

$$x^{-1}y^{-1}xyG' = G'$$

As $x^{-1}y^{-1}xy$ is a commutator and thus belongs to G'. But this forces

$$xyG' = yxG'$$

thus x, y commute in G/G' making it abelian. □

<back2top>

17. Show the characteristic subgroup is a normal subgroup

Let $H \leq G$ be characteristic. Prove $H \trianglelefteq G$.

Proof. We want to show

$$gHg^{-1} = H$$

for all $g \in G$. Define the automorphism $\phi_g(h) := ghg^{-1}$. Then we have that

$$\phi_g(H) = gHg^{-1} = H$$

where the last equality holds as H is characteristic. □

<*back2top*>

18. Subgroup is normal iff its the kernal of some group homomorphism.

Let G be a group and $N \leq G$ a subgroup. Prove $N \trianglelefteq G$ if and only if $N := \ker \phi$ for some

$$\phi : G \to H$$

a group homomorphism.

Proof. First suppose $N := \ker \phi$ where

$$\phi : G \to H$$

is a group homomorphism. Its enough to show for every $g \in G$ that

$$gNg^{-1} \subset N.$$

So let $x \in gNg^{-1}$, then $x = gng^{-1}$ for some $n \in N$. Then we check to see if $x \in \ker \phi$. We have that

$$\begin{aligned}
\phi(x) &= \phi(gng^{-1}) && \text{for some } n \in N \\
&= \phi(g)\phi(n)\phi(g)^{-1} && \text{as } \phi \text{ is a homomorphism} \\
&= \phi(g)e_H\phi(g)^{-1} && \text{as } n \in N := \ker \phi \\
&= \phi(g)\phi(g)^{-1} && \text{definition of mult by identity} \\
&= e_H && \text{definition of inverses}
\end{aligned}$$

thus $x \in \ker \phi := N$, as needed thus $N \trianglelefteq G$.
On the other hand suppose $N \trianglelefteq G$ and show its the kernal of some group homomorphism. Let $H = G/N$ and define

$$\pi : G \to G/N$$

via

$$g \mapsto gN$$

for every $g \in G$. By definition of operation in G/N, we have that

$$\begin{aligned}
\pi(g_1g_2) &= (g_1g_2)N \\
&= g_1Ng_2N \\
&= \pi(g_1)\pi(g_2)
\end{aligned}$$

thus π is a homomorphism. We compute its kernal as

$$\begin{aligned}
\ker \pi &= \{g \in G : \pi(g) = 1N\} \\
&= \{g \in G : gN = 1N\} \\
&= \{g \in G : g \in N\} \\
&= N
\end{aligned}$$

and thus N is the kernal of some group homomorphism. □

<back2top>

19. Show $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic of order mn iff $(m,n) = 1$

Let

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

be a group. Prove it is cyclic if and only if $(m,n) = 1$.

Proof. First suppose $(m,n) = 1$. Then

$$[m,n] = mn.$$

Thus the order of $(1,1)$ is mn which is the order of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\mathbb{Z}$ thus $(1,1)$ generates the group and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\mathbb{Z}$ is cyclic.
On the other hand, suppose $(m,n) > 1$, then $[m,n] < mn$. Let $(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\mathbb{Z}$ with p the order of $a \in \mathbb{Z}/m\mathbb{Z}$ and q the order of $b \in \mathbb{Z}/n\mathbb{Z}$. As $a \mid m$ and $b \mid n$, we can write

$$pk = [m,n] = ql.$$

Then we have

$$\begin{aligned}[m,n](a,b) &= ([m,n]a, [m,n]b) \\ &= (k(pa), l(qb)) \\ &= (k \cdot 0, l \cdot 0)\end{aligned}$$

Thus

$$|(a,b)| < mn$$

and as (a,b) was arbitrary, no element can have order mn thus $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\mathbb{Z}$ is not cyclic of order mn as a generator would need to have order mn. □

<back2top>

20. Order of elements in $\mathbb{Z}/n\mathbb{Z}$.

If $x \in \mathbb{Z}/n\mathbb{Z}$, then

$$|x| = \frac{n}{(n, x)}.$$

As the (multiplicative) order of the element.

<back2top>

21. Cylic groups need be abelian

Let G be a cyclic group. Prove G is abelian.

Proof. Let g be the generator of G. Let $a, b \in G$ be distinct. Then $a = g^m, b = g^n$ where $m \neq n$. Then we have

$$\begin{aligned} ab &= g^m g^n \\ &= g^{m+n} \\ &= g^{n+m} \\ &= g^n g^m \\ &= ba \end{aligned}$$

as needed making G abelian. □

<*back2top*>

22. If $H \leq G$, $K \leq G$, then $HK \leq G$ iff $HK = KH$.

Let $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.

Proof. First suppose $HK = KH$. Let $H, K \leq G$ and let $a, b \in HK$, then we wish to show $ab^{-1} \in HK$. But we can write

$$a = h_1k_1, b = h_2k_2$$

for some $h_1, h_2 \in H$, and $k_1, k_2 \in K$, then b^{-1} becomes

$$k_2^{-1}h_2^{-1}.$$

Then we have

$$ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$$

where $k_3 = k_1k_2^{-1} \in K$ as $K \leq G$. Letting $h_3 = h_2^{-1} \in H$ as $H \leq G$, we can write

$$ab^{-1} = h_1k_3h_3.$$

But since $HK = KH$, we have that

$$k_3h_3 = h_4k_4$$

for some $h_4, k_4 \in H, K$ respectively. Then we can write

$$ab^{-1} = h_1h_4k_4 \in HK$$

as $h_1h_4 \in H$ and $k_4 \in K$.
On the other hand suppose $HK \leq G$ and $H, K \leq G$. Then we show $HK = KH$ via set containment. As $K \leq HK, H \leq HK$, we have by subgroup closure that $KH \subseteq HK$. To show the reverse cntainment, let $hk \in HK$. As $HK \leq G$, we can write

$$hk = a^{-1}$$

for some $a \in HK$. Writing $a = h_1k_1$, we have that

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

as $k_1^{-1}, h_1^{-1} \in K, H$, respectively. □

<back2top>

23. Subgroups of cyclic groups need be cyclic

Let G be a cyclic group and let $H \leq G$ be a subgroup. Show that H is cyclic.

Proof. Suppose that $G = \langle g \rangle$. Then if $H \neq \{e\}$, then $g^n \in H$ for some $n \in \mathbb{Z}$, let $m \in \mathbb{Z}$ be the smallest integer such that

$$g^m \in H.$$

I claim that $H = \langle g^m \rangle = \langle h \rangle$. I e., every $a \in H$ can be written as a power of h. We know that

$$a = g^n$$

where we have that $n = mq + r$, by the division algorithm. Then

$$g^r = g^n (g^m)^{-q} \in H.$$

However as m was the minimum integer such that $g^m \in H$, this forces

$$n = qm.$$

Thus we can write

$$a = g^n = g^{qm} = (g^m)^q = h^q$$

and we have that a is a power of h as needed making H cyclic. □

<back2top>

24. Show $(\mathbb{Q}, +)$ is not finitely generated.

Show that $(\mathbb{Q}, +)$ is not finitely generated.

Proof. Suppose towards a contradiction that it is finitely generated. I.e., there exists a finite generating set, say

$$A = \langle \frac{p_1}{q_1}, ..., \frac{p_n}{q_n} \rangle$$

Then for each $1 \leq i \leq n$, one has that $\frac{p_i}{q_i}$ is an integer multiple of $\frac{1}{q_1 \cdot q_2 \cdot ... \cdot q_n}$. To see this we can write

$$\frac{p_i}{q_i} = p_i \cdot q_1 \cdot q_2 \cdot ... \cdot q_{i-1} \cdot q_{i+1} \cdot ... \cdot q_n (\frac{1}{q_1 \cdot ... \cdot q_n}).$$

Then $A \subset \langle \frac{1}{q_1 \cdot ... \cdot q_n} \rangle$ where $\langle \frac{1}{q_1 \cdot ... \cdot q_n} \rangle$ generates $(\mathbb{Q}, +)$ contradicting the fact that $\mathbb{Q}$ is non cyclic. □

<back2top>

25. Prime ideals in PIDs are maximal.

Let R be a PID. Let P be a prime ideal. Then P is maximal.

Proof. Let P be a prime ideal in a PID. Then as R is a PID, we can put

$$P = (p).$$

Suppose there exists an ideal $I \subset R$ such

$$(p) \subsetneq I \subsetneq R.$$

As I is an ideal in a PID, there exists some $m \in R$ such that

$$I = (m).$$

But $(p) \subset (m)$ implies there exists an $r \in R$ such that

$$p = rm \in (p).$$

As (p) is prime, either $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $I = (p)$. If $r \in (p)$, then there exists some $s \in R$ such that

$$r = sp.$$

But then

$$\begin{aligned} p &= rm \\ &= spm \end{aligned}$$

Thus $1 - sm = 0$ thus m a unit forcing $I = R$ hence there does not exists an ideal between (p) and R therefore (p) is maximal. □

<back2top>

26. Ideals in Euclidean domains are maximal.

Let R be a Euclidean domain. Any ideal in R is maximal.

Proof. Let R be a Euclidean domain. Let $d \in I$ have minimal norm. I claim $I = (d)$. For $\supset$ the case is trivial as $d \in I$. For $\subset$, let $a \in R \setminus \{0\}$ be arbitrary. As $a \neq 0$, there exists $q, r \in R$ such that

$$a = qd + r : \qquad \text{with } r = 0 \text{ or } N(r) < N(d).$$

I.e.,

$$r = a - qd \in I$$

by properties of ideals. However, by minimality of $N(d)$, this forces $r = 0$ thus

$$a = qd$$

which implies $a \in (d)$ thus $I = (d)$. □

<back2top>

27. Field iff only ideals are trivial and self.

R is a field if and only if only ideals are (0) and R itself.

Proof. First suppose R is a field. Let

$$(0) \neq I \subsetneq R.$$

Let $a \in I \setminus \{0\}$. Then $a \in R$ which is a field thus there exists an a^{-1} thus by properties of ideals, one has

$$1 = a^{-1}a \in I$$

thus I contains a unit and is thus all of R.
On the other hand, suppose that the only ideals are the trivial one and R itself and let $a \in R \setminus \{0\}$. Then consider the ideak generated by a, that is (a). As $a \neq 0$, and only ideals are trivial or entire ring it follows that

$$(a) = R.$$

Then there exists an $r \in R$ such that

$$ra = 1$$

forcing $r = a^{-1}$ thus R is a field. □

<back2top>

28. In integral domain prime implies irreducible.

Let R be an integral domain. If p is prime then p is irreducible. Put

$$p = ab.$$

I claim a or b a unit. As p is prime and

$$ab \in (p)$$

then by primality of (p) we have that $a \in (p)$ or $b(p)$. Without any loss of generality, suppose $a \in (p)$. Then there exists an $r \in R$ such that

$$a = rp.$$

But then

$$\begin{aligned} p &= ab \\ &= rpb. \end{aligned}$$

As R is an integral domain we have that $1 - rb = 0$ thus b is a unit forcing p to be irreducible.
<back2top>

29. In PID irreducible implies prime.

Let R be a PID and let p be irreducible, then p is prime.

Proof. Let R be a PID. Suppose p is irreducible. We show that (p) is maximal which implies it is prime. Suppose not, then there exists some ideal $I \subset R$ such

$$(p) \subsetneq I \subsetneq R.$$

As I is an ideal in a PID, there exists some $m \in R$ such that

$$I = (m).$$

But then $(p) \subset (m)$ which implies there exists some $r \in R$ such that

$$p = rm.$$

As p is irreducible, either r is a unit or m is a unit. If m is a unit then $I = R$, and if r is a unit then $I = (p)$ and thus (p) is maximal. □

<*back2top*>

30. In commutative ring with 1, P is prime iff R/P is an integral domain.

Proof. For the backwards direction, suppose P is not prime. Then there exists $a, b \in R$ such that $ab \in P$ but $a, b \notin P$. But then

$$\begin{aligned}(a+P)(b+P) &= ab + P \\ &= 0 + P \\ &\in R/P\end{aligned}$$

Thus R/P has zero divisors thus is not an integral domain.
For the forward direction, suppose R/P is an integral domain. Then there exists zero divisors $a + P, b + P \in R/P$. This implies $a, b \notin P$. But then

$$\begin{aligned}(a+P)(b+P) &= ab + P \\ &= 0 + P.\end{aligned}$$

Thus $ab \in P$ but $a, b \notin P$ thus P is not prime. □

<back2top>

In commutative ring with 1, every maximal ideal is principal

Let R be a commutative ring with 1. Then every maximal ideal is principal.

Proof. Let R be a commutative ring with 1. Let $M \subset R$ be a maximal ideal. Then by proposition stating M in R is maximal if and only if R/M is a field. Thus R/M is a field. Thus an integral domain. And in an integral domain, M is prime if and only if R/M is an integral domain and we are done. □

<back2top>