Abstract Algebra Select Solutions

MyMathYourMath.com
Solutions by: Sean Zhu & Hossien Sahebjame

2021

Contents

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. □