WAYNE STATE
UNIVERSITY

Algebra I
Winter 2020

Contents

1 Integers

1.1 Divisors

1. Let $m, n.r.s \in \mathbb{Z}$. If $m^2 + n^2 = r^2 + s^2 = mr + ns$, prove that $m = r$ and $n = s$.

Joe Starr

We select $m, n.r.s \in \mathbb{Z}$, given $m^2 + n^2 = r^2 + s^2 = mr + ns$ which can write as $m^2 + n^2 - mr - ns = r^2 + s^2 - mr - ns$. From here we can simplify:

$$\begin{aligned} m^2 + n^2 - mr - ns = r^2 + s^2 - mr - ns &\Rightarrow m(m-r) + n(n-s) = r(r-m) + s(s-n) \\ &\Rightarrow m(m-r) + n(n-s) - r(r-m) - s(s-n) = 0 \\ &\Rightarrow m(m-r) + r(m-r) + n(n-s) + s(n-s) = 0 \\ &\Rightarrow (m-r)(m+r) + (n-s)(n+s) = 0 \end{aligned}$$

from here we can see that in order for $(m-r)(m+r) + (n-s)(n+s) = 0$ to be true $m = r$ and $n = s$.

3. Find the quotient and reminder when a id divided by b.

a $a = 99$, $b = 17$

b $a = -99$, $b = 17$

c $a = 17$, $b = 99$

d $a = -1017$, $b = 99$

Joe Starr

a $99 = 17q + r \Rightarrow q = 5, r = 14$

b $-99 = 17q + r \Rightarrow q = -6, r = 3$

c $17 = 99q + r \Rightarrow q = 0, r = 17$

d $-1017 = 99q + r \Rightarrow q = -11, r = 72$

5. Use the Euclidean algorithm to find the following greatest common divisors

a $(6643, 2873)$

b $(7684, 4148)$

c $(26460, 12600)$

d $(6540, 1206)$

e $(12091, 8439)$

Joe Starr

(a) $(6643, 2873)$

$$
\begin{aligned}
6643 &= 2873 * 2 + 897 \\
2873 &= 897 * 3 + 182 \\
897 &= 182 * 4 + 169 \\
182 &= 169 * 1 + 13 \\
169 &= 13 * 13
\end{aligned}
$$

(b) $(7684, 4148)$

$$
\begin{aligned}
7684 &= 4148 * 1 + 3536 \\
4148 &= 3536 * 1 + 612 \\
3536 &= 612 * 5 + 476 \\
612 &= 476 * 1 + 136 \\
476 &= 136 * 3 + 68 \\
136 &= 68 * 68
\end{aligned}
$$

(c) $(26460, 12600)$

$$
\begin{aligned}
26460 &= 12600 * 2 + 1260 \\
12600 &= 1260 * 10
\end{aligned}
$$

(d) $(6540, 1206)$

$$
\begin{aligned}
6540 &= 1206 * 5 + 510 \\
1206 &= 510 * 2 + 186 \\
510 &= 186 * 2 + 138 \\
186 &= 138 * 1 + 48 \\
138 &= 48 * 2 + 42 \\
48 &= 42 * 1 + 6 \\
42 &= 6 * 7
\end{aligned}
$$

(e) $(12091, 8439)$

$$
\begin{aligned}
12091 &= 8439 * 1 + 3652 \\
8439 &= 3652 * 2 + 1135 \\
3652 &= 1135 * 3 + 247 \\
1135 &= 247 * 4 + 147 \\
247 &= 147 * 1 + 100 \\
147 &= 100 * 1 + 47 \\
100 &= 47 * 2 + 6 \\
47 &= 6 * 7 + 5 \\
6 &= 5 * 1 + 1 \\
5 &= 1 * 5
\end{aligned}
$$

7. For each part of Exercise 5, find integers m and n such that (a, b) is expressed in the form $ma + nb$.

Joe Starr

(a) $(6643, 2873)$
$(6643) - 16 + (2873)\,37 = 13$

(b) $(7684, 4148)$
$(7684)\,27 + (4148) - 50 = 68$

(c) $(26460, 12600)$ $(26460)\,1 + (12600) - 2 = 1260$

(d) $(6540, 1206)$ $(6540) - 26 + (1206)\,141 = 6$

(e) $(12091, 8439)$ $(12091)\,1435 + (8439) - 2056 = 1$

9. let a, b, c be integers such that $a + b + c = 0$. Show that if n is an integer which is a divisor of two of the three integers, then it is also a divisor of the third.

Joe Starr

Select $a, b, c \in \mathbb{Z}$ to satisfy $a + b + c = 0$, WLOG let $n \in \mathbb{Z}$ such that $n|a$ and $n|b$. Since $(a + b) + c = 0$ it must be that $(a + b) = -c$. From here we must show $n|(a + b)$, or $a + b = nq$. Since $n|a$ and $n|b$ we may write $a = nq_1$ and $b = nq_2$, yielding, $nq_1 + nq_2 = n(q_1 + q_2) = nq$ thus $n|c$, as desired.□

13. Show that if n is any integer, then $(10n_3, 5n + 2) = 1$

Joe Starr

We begin with the Euclidean algorithm,

$$10n + 3 = (5n + 2)\,1 + (5n + 1)$$
$$5n + 2 = (5n + 1)\,1 + 1$$

from here we have $(10n + 3, 5n + 2) = (5n + 2, 5n + 1) = 1$, as desired.

15. For what positive integers n is it true that $(n, n+2) = 2$? Prove your claim.

Joe Starr

The conjecture is that the statement is true for even values of n. We begin with rewriting n in terms of k, $n = 2k$the Euclidean algorithm,

$$\begin{aligned} (2k) + 2 &= (2k)\,1 + (2) \\ 2k &= (2)\,k \end{aligned}$$

from here we have $(n+2, n) = (2k+2, 2k) = 2$, as desired.

17. Show that the positive integer k is the difference of two odd squares if and only if k is divisible by 8.

Joe Starr

We begin by writing $k = a^2 - b^2$, since a and b are odd we can write,

$$a = 2r + 1$$
$$b = 2s + 1$$

from here we have $q^2 - b^2 = 4(r + s + 1)(r - s)$. Since $k > 0$ we must consider two cases $r - s = 2m + 1$ and $r - s = 2m$.

$r - s = 2m$:
In this case we have $q^2 - b^2 = 4(r + s + 1)\, 2m = 8(r + s + 1)\, m$ and we are done.

$r - s = 2m + 1$:
In this case we have $r - s = 2m + 1$ and $r + s = r - s + 2s = 2m + 1 + 2s$

$$\begin{aligned} q^2 - b^2 &= 4(r + s + 1)(2m + 1) \\ &= 4(2m(r + s + 1) + (r + s + 1)) \\ &= 4((2mr + 2ms + 2m) + (r + s + 1)) \\ &= 4(2mr + 2ms + 2m + r + s + 1) \\ &= 4(2mr + 2ms + 2m + 2m + 1 + 2s + 1) \\ &= 4(2mr + 2ms + 2m + 2m + 2s + 2) \\ &= 8(mr + ms + m + m + s + 1) \end{aligned}$$

as desired.

1.2 Primes

1. Find the prime factorizations of each of the following numbers, and use the them to compute the greatest common divisor and least common multiple of the given pairs of numbers.

(a) $(35, 14)$

(b) $(15, 11)$

(c) $(252, 11)$

(d) $(7684, 4148)$

(e) $(6643, 2873)$

Joe Starr

(a) $(35, 14)$
$35 : 5, 7$
$14 : 2, 7$
gcd: 7
lcm: 70

(b) $(15, 11)$
$15 : 3, 5$
$11 : 11$
gcd: 1
lcm: 165

(c) $(252, 180)$
$252 : 2, 2, 3, 3, 7$
$180 : 2, 2, 3, 3, 5$
gcd: 36
lcm: 1260

(d) $(7684, 4148)$
$7684 : 2, 2, 17, 113$
$4148 : 2, 2, 17, 61$
gcd: 68
lcm: 468724

(e) $(6643, 2873)$
$6643 : 7, 13, 73$
$2873 : 13, 13, 17$
gcd: 13
lcm: 1468103

2. US the sieve of Eratosthenes to find all prime numbers less than 200.

Joe Starr

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

3. For each composite number a. with $4 \leq a \leq 20$, find all positive numbers less than a that are relatively prime to a.

Joe Starr

$4:\ 2, 3$

$6:\ 2, 3, 5$

$8:\ 2, 3, 5, 7$

$9:\ 2, 3, 4, 5, 7, 8$

$10:\ 2, 3, 5, 7, 9$

$12:\ 2, 3, 5, 7, 11$

$14:\ 2, 3, 5, 7, 9, 11, 13$

$15:\ 2, 3, 4, 5, 7, 8, 11, 13, 14$

$16:\ 2, 3, 5, 7, 9, 11, 13, 15$

$18:\ 2, 3, 5, 7, 11, 13, 17$

$20:\ 2, 3, 5, 7, 9, 11, 13, 17, 19$

4. Find all positive integers less than 60 and relatively prime to 60.

Joe Starr

$60: \ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59$

9. (a) For which $n \in \mathbb{Z}^+$ is $n^3 - 1$ a prime number?

   (b) For which $n \in \mathbb{Z}^+$ is $n^3 + 1$ a prime number?

   (c) For which $n \in \mathbb{Z}^+$ is $n^2 - 1$ a prime number?

   (d) For which $n \in \mathbb{Z}^+$ is $n^2 + 1$ a prime number?

Joe Starr

(a) We can factor $n^3 - 1$ into $(n-1)(n^2+n+1)$. We have then $n-1|n^3-1$, for n^3-1 to be prime $n-1$ must be 1. This happens only for $n = 2$.

(b) We can factor $n^3 + 1$ into $(n+1)(n^2-n+1)$. We have then $(n^2-n+1)|n^3+1$, for n^3+1 to be prime (n^2-n+1) must be 1. This happens only for $n = 1$.

(c) We can factor $n^2 - 1$ into $(n-1)(n+1)$. We have then $(n11)|n^2-1$, for n^2-1 to be prime $(n-1)$ must be 1. This happens only for $n = 2$. For which $n \in \mathbb{Z}^+$ is $n^2 - 1$ a prime number?

(d) ????

11. Prove that $n^4 + 4^n$ is composite if $n > 1$.

Joe Starr

We are presented with two potability's, n is even or n is odd.

n even
It's obvious that $n^4 + 4^n$ is an even not 2 and can't be prime.

n odd
We begin by completing the square

$$\begin{aligned} n^4 + 4^n &= n^4 + 4^n \\ &= \left(n^2\right)^2 + \left(2^n\right)^2 \\ &= \left(n^2 + 2^n\right)^2 - 2n^2 2^n \end{aligned}$$

We from here we observe that $2^n 2 = 2^{n+1}$, since n is odd $n + 1$ is even yielding $2^{n+1} = 2^{2k}$. We can see we have a difference of squares

$$\begin{aligned} \left(n^2 + 2^n\right)^2 - 2n^2 2^n &= \left(n^2 + 2^n\right)^2 - \left(2^n n\right)^2 \\ &= \left(n^2 + 2^n + 2^n n\right)\left(n^2 + 2^n - 2^n n\right) \end{aligned}$$

since we are restricted to $n > 1$ we can see that both $(n^2 + 2^n + 2^n n) > 1$ and $(n^2 + 2^n - 2^n n) > 1$ for all n. Making $n^4 + 4^n$ composite as desired.

13. Let a, b, c be positive integers, and let $d = (a, b)$. Since $d|a$, there exists an integer h with $a = dh$. Show that $a|bc$, then $h|c$.

Joe Starr

We will proceed with a transitive proof:

$$\begin{aligned} a|abc &\to a|(a,b)\,c \\ &\to a|dc \\ &\to dh|dc \\ &\to h|c \end{aligned}$$

14. Show that $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]$.

Joe Starr

Let $x \in (a\mathbb{Z} \cap b\mathbb{Z})$, since $x \in a\mathbb{Z}$ we have $x = aq_1$, similarly since $x \in b\mathbb{Z}$ we have$x = bq_2$. We can see that $x = abq$, this means x is a multiple of $[a, b]$ putting $x \in [a, b]$. Next, we let $x \in [a, b]\,\mathbb{Z}$, this means x is of the form $x = [a, b]\,q$. We can see that $a|x$ and $b|x$ since $a|[a, b]$, This makes $x \in a\mathbb{Z}$ and $x \in b\mathbb{Z}$, as desired.

17. Let a, b be nonzero integers. Prove $(a, b) = 1$ if and only if $(a + b, ab) = 1$.

Joe Starr

$\Rightarrow$ We let $(a, b) = 1$, then consider the $(a + b, ab)$. We assume $(a + b, ab) = d$, with $d > 1$. Since $d > 1$ there must exist p a prime such that $p|d$. This means that $p|a + b$ and $p|ab$. Consequently, either $p|a$ or $p|b$. WOLG we have $p|a$, and since $p|a + b$ it must be that $p|b$. Finally, since $p|a$ and $p|b$, $p|(a, b)$ a contradiction. So $(a + b, ab) = 1$.

$\Leftarrow$ We let $(a + b, ab) = 1$, then consider the (a, b). We assume $(a, b) = d$, with $d > 1$. Since $d > 1$ there must exist p a prime such that $p|d$. This means that $p|a$ and $p|b$, further $p|ab$. Since p divides a and b, we have $p|a + b$. Finally, since $p|ab$, and $p|a + b$, $p|(a + b, ab)$, a contradiction so $(a, b) = 1$.

18. Let a, b be nonzero integers with $(a, b) = 1$. Compute $(a + b, a - b)$.

Joe Starr

We know that $d = (a + b, a - b)$, this means that $d|a+b$ and $d|a-b$. From here we have that $d|(a + b) + (a - b) \to d|2a$ and $d|(a + b) - (a - b) \to d|2b$. Since d divides both $2a$ and $2b$, d must also divide $2\,(a, b)$. Since $(a, b) = 1$ we have $(a + b, a - b) = 2$.

19. Let a and b be positive integers, and let m be an integer such that $ab = m\,(a, b)$. Without using the prime factorization theorem, prove that $(a, b)\,[a, b] = ab$ by verifying that m satisfies the necessary properties of $[a, b]$.

Joe Starr

We let $d = (a, b)$, this means that $ab = md$. We first show $a|m$ and $b|m$,

$$\begin{aligned} ab = md &\to a\,(dq) = md \\ &\to adq - md = 0 \\ &\to d(aq - m) = 0 \qquad\qquad (bydefd > 0) \\ &\to aq = m \\ &\to a|m \end{aligned}$$

similarly for b.
Next we will show that if $a|c$ and $b|c$ then $m|c$. We have that $c = aq_1 = bq_2$ or $c^2 = abq$. We can multiply $ab = md$ by q giving $abq = mdq$, this means we have $c^2 = mdq$, which is true only if $c = mdq$, $m|c$ as desired.

20. A positive integer a is called a square if $a = n^2$ for some $n \in \mathbb{Z}$. Show that the integer $a > 1$ is a square if and only if every exponent in its prime factorization is even.

Joe Starr

Let $a \in \mathbb{Z}$ be a square. Since a is a square by definiton there exists a n such that $nn = a$. Now by the fundamental theorem of arithmetic we know n has a prime factorization,written $p_1^{n_1} \cdots p_k^{n_k}$. If we consider nn, we have $nn = \left(p_1^{n_1} \cdots p_k^{n_k}\right)\left(p_1^{n_1} \cdots p_k^{n_k}\right)$, by combining terms we can see that $nn = \left(p_1^{2n_1} \cdots p_k^{2n_k}\right)$, as desired.

23. Let p and q be prime numbers. Prove that $pq + 1$ is a square if and only if p and q are twin primes.

Joe Starr

We begin by letting selecting p a prime and q a prime such that $q = p + 2$. Now we consider pq,

$$\begin{aligned} pq &\to p\,(p+2) \\ &\to p^2 + p2 \end{aligned}$$

We now consider $p + 1$, if we take $(p+1)^2$, we get $p^2 + 2p + 1$. It's obvious that $pq + 1 = p^2 + p2 + 1 = (p+1)^2$, so $pq + 1$ is a square when p and q are twin primes. We can now consider p a prime, and q a prime such that $q = p + n$ with $n > 2$. If we calculate pq we see that,

$$\begin{aligned} pq &\to p\,(p+n) \\ &\to p^2 + pn \end{aligned}$$

we then have that $pq + 1 = p^2 + pn + 1$ with $n > 2$, this is not a square, showing when p and q aren't twin primes $pq + 1$ is not a square.

26. Prove that if $a > 1$, then there is a prime p with $a < p \leq a! + 1$.

Joe Starr

We observe that $a! + 1$ is either prime or composite, if $a! + 1$ is prime we are done, if $a! + 1$ is composite we know by the fundamental theorem of arithmetic that $a! + 1$ has prime factors. Now if all prime factors p are such that $p \leq a$ since $p|a!$ we see that if we divide $a! + 1$ by any of these we get a remainder of 1, a contradiction so there must be a prime factor p with $a < p$.

Note: this is basically the same argument as euclid's proof of infinite primes

29. Show that $\log 2/\log 3$ is not a rational number.

Joe Starr

We observe this is an application of the change of base formula, making $\frac{\log 2}{\log 3} = \log_3 2$. From here we have $x = \log_3 2 \to 3^x = 2$, if x is rational then there exist m and n such that $\frac{m}{n} = x$. We now have $3^{\frac{m}{n}} = 2 \to 3^m = 2^n$, a contradiction since there is no m and n that satisfy this equivalence, making $\log 2/\log 3$ irrational as desired.

2 Functions

2.1 Functions

1. In each of the following parts, determine whether the given function is 1:1 and whether it is onto.

(a) $f : \mathbb{R} \to \mathbb{R}; f(x) = x + 3$

(b) $f : \mathbb{C} \to \mathbb{C}; f(x) = x^2 + 2x + 1$

(c $f : \mathbb{Z}_n \to \mathbb{Z}_n; f([x]_n) = [mx + b]_n$, where$m, b \in \mathbb{Z}$

(d) $f : \mathbb{R}^+ \to \mathbb{R}; f(x) = \ln x$

Joe Starr

(a) We can see that $f(x) = x + 3$ then $f^{-1}(x) = x - 3$, $f\left(f^{-1}(x)\right) = (x - 3) + 3 = x$. Showing f is a bijection.

(b) 1:1:

Assume $f(x) = 25 = f(y)$, we can see that if $x = 4$, $f(x) = 25$, and $y = -6$, $f(y) = 25$, showing f not injective.

onto:

Let $y \in \mathbb{C}$ we must now show there exists a $x \in \mathbb{C}$ such that $f(x) = y$. Consider $x = \sqrt{y} - 1$, we can then take:

$$\begin{aligned} f(x) &= x^2 + 2x + 1 \\ &= (\sqrt{y} - 1)^2 + 2(\sqrt{y} - 1) + 1 \\ &= (\sqrt{y} - 1)^2 + 2\sqrt{y} - 2 + 1 \\ &= 1 - 2\sqrt{y} + y + 2\sqrt{y} - 1 \\ &= y \end{aligned}$$

showing f surjective.

(c) Consider $f^{-1}(x) = [(y - b)m^{-1}]_n$, now taking $f\left(f^{-1}(x)\right)$

$$\begin{aligned} f\left(f^{-1}(x)\right) &= \left[m(x - b)m^{-1} + b\right]_n \\ &= [(x - b) + b]_n \\ &= [x]_n \end{aligned}$$

showing f a bijection.

(d) $f : \mathbb{R}^+ \to \mathbb{R}; f(x) = \ln x$ If we take $f^{-1}(x) = e^x$, $f\left(f^{-1}(x)\right) = \ln e^x = x$, showing f a bijection.

3. For each 1:1 and onto function in Exercise 1, find the inverse of the function

(a) $f : \mathbb{R} \to \mathbb{R}; f(x) = x + 3$

(b) $f : \mathbb{C} \to \mathbb{C}; f(x) = x^2 + 2x + 1$

(c $f : \mathbb{Z}_n \to \mathbb{Z}_n; f([x]_n) = [mx + b]_n$, where$m, b \in \mathbb{Z}$

(d) $f : \mathbb{R}^+ \to \mathbb{R}; f(x) = \ln x$

Joe Starr

(a) see question 1

(b) not a bijection

(c see question 1

(d) see question 1

4. For each 1:1 and onto function in Exercise 2, find the inverse of the function

(a) $f : \mathbb{R} \to \mathbb{R}; f(x) = x^2$

(b) $f : \mathbb{C} \to \mathbb{C}; f(x) = x^2$

(c $f : \mathbb{R}^+ \to \mathbb{R}^+; f(x) = x^2$

(d) $f : \mathbb{R}^+ \to \mathbb{R}^+; f(x) = \begin{cases} x & \text{if } x \text{ is rational} \\ x^2 & \text{if } x \text{ is irrational} \end{cases}$

Joe Starr

(a) Not a bijection

(b) Not a bijection

(c $f^{-1}(x) = +\sqrt{x}$

(d) $f : \mathbb{R}^+ \to \mathbb{R}^+; f^{-1}(x) = \begin{cases} x & \text{if } x \text{ is rational} \\ +\sqrt{x} & \text{if } x \text{ is irrational} \end{cases}$

13. Let $f : A \to B$ be a function, and let $f(A) = \{f(a) \,|a \in A\}$ be the image of f. Show that $f$is onto if and only if $f(A) = B$.

Joe Starr

Let $f(A) = B$, select $y \in B$, since $y \in B$ we have $y \in f(A)$, that means there exists $a \in A$ such that $f(a) = y$. Showing f surjective. Let $f(A) \neq B$, let $y \in B$, such that $y \notin B \cap f(A)$. Since we have $y \notin f(A)$ we have no $a \in A$ that maps to y showing f not surjective, as desired.

15. Let $f : A \to B$ and $g : B \to C$ be functions. Prove that if $g \circ f$ is 1:1, then f is 1:1, and that if $g \circ f$ is onto g is onto.

Joe Starr

Let $g \circ f$ be injective, but f not injective. Since f is not injective $\exists a, x \in A$ such tha $a \neq x$ but $f(x) = f(a)$. We consider $g \circ f(a)$ and $g \circ f(x)$, since $f(x) = f(a)$ it must be that $g(f(x)) = g(f(a))$. This means that with $a \neq b$, $g(f(x)) = g(f(a))$, making $g \circ f$ not injective a contradiction so f injective.

Let $g \circ f$ be surjective, but g not surjective. Since g not surjective there exists some $c \in C$ such that $g(b) \neq c$ for all $b \in B$. However since $g \circ f$ surjective there exists $g \circ f(a) = c$ a contradiction, making g surjective.

17. Let $f : A \to B$ be a function. Prove that f is onto if and only if $h \circ f = k \circ f$ implies $h = k$, for every set C and all choices of functions $h : B \to C$ and $k : B \to C$.

Joe Starr

Assume f is surjective, that is for all $y \in B$ there exists $x \in A$ such that $f(x) = y$. We know $h(f(x)) = k(f(x))$, so $h(y) = k(y)$ for all y in the domain of f as desired.

Next assume f is not surjective, then for some $y \in B$ there exists no x such that $f(x) = y$. We can select $C = \{a, b\}$. We say that $h(c) = a$ now we construct k,

$$k(x) = \begin{cases} b & \text{if } x = y \\ a & \text{if } x \neq y \end{cases}$$

from here we have that when the input of h and k are in the domain of f $h \neq k$, as desired.

19. Let $f : A \to B$ be a function. Prove that f is 1:1 if and only if $f \circ h = f \circ k$ implies $h = k$, for every set C and all choices of functions $h : C \to A$ and $k : C \to A$.

Joe Starr

Assume that f is injective, this means that $f(x) = f(y)$ implies $x = y$. Also assume $f \circ h = f \circ k$ for some h, k. We assume $h \neq k$ for some $c \in C$. Since we know f is injective we have $f(h(c)) \neq f(k(c))$, a contradiction from our assumption that $f \circ h = f \circ k$ meaning $h = k$ as desired.

Assume $f \circ h = f \circ k$ implies $h = k$. suppose f be not injective, this means that there exists some x, y such that $f(x) = f(y)$ but $x \neq y$. We can select $C = \{a, b\}$, and define h, k:

$$k(a) = x \qquad h(a) = y$$
$$k(b) = y \qquad h(b) = x$$

We can see from here we have that for $f(h(a)) = f(k(a))$ but $h \neq k$ a contradiction making f injective as desired.

2.2 Equivalence Relations

2.3 Permutations

1. Consider the following Permutations in S_7.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix}$$

(a) $\sigma\tau$

(b) $\tau\sigma$

(c) $\tau^2\sigma$

(d) σ^{-1}

(e) $\sigma\tau\sigma^{-1}$

(f) $\tau^{-1}\sigma\tau$

Joe Starr

(a) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 7 & 4 & 1 & 5 \end{pmatrix}$

(b) $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 4 & 7 & 6 & 2 & 3 \end{pmatrix}$

(c) $\tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 3 & 6 & 1 & 5 \end{pmatrix}$

(d) $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 4 & 3 & 5 & 7 \end{pmatrix}$

(e) $\sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 7 & 6 & 4 & 5 \end{pmatrix}$

(f) $\tau^{-1}\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix}$

2. Write each of the permutations $\sigma\tau, \tau\sigma, \tau^2\sigma, \sigma^{-1}, \sigma\tau\sigma^{-1},$ and $\tau^{-1}\sigma\tau$ in Exercise 1 as a product of disjoint cycles. Write σ and τ as products of transpositions.

Joe Starr

(a) $\sigma\tau = (1236)\,(475)$

(b) $\tau\sigma = (1562)\,(347)$

(c) $\tau^2\sigma = (143756)$

(d) $\sigma^{-1} = (1653)$

(e) $\sigma\tau\sigma^{-1} = (23)\,(4756)$

(f) $\tau^{-1}\sigma\tau = (1356)$

(σ) $\sigma = (13)\,(35)\,(56)$

(τ) $\tau = (12)\,(35)\,(54)\,(47)\,(73)$

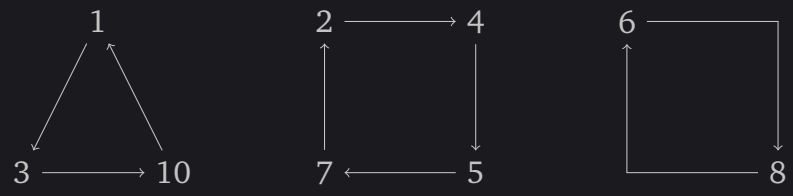
3. Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 10 & 5 & 7 & 8 & 2 & 6 & 9 & 1 \end{pmatrix}$ as the product of disjoint cycles and as a product of transpositions. Construct its associated diagram, find its inverse, and find it's order.

Joe Starr

Disjoint cycles:
$(1, 3, 10)\,(2, 4, 5, 7)\,(6, 8)$

Transpositions:
$(1, 3)\,(3, 10)\,(2, 4)\,(4, 5)\,(5, 7)\,(6, 8)$

Diagrams:



Inverse:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 1 & 2 & 4 & 8 & 5 & 6 & 9 & 3 \end{pmatrix}$$

Order:
$(1, 3, 10) = 3, (2, 4, 5, 7) = 4\,(6, 8) = 2$ order is 12

4. Find the oder of each of the following permutations.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 2 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 5 & 1 & 8 & 2 & 3 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 7 & 3 & 4 & 6 & 1 & 2 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 4 & 9 & 6 & 5 & 2 & 3 & 1 & 7 \end{pmatrix}$

Joe Starr

(a) $(1, 6)\,(2, 4, 2, 5)$ order is 4

(b) $(1, 4, 5)\,(2, 6, 8, 3, 7)$ order 15

(c) $(1, 5, 3, 8)\,(2, 9)\,(4, 7, 6)$ order 12

(d) $(1, 8)\,(2, 4, 6)\,(3, 9, 7)$ order 6

5. Let $3 \leq m \leq n$. Calculate $\sigma\tau^{-1}$ for cycles $\sigma = (1, 2, \ldots, m-1)$ and $\tau = (1, 2, \ldots, m-1, m)$ in S_n.

Joe Starr

We begin with finding τ^{-1}. We take τ of, $[1, 2, \ldots, m-1, m]$, we get $[2, 3, \ldots, m, 1]$. If we now apply $\tau^{-1} = (m, 1, 2, \ldots, m-1)$, we get $[1, 2, \ldots, m-1, m]$.

We can now compose τ^{-1} and σ yielding $(m, m-1, 1, 2, \ldots, m-3, m-2)$.

3 Groups

3.1 Definition of a Group

1. Using ordinary addition of integers as the operation, show that the set of even integers is a group but the set of odd integers is not.

Joe Starr

We begin considering the even integers, that is integers of the form $2k$. We must also include 0 in the even integers. We get the identity element as well as Associativity and inverses for free from integer addition on $\mathbb{Z}$. We then consider closure. Let n and m be even integers, if we take $m+n$ we can see we have, $m+n = 2k_m + 2k_n = 2(k_m + k_n)$ an even integer. Making the even integers a group under addition.

Next we consider the odd integers, take $3+3 = 2(3)$ an even integer, showing odds are not closed under addition and not a group.

2. For each binary operation $*$ defined on a set below, determine whether or not $*$ gives a group structure on the set. If it is not a group, say which axioms fail to hold.

(a) Define $*$ on $\mathbb{Z}$ by $a * b = ab$.

(b) Define $*$ on $\mathbb{Z}$ by $a * b = \max a, b$.

(c) Define $*$ on $\mathbb{Z}$ by $a * b = a - b$.

(d) Define $*$ on $\mathbb{Z}$ by $a * b = |ab|$.

(e) Define $*$ on $\mathbb{R}^+$ by $a * b = ab$.

(f) Define $*$ on $\mathbb{Q}$ by $a * b = ab$.

Joe Starr

(a) Inverses: Let $a \in \mathbb{Z}$ but $a \neq 1$ and $a \neq 1$, $a^{-1} \notin \mathbb{Z}$.

(b) Identity: $\max a, a - 1 = a$ for all $a \in \mathbb{Z}$ this means there is no e with $\max a, e = a$ for all a.

(c) Associativity:

$$\begin{aligned}(a * b) * c &= (a - b) * c \\ &= (a - b) - c \\ &= a - (b - c) \\ &= a * (b * c)\end{aligned}$$

Inverses: Select $a \in \mathbb{Z}$,

$$a * a = a - a = 0$$

Closure: Obvious from closure of $(\mathbb{Z}, +)$

Identity: 0 is the identity, Obvious from $(\mathbb{Z}, +)$

(d) Inverses: Let $a \in \mathbb{Z}$ but $a \neq 1$ and $a \neq 1$, $a^{-1} \notin \mathbb{Z}$.

(e) Associativity:

$$\begin{aligned}(a * b) * c &= (ab) * c \\ &= (ab)\, c \\ &= a\,(bc) \\ &= a * (b * c)\end{aligned}$$

Inverses: Select $a \in \mathbb{R}$,

$$a * a = a\frac{1}{a} = 1$$

Closure: Obvious from closure of $(\mathbb{R}, \cdot)$

Identity: 1 is the identity, Obvious from $(\mathbb{R}, \cdot)$

(f) Associativity:

$$\begin{aligned}(a * b) * c &= (ab) * c \\ &= (ab)\, c \\ &= a\,(bc) \\ &= a * (b * c)\end{aligned}$$

Inverses: Select $a \in \mathbb{Q}$,

$$a * a^{-1} = a\frac{1}{a} = 1$$

Closure: $a, b \in \mathbb{Q}$, $a = \frac{p_1}{q_1}$ $b = \frac{p_2}{q_2}$, $p_1, q_1, p_2, q_2 \in \mathbb{Z}$, $q_1 \neq 0 \neq q_2$.

$$\begin{aligned}a * b = ab \qquad\qquad &= \\ = \frac{p_1 p_2}{q_1 q_2} &\in \mathbb{Q}\end{aligned}$$

Identity: 1 is the identity, Obvious from $(\mathbb{R}, \cdot)$

3. Let $(G\,,\,\cdot)$ be a group. Define a new binary operation $*$ on G by the formula $a * b = b \cot a$, for all $a, b \in G$.

(a) Show that $(G\,,\,\cdot)$ is a group.

(b) Give examples to show that $(G\,,\,\cdot)$ may or may not be the same as $(G\,,\,*)$.

Joe Starr

(a) Associativity:

$$\begin{aligned}(a * b) * c &= (b \cdot a) * c \\ &= c \cdot (b \cdot a) \\ &= (c \cdot b) \cdot a \\ &= (b * c) \cdot a \\ &= a * (b * c)\end{aligned}$$

Inverses: Let $a \in G$ since $(G\,,\,\cdot)$ is a group we know $a^{-1} \in G$. Now $a * a^{-1} = a^{-1} \cdot a = 1$.

Closure: We select $a, b \in G$ consier $a * b = b \cdot a$ by closure of $(G\,,\,\cdot)$, $a * b \in G$.

Identity: Let $a \in G$, consider $1 * a = a \cdot 1 = a$ and $a * 1 = 1 \cdot a = a$.

(b) Let $G =$

·	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

so $a * b = b \cdot a = f$ but $a \cdot b = d$. In this case they are not equal.

If we let $G = (\mathbb{Z}\,,\,+)$, we have $a * b = b + a = a + b$. In this case they are equal.

5. Is $\mathrm{GL}_n(\mathbb{R})$ an Abelian group? Support your answer by either proof or a counter example.

Joe Starr

No, select

$$A = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} B = \begin{bmatrix} 11 & 13 \\ 17 & 19 \end{bmatrix}$$

we calculate

$$AB = \begin{bmatrix} 73 & 83 \\ 174 & 198 \end{bmatrix} BA = \begin{bmatrix} 87 & 124 \\ 129 & 184 \end{bmatrix}$$

8. Write out the multiplication table for the following set of matrices over $\mathbb{Q}$:

$$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}\text{-}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & \text{-}1\end{bmatrix}, \begin{bmatrix}\text{-}1 & 0\\0 & \text{-}1\end{bmatrix}$$

Joe Starr

Let

$$i = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, j = \begin{bmatrix}\text{-}1 & 0\\0 & 1\end{bmatrix}, k = \begin{bmatrix}1 & 0\\0 & \text{-}1\end{bmatrix}, l = \begin{bmatrix}\text{-}1 & 0\\0 & \text{-}1\end{bmatrix}$$

·	i	j	k	l
i	i	j	k	l
j	j	i	l	k
k	k	l	i	j
l	l	k	j	i

9. Let $G = \{x \in \mathbb{R} | x > 0 extand x \neq 1\}$. Define the operation $*$ on G by $a * b = a^{\ln b}$, for all $a, b \in G$. Prove that G is an Abelian group under the operation $*$.

Joe Starr

Associativity:

$$\begin{aligned}(a * b) * c &= \left(a^{\ln b}\right) * c \\ &= \left(a^{\ln b}\right)^{\ln c} \\ &= a^{\ln b \ln c} \\ &= a^{\ln b^{\ln c}} \\ &= a * (b * c)\end{aligned}$$

Inverses: Let $a \in G$, consider $a^{-1} = e^{\frac{1}{\ln a}}$.

$$\begin{aligned}a * a^{-1} &= a^{\ln a^{-1}} \\ &= a^{\ln e^{\frac{1}{\ln a}}} \\ &= a^{\frac{1}{\ln a}} \\ &= a^{\log_a e} \\ &= e\end{aligned}$$

$$\begin{aligned}a^{-1} * a &= \left(a^{-1}\right)^{\ln a} \\ &= \left(e^{\frac{1}{\ln a}}\right)^{\ln a} \\ &= \left(e^{\log_a e}\right)^{\ln a} \\ &= \left(e^{\ln a}\right)^{\log_a e} \\ &= a^{\log_a e} \\ &= e\end{aligned}$$

Closure: Let $a, b \in G$, $a * b = a^{\ln b}$ we know that $b > 0$ so $\ln b$ exists, further since $1 \notin G$ we have $\ln b \neq 0$. We observe that for any $a \in G$ $a^{\ln b} > 0$ since $a > 0$ and since $\ln b \neq 0$ $a^{\ln b} \neq 1$.

Identity: Our conjecture is that e is the identity element. Let $a \in G$, $e * a = e^{\ln a} = a$ and $a * e = a^{\ln e} = a$

10. Show that the set $A = \{f_{m,b} : \mathbb{R}o\mathbb{R} | m \neq 0extandf_{m,b} = mx + b\}$. of affine functions from $\mathbb{R}$ to $\mathbb{R}$ forms a group under function composition.

Joe Starr

Associativity: We've proved this previously.

Inverses: Let $f \in A$, $f(x) = mx + b$. Consider $I(x) = \frac{1}{m}(x - b)$

$$f(I(x)) = m\left(\frac{1}{m}(x-b)\right) + b = x - b + b = x$$

$$I(f(x)) = \frac{1}{m}((mx+b) - b) = \frac{1}{m}(mx) = x$$

Closure: Let $f, g \in A$, so $f(x) = m_1x + b_1$ and $g(x) = m_2x + b_2$. Now composing f and g $f(g(x))$.

$$\begin{aligned} f(g(x)) &= m_1(m_2x + b_2) + b_1 \\ &= m_1m_2x + m_1b_2 + b_1 \\ &= mx + m_1b_2 + b_1 \\ &= mx + b \end{aligned}$$

Identity: Let $f \in A$, $f(x) = mx + b$. Conjecture $e(x) = x$

$$f(e(x)) = m(x) + b = mx + b$$

$$e(f(x)) = mx + b$$

11. Show that the set of all $2imes2$ matrices over $\mathbb{R}$ of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ with $m \neq 0$ forms a group under matrix multiplication.

Joe Starr

Let G be the set of all $2imes2$ matrices over $\mathbb{R}$ of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ with $m \neq 0$.

Associativity: Free from $M_2(\mathbb{R})$

Inverses: Let $a \in G$, so $a = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ we can calculate the determinate of a. $m1 - b0 = m$ and by definition of the set $m \neq 0$. So we have inverses.

Closure: Let $a, b \in G$, so $a = \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix}$

$$\begin{aligned} ab &= \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} m_2 m_1 & b_1 + m_1 b_2 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Identity: Free from $M_2(\mathbb{R})$

12. In the group defined in question 11 find all elements that commute with $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$

Joe Starr

We can begin by letting $a \in G$ calculating $a \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} a$.

$$a \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2m & b \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} a = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2m & 2b \\ 0 & 1 \end{bmatrix}$$

So for a matrix of to commute with $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ it must be of the form $\begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix}$.

13. Define $*$ on $\mathbb{R}$ by $a * b = a + b - 1$, for all $a, b \in \mathbb{R}$. Show that $(\mathbb{R}, *)$ is an Abelian group.

Joe Starr

Abelian:

$$\begin{aligned} a * b &= a + b - 1 \\ &= b + a - 1 \\ &= b * a \end{aligned}$$

Associativity:

$$\begin{aligned} (a * b) * c &= (a + b - 1) * c \\ &= (a + b - 1) + c - 1 \\ &= a + b + c - 1 - 1 \\ &= a + (b + c - 1) - 1 \\ &= a * (b * c) \end{aligned}$$

Inverses: Let $a \in (\mathbb{R}, *)$, consider $a^{-1} = 2 - a$

$$\begin{aligned} a * a^{-1} &= a + (2 - a) - 1 \\ &= 1 \end{aligned}$$

$$\begin{aligned} a^{-1} * a &= (2 - a) + a - 1 \\ &= 1 \end{aligned}$$

Closure: Obvious from closure of $(\mathbb{R}, +)$.

Identity: Conjecture is that 1 is the identity element of $(\mathbb{R}, *)$.

$$\begin{aligned} a * 1 &= a + 1 - 1 \\ &= a \end{aligned}$$

$$\begin{aligned} 1 * a &= a + 1 - 1 \\ &= a \end{aligned}$$

Joe Starr

Let $\varphi : (\mathbb{R}, *)\, o\, (\mathbb{R}, +)$, with $\phi(x) = x - 1$, $\phi(a * b) = (a + b - 1) - 1 = a - 1 + b - 1 = \phi(a) + \phi(b)$. Further $\varphi^{-1}(x) = x + 1$, $\phi\left(\varphi^{-1}(x)\right) = (x + 1) - 1 = x$. Showing a group structure isomorphic to $(\mathbb{R}, +)$.

14. Let $S = \mathbb{R} - \{\text{-}1\}$. Define $*$ on S by $a * b = a + b + ab$ for all $a, b \in S$. Show that $(S\,,\,*)$ is an Abelian group.

Joe Starr

Abelian:

$$\begin{aligned} a * b &= a + b + ab \\ &= b + a + ba \\ &= b * a \end{aligned}$$

Inverses: Consider $a^{\text{-}1} = \frac{\text{-}a}{a+1}$

$$\begin{aligned} a * a^{\text{-}1} &= a + \frac{\text{-}a}{a+1} + a\frac{\text{-}a}{a+1} \\ &= a + \frac{\text{-}a\,(a+1)}{a+1} \\ &= a + \text{-}a \\ &= 0 \end{aligned}$$

Closure: Let $a, b \in \mathbb{R}$, if we take $a * b = a + b + ab$. Assume that $a * b = \text{-}1$

$$\begin{aligned} \text{-}1 = a + b + ab &\Rightarrow \text{-}1 - a = b + ab \\ &\Rightarrow \text{-}1 - a = b\,(1 + a) \\ &\Rightarrow \text{-}\frac{a+1}{1+a} = b \\ &\Rightarrow \text{-}1 = b \end{aligned}$$

a contradiction.

Identity: Conjecture is that 0 is the identity element of $(S\,,\,*)$.

$$\begin{aligned} a * 0 &= a + 0 + a0 \\ &= a \end{aligned}$$

Associativity:

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= a + b + ab + c + ca + cb + cab \\ &= a + (b + c + bc) + a\,(b + c + bc) \\ &= a * (b + c + bc) \\ &= a * (b * c) \end{aligned}$$

15. Let $G = \{x \in \mathbb{R} | x > 1\}$. Define $*$ on G by $a * b = ab - a - b + 2$, for all $a, b \in G$. Show that $(G\,,\,*)$ is an Abelian group.

Joe Starr

Abelian:

$$\begin{aligned} a * b &= ab - a - b + 2 \\ &= ba - b - a + 2 \\ &= b * a \end{aligned}$$

Inverses: Consider $a^{-1} = \frac{a}{a-1}$

$$\begin{aligned} a * a^{-1} &= a\frac{a}{a-1} - a - \frac{a}{a-1} + 2 \\ &= \frac{a}{a-1}(a-1) - a + 2 \\ &= a - a + 2 \\ &= 2 \end{aligned}$$

Identity: Conjecture is that 2 is the identity element of $(G\,,\,*)$.

$$\begin{aligned} a * 2 &= a2 - a - 2 + 2 \\ &= a \end{aligned}$$

Closure: We begin by letting $a, b \in G$, we observe $a \geq b > 1$. We can then multiply through by b yeilding $ab \geq bb > b > 1$. Next we subtract both a and b, $ab - a - b \geq 1 > -a$, finaly adding two gives $ab - a - b + 2 \geq 3$ showing $a * b \in G$.

Associativity:

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)\, c \\ &= (a + b + ab) + c + (a + b + ab)\, c \\ &= (a + b + ab) + c + (a + b + ab)\, c \\ &= a + b + ab + c + ca + cb + cab \\ &= a + (b + c + bc) + a\,(b + c + bc) \\ &= a * (b + c + bc) \\ &= a * (b * c) \end{aligned}$$

16. Let G be a group. We have shown that $(ab)^{-1} = b^{-1}a^{-1}$. Find a similar expression for $\left(abc^{-1}\right)$

Joe Starr

We will use a transitive proof:

$$\begin{aligned}(abc)^{-1} &= c^{-1}(ab)^{-1} \\ &= c^{-1}b^{-1}a^{-1}\end{aligned}$$

17. Let G be a group. If $g \in G$ and $g^2 = g$,then prove that $g = e$.

Joe Starr

We begin with letting $g \in G$, such $g^2 = g$ we then multiply by g^{-1} on the left:

$$g^2 = g \to g^{-1}g^2 = g^{-1}g$$
$$\to g = e$$

as desired.

18. Show that a nonabelian group must have at least 5 elements.

Joe Starr

Let G be a nonabelian group. Since G a group then $e \in G$ the identity. G can't be the trivial group since the trivial group is Abelian, this puts $a \in G$ with $a \neq e$ further $a^{-1} \in G$. With the same argument G is not a group of three elements, so $b, b^{-1} \in G$. This puts $a, b, b^{-1}, a^{-1}, e \in G$ showing G with at lest 5 elements.

22. Let S be a nonempty finite set with a binary operation $*$ that satisfies the associative law. Show that S is a group if $a * b = a * c$ implies $b = c$ and $a * c = b * c$ implies $a = b$ for all $a, b, c \in S$. What can we say if S is infinite?

Joe Starr

24. Let G be a group. Prove that G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Joe Starr

wocase Let G be an abelian group and $a, b \in G$. Consider $(ab)^{-1}$, we have shown $(ab)^{-1} = b^{-1}a^{-1}$ since G is abelian we have $(ab)^{-1} = a^{-1}b^{-1}$. Let $(ab)^{-1} = a^{-1}b^{-1}$, we have shown $(ab)^{-1} = b^{-1}a^{-1}$ so $b^{-1}a^{-1} = a^{-1}b^{-1}$ showing G abelian.

25. Let G be a group. Prove that if $x^2 = e$ for all $x \in G$, then G is abelian.

Joe Starr

Let G be a group with the given property $a, b \in G$. Observe that $a^2 = e \Rightarrow a = a^{-1}$. We have shown that $(ab)^{-1} = b^{-1}a^{-1}$. We proceed with a transitive proof:

$$\begin{aligned}(ab)^{-1} = b^{-1}a^{-1} &\rightarrow (ab) = b^{-1}a^{-1} \\ &\rightarrow (ab) = ba\end{aligned}$$

showing G abelian as desired.

26. Show that if G is a finite group with an even number of elements, then there must exist an element $a \in G$ with $a \neq e$ such that $a^2 = e$.

Joe Starr

Let G be a group with the given property. Since G a group $e \in G$. Observe G is not the trivial group since it has even cardinality. If we consider the cardinality of G/e it's $|G| - 1$ an odd number. Let $a \in G$ with $a \neq e$, observe that since G a group $a^{-1} \in G$. We are left with two possibilities $a = a^{-1}$ or $a \neq a^{-1}$. If $a = a^{-1}$ we are done, otherwise we can delete a and a^{-1} from G and select from the remaining elements of G. Since G/e has odd cardinality we can repeat this process until there is a single element remaining. It must be that $a = a^{-1}$ as desired.

3.2 Subgroups

1. In $\mathrm{GL}_2(\mathbf{R})$, find the order of each of the following elements.

(a)† $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$ | (b) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ | †(c) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ | (d) $\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$

Joe Starr

(a)

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(b)

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(c)

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

Infinite order.

(d)

$$\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2. Let $A = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix} \in \mathrm{GL}_2(\mathrm{R})$. Show that A has infinite order by proving that $A^n = \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix}$, for $n \geq 1$, where $F_0 = 0, F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ is the Fibonacci sequence.

Joe Starr

We will proceed with induction:

Base Case: Consider 1 for the basecase. $\begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$ showing the base case to be true.

Inductive Case: Assume that it's ture for the nth power we will show this implies the $n+1$th case to be true.

$$A^{n+1} = A^n A^1 = \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} F_{n+2} & -F_{n+1} \\ -F_{n+1} & F_n \end{bmatrix}$$

showing the Inductive case to be true, and A of infinite order.

3. Prove that the set of all rational numbers of the form m/n, where $m, n \in \mathbf{Z}$ and n is square-free, is a subgroup of Q (under addition).

Joe Starr

Inverses: Let $m, n \in \mathbb{Z}$ with the given properties. Take $\frac{-m}{n}$ and consider $\frac{m}{n} + \frac{-m}{n} = \frac{m-m}{n} = 0$ as desired.

Closure: Let $m, n, a, b \in \mathbb{Z}$ with the given properties. Take $\frac{m}{n} + \frac{a}{b} = \frac{mb+an}{bn}$, since b and n are square free bn is also square free.

4. Show that $\{ (1),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3) \}$ is a subgroup of S_4

Joe Starr

We begin by labeling each permutation

$$A = (1,2)(3,4) =$$

$$B = (1,3)(2,4)$$

$$C = (1,4)(2,3)$$

Inverses:

$$AA = (1,2)(3,4)(1,2)(3,4) = (1)$$

$$BB = (1,3)(2,4)(1,3)(2,4) = (1)$$

$$CC = (1,4)(2,3)(1,4)(2,3) = (1)$$

Closure:

$$AB = (1,4)(2,3)$$

$$BA = (1,4)(2,3)$$

$$AC = (1,3)(2,4)$$

$$CA = (1,3)(2,4)$$

$$CB = (1,2)(3,4)$$

$$BC = (1,2)(3,4)$$

(a) Show that $T = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} | ad \neq 0 \right\}$ is a subgroup of G.

(b) Show that $D = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} | ad \neq 0 \right\}$ is a subgroup of G.

Joe Starr

(a) Inverses: We know by construction of G there exist an inverse of the form $\begin{bmatrix} \frac{1}{a} & 0 \\ \frac{-c}{ad} & \frac{1}{d} \end{bmatrix}$, by taking $\frac{1}{a}\frac{1}{d}$ that this is not 0 so the inverse is in T.

Closure: If we take $A, B \in T$

$$AB = \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \begin{bmatrix} w & 0 \\ y & z \end{bmatrix} = \begin{bmatrix} aw & 0 \\ cw + dy & zd \end{bmatrix}$$

since both $ad \neq 0$ and $wz \neq 0$ it holds $adwz \neq 0$.

(b) Inverses: We know by construction of G there exist an inverse of the form $\begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{d} \end{bmatrix}$, by taking $\frac{1}{a}\frac{1}{d}$ that this is not 0 so the inverse is in T.

Closure: If we take $A, B \in T$

$$AB = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} w & 0 \\ 0 & z \end{bmatrix} = \begin{bmatrix} aw & 0 \\ 0 & zd \end{bmatrix}$$

since both $ad \neq 0$ and $wz \neq 0$ it holds $adwz \neq 0$.

7. Let $G = \mathrm{GL}_2(\mathrm{R})$. Show that the subset S of G defined by $S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | b = c \right\}$ of symmetric 2×2 matrices does not form a subgroup of G.

Joe Starr

Consider

$$\begin{bmatrix} 1 & 3 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 10 & 6 \\ 18 & 14 \end{bmatrix}$$

showing this set is not closed.

8. Let $G = \mathrm{GL}_2(\mathrm{R})$. For each of the following subsets of $M_2(\mathbf{R})$, determine whether or not the subset is a subgroup of G.

(a) $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} | ab \neq 0 \right\}$

(b) $B = \left\{ \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} | bc \neq 0 \right\}$

(c) $C = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} | c \neq 0 \right\}$

Joe Starr

(a) This set doesn't contain the identity so can not be a subgroup

(b) This set doesn't contain the identity so can not be a subgroup

(c) Inverses: Let $\begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}$ with the given properties. We consider the inverse of $\begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}$ which is $\begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{c} \end{bmatrix}$ which is in C;

Closure: Let $\begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}$ and Let $\begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$ with the given properties. Consider

$$\begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & ca \end{bmatrix}$$

We observe that $a \neq 0$ and $c \neq 0$, consequently $ac \neq 0$.

9. Let $G = \mathrm{GL}_3(\mathbf{R})$. Show that $H = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \right\}$ is a subgroup of G.

Joe Starr

Inverses: Let $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}$ with the given properties. We consider the inverse of $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}$ which is $\begin{bmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ ac-b & -c & 1 \end{bmatrix}$ which is in H;

Closure: Let $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}$ and Let $\begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & z & 1 \end{bmatrix}$ with the given properties. Consider

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & z & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ a+x & 1 & 0 \\ b+cx+y & c+z & 1 \end{bmatrix}$$

10. Let m and n be nonzero integers, with $(\, m, n \,) = d$. Show that m and n belong to $d\mathbf{Z}$, and that if H is any subgroup of $\mathbf{Z}$ that contains both m and n, then $d\mathbf{Z} \subseteq H$

Joe Starr

We will first show that m and n are in $d\mathbb{Z}$. Let $m, n \in \mathbb{Z}$ with the given properties. Since $\gcd(m, n) = d$ we observe that $dq_1 = m$ and $dq_2 = n$ making $m, n \in d\mathbb{Z}$ as desired.

Next let H be a subgroup of $\mathbb{Z}$ with $m, n \in H$. Let $a \in d\mathbb{Z}$, with $a < m \leq n$ by construction we have $a = dq$ for some q.

11. Let S be a set, and let a be a fixed element of S. Show that $\{\sigma \in \mathrm{Sym}(S) | \sigma(a) = a\}$ is a subgroup of $\mathrm{Sym}(S)$

Joe Starr

Let $A = \{\sigma \in \mathrm{Sym}(S) | \sigma(a) = a\}$

Inverses: By proposition 2.1.7 in the text we have inverses.

Closure: Let $\sigma, \varphi \in A$, consider the composition of these two functions around a, $\phi(\sigma(a)) = \phi(a) = a$ showing closure, as desired.

12. For each of the following groups, find all elements of finite order.

(a) $\mathbf{R}^\times$

(b) $\mathbf{C}^\times$

Joe Starr

(a) 1 and -1 are the only elements of finite order. d

(b) $1, -1, -i$, and i are the only elements of finite order.

13. Let G be an abelian group, such that the operation on G is denoted additively. Show that $\{a \in G | 2a = 0\}$ is a subgroup of G. Compute this subgroup for $G = \mathbf{Z}_{12}$

Joe Starr

Let $S = \{a \in G | 2a = 0\}$

Inverses: Let $a \in S$, by transitive proof $2a = 0 \to a + a = 0 \to a = -a$

Closure: Let $a, b \in S$, by transitive proof,

$$\begin{aligned} 2a = 0 &\to 2a + 2b = 0 + 0 \\ &\to 2(a + b) = 0 \end{aligned}$$

showing closure of S.

next we let $G = \mathbb{Z}_{12}$ we can calculate $a + a$ for all $a \in \mathbb{Z}_{12}$

$$\begin{aligned} 0 + 0 &= 0 \\ 1 + 1 &= 2 \\ 2 + 2 &= 4 \\ 3 + 3 &= 6 \\ 4 + 4 &= 8 \\ 5 + 5 &= 10 \\ 6 + 6 &= 0 \\ 7 + 7 &= 2 \\ 8 + 8 &= 4 \\ 9 + 9 &= 6 \\ 10 + 10 &= 8 \end{aligned}$$

14. Let G be an abelian group, and let H be the set of all elements of G of finite order.

(a) Show that H is a subgroup of G.

(b) For a fixed positive integer k, show that $\{a \in G | o(a) \text{is a divisor of } k\}$ is a subgroup of H

(c) For a fixed positive integer k, is $\{a \in G | o(a) \leq k\}$ a subgroup of H? Either give a proof or give a counterexample.

Joe Starr

(a) Inverses: Let $a \in H$, since a is of finite order we have $a^n = 1$ for some $n \in \mathbb{Z}$. We observe that $aa^{n-1} = 1$, now considering a^{n-1}, we take this to the nth power $(a^{n-1})^n = (a^n)^{n-1} = 1$ showing existence of inverses in H.

Closure: Let $a, b \in H$, we consider ab if we know $a^n = 1$ and $b^m = 1$ for some $m, n \in \mathbb{Z}$, if we take $a^{mn}b^{mn} = (a^n)^m (b^m)^n = 1$.

(b) Let $A = \{a \in G | o(a) \text{is a divisor of } k\}$

Inverses: Let $a \in A$ we observe that since $k | \text{ord}(a)$ we have $a^{kq} = 1$ for some $kq \in \mathbb{Z}$ meaning $a^{kq-1}a = 1$ now considering a^{n-1}, we take this to the nth power $\left(a^{kq-1}\right)^{kq} = \left(a^{kq}\right)^{kq-1} = 1$ showing existence of inverses in A.

Closure: Let $a, b \in A$, we consider ab if we know $a^{kn} = 1$ and $b^{km} = 1$ for some $m, n \in \mathbb{Z}$, if we take $a^{kmn}b^{kmn} = \left(a^k n\right)^m \left(b^k m\right)^n = 1$.

(c) Let $G = \mathbb{Z}_{10}^+$, and $k = 5$, this makes $A = \{2,\ 4,\ 5,\ 6,\ 8\}$ if we take $2 + 5 = 7$ we can see A is not closed under addition.

15. Prove that any cyclic group is abelian.

Joe Starr

Let G be a cyclic group generated by g, select $a, b \in G$, we consider $aba^{-1}b^{-1}$. We observe $a = g^k$ and $a^{-1} = g^{k-1}$ for some k, similarly for b and some h. Now rewriting $aba^{-1}b^{-1} = g^k g^h g^{k-1} g^{h-1} = 1$ showing G abelian.

16. Prove or disprove this statement. If G is a group in which every proper subgroup is cyclic, then G is cyclic.

Joe Starr

Select G with the given property. Let H

17. Prove that the intersection of any collection of subgroups of a group is again a subgroup.

Joe Starr

Let H and K be subgroups of a group G, consider $a \in H \cap K$. Since both K and H are groups $a^{-1} \in H$ and $a^{-1} \in K$ putting it in the intersection. Next we consider $a, b \in H \cap K$, since both K and H are groups $ab \in H$ and $ab \in K$ putting it in the intersection. Showing $H \cap K$ a subgroup.

18. Let G be the group of rational numbers, under addition, and let H, K be subgroups of G. Prove that if $H \neq \{0\}$ and $K \neq \{0\}$, then $H \cap K \neq \{0\}$.

Joe Starr

We have previously shown that the intersection of two subgroups is a subgroup. Since neither H nor K are the trivial subgroup we have $\frac{a}{b} \in H$ and $\frac{m}{n} \in K$, $a,\ b,\ m,\ n$ with the usual properties. We observe $b\frac{a}{b} \in H$ and $n\frac{m}{n} \in K$, we then can add these m and a times respectively, yielding $bm\frac{a}{b} = ma$ and $na\frac{m}{n} = ma$ putting $ma \in H \cap K$.

19. Let G be a group, and let $a \in G$. The set $C(a) = \{x \in G | xa = ax\}$ of all elements of G that commute with a is called the centralizer of a.

(a) Show that $C(a)$ is a subgroup of G

(b) Show that $\langle a \rangle \subseteq C(a)$

(c) Compute $C(a)$ if $G = S_3$ and $a = (1, 2, 3)$

(d) Compute $C(a)$ if $G = S_3$ and $a = (1, 2)$

Joe Starr

(a) Inverses: Let $x \in C(a)$, by construction we know $xa = ax$, by transitive proof

$$\begin{aligned} xa = ax &\rightarrow x^{-1}xa = x^{-1}ax \\ &\rightarrow ax^{-1} = x^{-1}axx^{-1} \\ &\rightarrow ax^{-1} = x^{-1}a \end{aligned}$$

putting $x^{-1} \in C(a)$.

Closure: let $x,\ y \in C(a)$, by construction we know $xa = ax$ and $ya = ay$. if we take $xa = ax$ and multiply by y on the left we get $yxa = yax$ then by commutativity we have $yxa = ayx$ putting $yx \in C(a)$ similarly for xy.

(b) If we consider $x \in \langle a \rangle$, observe by construction $x = a^n$ for some n. If we take $xa = a^n a = a^{n+1} = aa^n = ax$ putting $x \in C(a)$.

(c) Since a is the identity element $C(a) = S_3$

(d) $C(a) = \{(1, 2, 3),\ (1, 2)\}$

20. Compute the centralizer in GL_2 ($\mathbf{R}$) of the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Joe Starr

We can calculate $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix}$. From here we observe that for a matrix to commute it must satisfy $c = c,\ a+c = a,\ d+b = a+b,\ c+d = d$ making it of the form $\begin{bmatrix} a & d-a \\ 0 & d \end{bmatrix}$.

22. Show that if a group G has a unique element a of order 2, then $a \in Z(G)$

Joe Starr

23. If the group G is not abelian, show that its center $Z(G)$ is a proper subgroup of an abelian subgroup of G.

Joe Starr

26. Let G be a group with $a, b \in G$. (a) Show that $o\left(a^{-1}\right) = o(a)$ (b) Show that $o(ab) = o(ba)$ (c) Show that $o\left(aba^{-1}\right) = o(b)$

Joe Starr

27. Let G be a finite group, let $n > 2$ be an integer, and let S be the set of elements of G that have order n. Show that S has an even number of elements.

Joe Starr

28. Let G be a group with $a, b \in G$. Assume that $o(a)$ and $o(b)$ are finite and relatively prime, and that $ab = ba$. Show that $o(ab) = o(a)o(b)$

Joe Starr

29. Find an example of a group G and elements $a, b \in G$ such that a and b each have finite order but ab does not.

Joe Starr

2.

Joe Starr

2.

Joe Starr

3.3 Constructing Examples

1. † Find HK in $\mathbf{Z}_{16}^{\times}$, if $H = \langle [3] \rangle$ and $K = \langle [5] \rangle$

Joe Starr

We begin by calculating $H = \{1,\ 3,\ 9,\ 11\}$ and $K = \{1,\ 5,\ 9,\ 13\}$. now by observing $(3 \cdot 13)\%16 = 7$ and $(3 \cdot 5)\%16 = 15$ we get $\mathbb{Z}_{16}^{\times}$.

2. Find HK in $\mathbf{Z}_{21}^{\times}$, if $H = \{[1], [8]\}$ and $K = \{[1], [4], [10], [13], [16], [19]\}$

Joe Starr

$$(1 \cdot 1)\,\%21 = 1$$
$$(1 \cdot 4)\,\%21 = 4$$
$$(1 \cdot 10)\,\%21 = 10$$
$$(1 \cdot 13)\,\%21 = 13$$
$$(1 \cdot 16)\,\%21 = 16$$
$$(1 \cdot 19)\,\%21 = 19$$
$$(8 \cdot 1)\,\%21 = 8$$
$$(8 \cdot 4)\,\%21 = 11$$
$$(8 \cdot 10)\,\%21 = 17$$
$$(8 \cdot 13)\,\%21 = 20$$
$$(8 \cdot 16)\,\%21 = 2$$
$$(8 \cdot 19)\,\%21 = 5$$

$H = \{1,\ 2,\ 4,\ 5,\ 8,\ 10,\ 11,\ 13,\ 16,\ 17,\ 19,\ 20\}$

3. Find an example of two subgroups H and K of S_3 for which HK is not a subgroup.

Joe Starr

Let $H = \{(\,),\ (1,2)\}$ and $K = \{(\,),\ (1,2,3),\ (1,3,2)\}$ we then take $HK = \{(\,),\ (1,2),\ (2,3),\ (1,3),\ (1,2,3),\ (1,3,2)\}$ we observe this isn't a proper subgroup of S_3.

4 Show that the list of elements of $\mathrm{GL}_2(\mathbf{Z}_2)$ given in Example 3.3.6 is correct.

Joe Starr

$$a = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad b = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad c = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad d = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

$$e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad f = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad g = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad h = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$i = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad j = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad k = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad l = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$m = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad n = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad o = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad p = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Det of a is 0
Det of b is 0
Det of c is 0
Det of d is 0
Det of e is 0
Det of f is 0
Det of g is -1
Det of h is -1
Det of i is 0
Det of j is 1
Det of k is 0
Det of l is 1
Det of m is 0
Det of n is 1
Det of o is -1
Det of p is 0

5 Find $|\mathrm{GL}_2(\mathbf{Z}_3)|$

Joe Starr

$$\det\left(\begin{bmatrix}0&1\\1&0\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}0&1\\1&1\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}0&1\\1&2\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}0&1\\2&0\end{bmatrix}\right)=1$$

$$\det\left(\begin{bmatrix}0&1\\2&1\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}0&1\\2&2\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}0&2\\1&0\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}0&2\\1&1\end{bmatrix}\right)=1$$

$$\det\left(\begin{bmatrix}0&2\\1&2\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}0&2\\2&0\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}0&2\\2&1\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}0&2\\2&2\end{bmatrix}\right)=2$$

$$\det\left(\begin{bmatrix}1&0\\0&1\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&0\\0&2\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}1&0\\1&1\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&0\\1&2\end{bmatrix}\right)=2$$

$$\det\left(\begin{bmatrix}1&0\\2&1\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&0\\2&2\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}1&1\\0&1\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&1\\0&2\end{bmatrix}\right)=2$$

$$\det\left(\begin{bmatrix}1&1\\1&0\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}1&1\\1&2\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&1\\2&0\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&1\\2&1\end{bmatrix}\right)=2$$

$$\det\left(\begin{bmatrix}1&2\\0&1\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&2\\0&2\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}1&2\\1&0\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}1&2\\1&1\end{bmatrix}\right)=2$$

$$\det\left(\begin{bmatrix}1&2\\2&0\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}1&2\\2&2\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}2&0\\0&1\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&0\\0&2\end{bmatrix}\right)=1$$

$$\det\left(\begin{bmatrix}2&0\\1&1\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&0\\1&2\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}2&0\\2&1\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&0\\2&2\end{bmatrix}\right)=1$$

$$\det\left(\begin{bmatrix}2&1\\0&1\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&1\\0&2\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}2&1\\1&0\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&1\\1&1\end{bmatrix}\right)=1$$

$$\det\left(\begin{bmatrix}2&1\\2&0\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}2&1\\2&2\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&2\\0&1\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&2\\0&2\end{bmatrix}\right)=1$$

$$\det\left(\begin{bmatrix}2&2\\1&0\end{bmatrix}\right)=1\quad\det\left(\begin{bmatrix}2&2\\1&2\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&2\\2&0\end{bmatrix}\right)=2\quad\det\left(\begin{bmatrix}2&2\\2&1\end{bmatrix}\right)=1$$

$|\mathrm{GL}_2(\mathbb{Z}_3)|=48$

6. Find the cyclic subgroup generated by $\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$ in $\mathrm{GL}_2(\mathbf{Z}_3)$

Joe Starr

$$a^1 = \left(\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}\right) \quad a^2 = \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) \quad a^3 = \left(\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}\right)$$

$$a^4 = \left(\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\right) \quad a^5 = \left(\begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix}\right) \quad a^6 = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$$

7. Let F be a field. Compute the center of $\mathrm{GL}_2(F)$

Joe Starr

8. Prove that if G_1 and G_2 are abelian groups, then the direct product $G_1 \times G_2$ is abelian.

Joe Starr

Let $(a, b)\,,\ (x, y) \in G_1 \times G_2$ we Consider $(a, b)\,(x, y) = (ax, by) = (xa, yb) = (x, y)\,(a, b)$ showing the group is abelian.

9. Construct an abelian group of order 12 that is not cyclic.

Joe Starr

Consider $Z_3^+ \times Z_8^\times$

$$(0,1) \quad (0,3) \quad (0,5)$$

$$(0,7) \quad (1,1) \quad (1,3)$$

$$(1,5) \quad (1,7) \quad (2,1)$$

$$(2,3) \quad (2,5) \quad (2,7)$$

by proposition 3.3.4 we can see this is not cyclic. Let since both Z_3^+ and $Z_8^\times$ are abelian the group is abelian.

10 . Construct a group of order 12 that is not abelian.

Joe Starr

Consider $Z_2^+ \times S_3$

$$(0,())\quad (0,(1,\ 2))\quad (0,(1,\ 3))$$

$$(0,(2,\ 3))\quad (0,(1,\ 2,\ 3))\quad (0,(1,\ 3,\ 2))$$

$$(1,())\quad (1,(1,\ 2))\quad (1,(1,\ 3))$$

$$(1,(2,\ 3))\quad (1,(1,\ 2,\ 3))\quad (1,(1,\ 3,\ 2))$$

Let $(a,(1,\ 2))\,,\ (x,(2,\ 3)) \in Z_3^+ \times S_3$ we Consider

$$(a,(1,\ 2))\,(x,(2,\ 3)) = (a+x,(1,\ 2,\ 3))$$
$$(x,(2,\ 3))\,(a,(1,\ 2)) = (x+a,(1,\ 3,\ 2))$$

the group is not abelian.

13. Let $n > 2$ be an integer, and let $X \subseteq S_n \times S_n$ be the set $X = \{(\sigma, \tau) | \sigma(1) = \tau(1)\}$ Show that X is not a subgroup of $S_n \times S_n$

Joe Starr

We will use S_3 as an example calculating X yields:

$$((),\ ()) \qquad ((),\ (2,\ 3)) \quad ((1,\ 2),\ (1,\ 2,\ 3))$$

$$((1,\ 3),\ (1,\ 3,\ 2)) \quad ((2,\ 3),\ ()) \quad ((1,\ 2,\ 3),\ (1,\ 2))$$

$$((1,\ 3,\ 2),\ (1,\ 3))$$

if we consider the inverse of $((1,\ 3,\ 2),\ (1,\ 3))$, which is $((1,\ 2,\ 3),\ (1,\ 3))$ we see this not in X showing X not a subgroup.

17. Let G be a finite group, and let H, K be subgroups of G. Prove that

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Joe Starr

Let G be of order n.

20. Let G be a group of order 6, and suppose that $a, b \in G$ with a of order 3 and b of order 2. Show that either G is cyclic or $ab \neq ba$

Joe Starr

First assume $ab = ba$ for $a,\ b \in G$ with the given properties. We observe that $(ab)^6 = 1$ making $G = \langle ab \rangle$.
Next assume that $ab \neq ba$, for $a,\ b \in G$ with the given properties. Since G is not abelian by question 15 from section 3.2 G is not cyclic.

3.4 Isomorphisms

1. Show that the multiplicative group $\mathbf{Z}_{10}^{\times}$ is isomorphic to the additive group $\mathbf{Z}_4$. Hint: Find a generator $[a]_{10}$ of $\mathbf{Z}_{10}^{\times}$ and define $\phi : \mathbf{Z}_4 \to \mathbf{Z}_{10}^{\times}$ by $\phi([n]_4) = [a]_{10}^n$

Joe Starr

We begin by considering $\mathbb{Z}_{10}^{\times} = \{1, 3, 7, 9\}$, observe $3 = 3,\ 3^2 = 9,\ 3^3 = 7,\ 3^4 = 1$ showing $\mathbf{Z}_{10}^{\times} = \langle 3 \rangle$. We can then let $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_{10}^{\times}$ be $\phi(n) = 3^n$ we can construct $\phi^{-1}(3^n) = n$ and observe $\phi\left(\phi^{-1}(3^n)\right) = \phi(n) = 3^n$ showing φ a bijection. We will now show φ is a homomorphism. Let $n, k \in \mathbb{Z}_4$, and $\phi(n+k) = 3^{n+k} = 3^n 3^n = \phi(n)\,\phi(k)$, showing φ an isomorphism.

2. Show that the multiplicative group $\mathbf{Z}_7^\times$ is isomorphic to the additive group $\mathbf{Z}_6$.

Joe Starr

We begin by considering $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$, observe $3 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1$ showing $\mathbb{Z}_7^\times = \langle 3 \rangle$. We can then let $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_7^\times$ be $\phi(n) = 3^n$ we can construct $\phi^{-1}(3^n) = n$ and observe $\phi\left(\phi^{-1}(3^n)\right) = \phi(n) = 3^n$ showing φ a bijection. We will now show φ is a homomorphism. Let $n, k \in \mathbb{Z}_6$, and $\phi(n+k) = 3^{n+k} = 3^n 3^n = \phi(n)\,\phi(k)$, showing φ an isomorphism.

3. Show that the multiplicative group $\mathbf{Z}_8^\times$ is isomorphic to the group $\mathbf{Z}_2 \times \mathbf{Z}_2$

Joe Starr

We let $\varphi : \mathbf{Z}_8^\times \to \mathbf{Z}_2 \times \mathbf{Z}_2$ by

$$\phi(a) = \begin{cases} (0,0) & \text{For } a = 1 \\ (0,1) & \text{For } a = 3 \\ (1,0) & \text{For } a = 5 \\ (1,1) & \text{For } a = 7 \end{cases} \tag{1}$$

observe the tables for the two groups:

$\cdot$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

4. Show that $\mathbf{Z}_5^\times$ is not isomorphic to $\mathbf{Z}_8^\times$ by showing that the first group has an element of order 4 but the second group does not.

Joe Starr

We first consider $2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1$ showing $\langle 2 \rangle$ is of order 4. We can then observe the order of the elements of $\mathbf{Z}_8^\times$, $3^2 = 1,\ 5^2 = 1,\ 7^2 = 1$ since none of the elements of $\mathbf{Z}_8^\times$ have order 4 it cant me that $\mathbf{Z}_8^\times$ and $\mathbf{Z}_5^\times$ are isomorphic.

6. Is the additive group $\mathbf{C}$ of complex numbers isomorphic to the multiplicative group $\mathbf{C}^\times$ of nonzero complex numbers?

Joe Starr

7. Let G_1 and G_2 be groups. Show that $G_2 \times G_1$ is isomorphic to $G_1 \times G_2$

Joe Starr

Let $\varphi : G_2 \times G_1 \to G_1 \times G_2$ be $\phi((a,b)) = (b,a)$ and $\phi^{-1}((b,a)) = (a,b)$. We first establish φ as a bijection, $\phi\left(\phi^{-1}((b,a))\right) = \phi((a,b)) = (b,a)$. Now we will establish φ as a homomorphism, let $(a,b),(x,y) \in G_2 \times G_1$ consider

$$\begin{aligned}\phi((a,b)(x,y)) &= \phi((ax,by)) \\ &= (by,ax) \\ &= (b,a)(y,x) \\ &= \phi((a,b))\phi((x,y))\end{aligned}$$

showing the groups to be isomorphic.

8. Let G be a group. Show that the group $(G, *)$ defined in Exercise 3 of Section 3.1 is isomorphic to G.

Joe Starr

Let $(G\,,\,\cdot)$ be a group. Define a new binary operation $*$ on G by the formula $a*b = b\cdot a$, for all $a, b \in G$. Define $\varphi : (G, \cdot) \to (G, *)$, with $\phi\,(a) = a$ the trivial map is a bijection. Next we will show φ to be a homomorphism let $a, b \in G$, observe $\phi\,(a \cdot b) = a \cdot b = b * a = \phi\,(b) * \phi\,(a)$.

9. Prove that any group with three elements must be isomorphic to $\mathbf{Z}_3$.

Joe Starr

Let G be a group of three elements. Since G is a group there exists an identity element e in G. This makes $a, b \in G$ with $a \neq b \neq e$ and WOLG we are left with two options either $aa = e$ or $ab = e$. If $aa = e$ we get the table

$\cdot$	e	a	b
e	e	a	b
a	a	e	b
b	b	b	e

observe $a \cdot (b \cdot b) = a$ but $(a \cdot b) \cdot b = e$ showing this is not a group under $\cdot$. Leaving us with one option given by the table below, which by comparison is isomorphic to $\mathbb{Z}_3$

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\cdot$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

13. Let G be the set of all matrices in $\mathrm{GL}_2(\mathbf{Z}_3)$ of the form $\begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix}$. That is, $c, d \in \mathbf{Z}_3$ and $d \neq [0]_3$. Show that G is isomorphic to S_3

Joe Starr

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$$
$$C = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \quad E = \begin{bmatrix} 1 & 0 \\ 2 & 2 \end{bmatrix}$$

$\cdot$	$()$	$(1,2)$	$(2,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$
$()$	$()$	$(1,2)$	$(2,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)$	$(1,2)$	$()$	$(1,2,3)$	$(1,3,2)$	$(2,3)$	$(1,3)$
$(2,3)$	$(2,3)$	$(1,3,2)$	$()$	$(1,2,3)$	$(1,3)$	$(1,2)$
$(1,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$	$()$	$(1,2)$	$(2,3)$
$(1,2,3)$	$(1,2,3)$	$(1,3)$	$(1,2)$	$(2,3)$	$(1,3,2)$	$()$
$(1,3,2)$	$(1,3,2)$	$(2,3)$	$(1,3)$	$(1,2)$	$()$	$(1,2,3)$

$$I \times I = I \quad I \times A = A \quad I \times B = B \quad I \times C = C$$

$$I \times D = D \quad I \times E = E \quad A \times I = A \quad A \times A = D$$

$$A \times B = E \quad A \times C = B \quad A \times D = I \quad A \times E = C$$

$$B \times I = B \quad B \times A = C \quad B \times B = I \quad B \times C = A$$

$$B \times D = E \quad B \times E = D \quad C \times I = C \quad C \times A = E$$

$$C \times B = D \quad C \times C = I \quad C \times D = B \quad C \times E = A$$

$$D \times I = D \quad D \times A = I \quad D \times B = C \quad D \times C = E$$

$$D \times D = A \quad D \times E = B \quad E \times I = E \quad E \times A = B$$

$$E \times B = A \quad E \times C = D \quad E \times D = C \quad E \times E = I$$

15. Let C_2 be the subgroup $\{\pm 1\}$ of the multiplicative group $\mathbf{R}^\times$. Show that $\mathbf{R}^\times$ is isomorphic to $\mathbf{R}^+ \times C_2$

Joe Starr

Let $\phi((x,a)) = ae^x$, and $\phi^{-1}(ae^x) = (x,a)$ observe $\phi\left(\phi^{-1}(ae^x)\right) = \phi((x,a)) = ae^x$.

Next consider $\phi((x,a)(y,b)) = (x+y, ab) = abe^{x+y} = ae^x be^y = \phi((x,a))\,\phi((y,b))$ as desired.

17. Let G be any group, and let a be a fixed element of G. Define a function $\phi_a : G \to G$ by $\phi_a(x) = axa^{-1}$, for all $x \in G$. Show that ϕ_a is an isomorphism.

Joe Starr

Define $\phi^{-1}(x) = a^{-1}xa$, consider $\phi^{-1}(\phi(x)) = \phi^{-1}(axa^{-1}) = a^{-1}axa^{-1}a = x$.
Next consider $\phi(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi(x)\phi(y)$.

18. Let G be any group. Define $\phi : G \to G$ by $\phi(x) = x^{-1}$, for all $x \in G$ (a) Prove that ϕ is one-to-one and onto. (b) Prove that ϕ is an isomorphism if and only if G is abelian.

Joe Starr

We've shown uniqueness of inverses, and since G is a group φ is a bijection. G is abelian:
$\phi(ab) = ab^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$ G is non-abelian:
$\phi(ab) = ab^{-1} \neq a^{-1}b^{-1}$ so is not a homomorphism.

22. Let G_1 and G_2 be groups. Show that G_1 is isomorphic to the subgroup of the direct product $G_1 \times G_2$ defined by $\{(x_1, x_2) \,|x_2 = e\}$

Joe Starr

Define $\phi(a) = (a, e)$, and $\phi^{-1}((a, e)) = a$, consider $\phi^{-1}(\phi(a)) = \phi^{-1}((a, e)) = a$.
Now consider $\phi(ab) = (ab, e) = (a, e)(b, e) = \phi(a)\phi(b)$

23. Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $\mathbf{Z}_{mn}^{\times}$ is isomorphic to $\mathbf{Z}_m^{\times} \times \mathbf{Z}_n^{\times}$

Joe Starr

30. Let G_1 and G_2 be groups. A function from G_1 into G_2 that preserves products but is not necessarily a one-to-one correspondence will be called a group homomorphism, from the Greek word homos meaning same. Show that $\phi : \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^\times$ defined by $\phi(A) = \det(A)$ for all matrices $A \in \mathrm{GL}_2(\mathbf{R})$ is a group homomorphism.

Joe Starr

3.5 Cyclic Groups

1. Let G be a group and let $a \in G$ be an element of order 12. What is the order of a^j for $j = 2, \ldots, 11$?

Joe Starr

By applying 3.5.3 and 3.5.4 we get $(a^1)^{12}, (a^2)^6, (a^3)^4, (a^4)^3, (a^5)^{12}, (a^6)^2, (a^7)^{12}, (a^8)^3, (a^9)^4, (a^{10})^6, (a^{11})^{12}$

2. Let G be a group and let $a \in G$ be an element of order 30. List the powers of a that have order 2, order 3 or order 5

Joe Starr

$2 : 15$

$3 : 10, 20$

$5 : 6, 12, 18, 24$

5. Find the cyclic subgroup of $C^\times$ generated by $\frac{\sqrt{2}+\sqrt{2}i}{2}$.

Joe Starr

$$
\begin{aligned}
a^1 &= \frac{\sqrt{2}+\sqrt{2}i}{2} \\
a^2 &= \frac{\sqrt{2}+\sqrt{2}i}{2}\frac{\sqrt{2}+\sqrt{2}i}{2} = i \\
a^4 &= i = -1 \\
a^8 &= i = 1
\end{aligned}
$$

6. Find the order of the cyclic subgroup of $\mathbf{C}^{\times}$ generated by $1+i$

Joe Starr

$$
\begin{aligned}
a^1 &= 1+i \\
a^2 &= (1+i)(1+i) = 2i \\
a^4 &= -4 \\
a^8 &= 16 \\
a^{2^{3+n}} &= 2^{4+n}
\end{aligned}
$$

we observe 2^{4+n} has infinite order so a must have infinite order.

7. Which of the multiplicative groups $\mathbf{Z}_{15}^{\times}, \mathbf{Z}_{18}^{\times}, \mathbf{Z}_{20}^{\times}, \mathbf{Z}_{27}^{\times}$ are cyclic?

Joe Starr

$\mathbf{Z}_{15}^{\times} : 15 = 5 \cdot 3$ The product of two odd primes, not cyclic
$\mathbf{Z}_{18}^{\times} : 18 = 2 \cdot 3^2$ The product of two and power of an odd prime, cyclic
$\mathbf{Z}_{20}^{\times} : 20 = 2^2 \cdot 5$ The product of four and an odd prime, not cyclic
$\mathbf{Z}_{27}^{\times} : 15 = 3^3$ The power of an odd prime, cyclic

11. Which of the multiplicative groups $\mathbb{Z}_7^\times,\ \mathbb{Z}_{10}^\times,\ \mathbb{Z}_{12}^\times,\ \mathbb{Z}_{14}^\times$ are isomorphic.

Joe Starr

$\mathbb{Z}_7^\times : 7 = 7$ The power of an odd prime, cyclic
$\mathbb{Z}_{10}^\times : 10 = 2 \cdot 5$ The product of two and power of an odd prime, cyclic
$\mathbb{Z}_{12}^\times : 12 = 2^2 \cdot 3 \cdot 5$ The product of four and an odd prime, not cyclic
$\mathbb{Z}_{14}^\times : 14 = 2 \cdot 7$ The product of two and power of an odd prime, cyclic

$\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$
$\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$
$\mathbb{Z}_{14}^\times = \{1, 3, 5, 9, 11, 13\}$

Since $\mathbb{Z}_{14}^\times$ has order six and and $\mathbb{Z}_7^\times$ has order six, and both are cyclic they must both be isomorphic to $\mathbb{Z}_6$.

12. Let a, b be positive integers, and let $d = \gcd(a\,,\,b)$ and $m = \text{lcm}\,(a\,,\,b)$. Use proposition 3.5.5 to prove that $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_d \times \mathbb{Z}_m$.

Joe Starr

By $3.5.5$ we have that $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$, and $\mathbb{Z}_{dm} \cong \mathbb{Z}_d \times \mathbb{Z}_m$, we've previously shown $\gcd(a\,,\,b) \cdot \text{lcm}\,(a\,,\,b) = ab$ making $\mathbb{Z}_{dm} = \mathbb{Z}_{ab}$ showing $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_d \times \mathbb{Z}_m$.

18. Let G be the set of all 3 $\times 3$ matrices of the form $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}$

(a) Show that if $a, b, c \in \mathbf{Z}_3$, then G is a group with exponent 3

(b) Show that if $a, b, c \in \mathbf{Z}_2$, then G is a group with exponent 4.

Joe Starr

(a)

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} a^2 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \right) a^3 = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)$$

$$a=\begin{bmatrix}1&0&0\\2&1&0\\1&0&1\end{bmatrix}\ a^2=\left(\begin{bmatrix}1&0&0\\1&1&0\\2&0&1\end{bmatrix}\right)\ a^3=\left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right)$$

$$a=\begin{bmatrix}1&0&0\\2&1&0\\1&1&1\end{bmatrix}\ a^2=\left(\begin{bmatrix}1&0&0\\1&1&0\\1&2&1\end{bmatrix}\right)\ a^3=\left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right)$$

$$a=\begin{bmatrix}1&0&0\\2&1&0\\1&2&1\end{bmatrix}\ a^2=\left(\begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix}\right)\ a^3=\left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right)$$

$$a=\begin{bmatrix}1&0&0\\2&1&0\\2&0&1\end{bmatrix}\ a^2=\left(\begin{bmatrix}1&0&0\\1&1&0\\1&0&1\end{bmatrix}\right)\ a^3=\left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right)$$

$$a=\begin{bmatrix}1&0&0\\2&1&0\\2&1&1\end{bmatrix}\ a^2=\left(\begin{bmatrix}1&0&0\\1&1&0\\0&2&1\end{bmatrix}\right)\ a^3=\left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right)$$

$$a=\begin{bmatrix}1&0&0\\2&1&0\\2&2&1\end{bmatrix}\ a^2=\left(\begin{bmatrix}1&0&0\\1&1&0\\2&1&1\end{bmatrix}\right)\ a^3=\left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right)$$

We observe that every element is order 3 meaning exponent of G is 3.

(b)

$$a=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$a=\begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix}\ a^2=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$a=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\ a^2=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$a=\begin{bmatrix}1&0&0\\0&1&0\\1&0&1\end{bmatrix}\ a^2=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$a=\begin{bmatrix}1&0&0\\0&1&0\\1&1&1\end{bmatrix}\ a^2=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \; a^4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \; a^4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \; a^4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We observe that every element is either order two or four. This makes exponent of G 4.

19. Prove that $\sum_{d|n} \varphi(d) = n$ for any positive integer n Hint: Interpret the equation in the cyclic group $\mathbf{Z}_n$, by considering all of its sub-groups.

Joe Starr

20. Let $n = 2^k$ for $k > 2$. Prove that $\mathbf{Z}_n^\times$ is not cyclic. Hint: Show that ± 1 and $(n/2) \pm 1$ satisfy the equation $x^2 = 1$, and that this is impossible in any cyclic group.

Joe Starr

21. Prove that if p and q are different odd primes, then $\mathbf{Z}_{pq}^{\times}$ is not a cyclic group.

Joe Starr

3.6 Permutation Groups

1. Find the orders of each of these permutations.

   (a) $(1,2)(2,3)(3,4)$

   (b) $(1,2,5)(2,3,4)(5,6)$

   (c) $(1,3)(2,6)(1,4,5)$

   (d) $(1,2,3)(2,4,3,5)(1,3,2)$

Joe Starr

(a) $(1,2)(2,3)(3,4) = (1,2,3,4)$ order is 4

(b) $(1,2,5)(2,3,4)(5,6) = (1,2,3,4,5,6)$ order is 6

(c) $(1,3)(2,6)(1,4,5) = (2,6)(1,3)(1,4,5) = (2,6)(3,1,4,5)$ order is 4

(d) $(1,2,3)(2,4,3,5)(1,3,2) = (1,5,3,4)$ order is 4

5. Show that no proper subgroup of S_4 contains both $(1,2,3,4)$ and $(1,2)$

Joe Starr

We let $H \leq S_4$ with $(1,2,3,4)\,,\ (1,2) \in H$,by Lagrange's theorem we know that any subgroups of S_4 must be of order $1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 24$. We observe the cyclic subgroup of $\langle(1,2,3,4)\rangle \in H$ the order of H must be larger then 4. Similarly observe that $(1,2)\,(1,2,3,4) = (2,3,4)$, meaning $6 \geq |H|$. Finely we have by construction, $(1,2) \in H$, so $7 \leq |H|$. Since $|H| \mid |S_4|$, it must be that $8 \geq |H|$.

13. List the elements of A_4

Joe Starr

$(), (123), (124), (132), (134), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23)$

16. Let H be a subgroup of S_n

(a) Show that either all permutations in H are even, or else half of the permutations in H are even and half are odd.

(b) Show that the set of all even permutations in H forms a subgroup of H

Joe Starr

(a) If H has only even permutations we are done. Otherwise we know there exists a set of odd permutations $H_o \subset H$, and even $H_e \subset H$. Further we know that $H = H_o \cup H_e$. We know that parity follows normal parity rules, so $p \in H_o$, pH_o makes all $px \in pH_o$ even parity and pH_e makes all $px \in pH_e$ odd parity. We observe $H = pH_o \cup pH_e$. Now, since for $x \in pH_e$ x is an odd Permutation so it must be that $x \in H_o$. Similarly $x \in pH_o$ means $x \in H_e$. From here we have $|H_o| = |pH_o| = |pH_e| = |H_e|$, showing there are the same number of even and odd elements of H. Since $H = H_o \cup H_e$ it must be that $|H_e| = \frac{1}{2}|H|$.

(b) If σ and τ are even permutations, then each can be expressed as a product of an even number of transpositions. It follows that $\tau\sigma$ can be expressed as a product of an even number of transpositions, and so the set of all even permutations of H is closed under multiplication of permutations. Furthermore, the identity permutation is even. since H is a finite set, this is enough to imply that we have a subgroup.

17. For any elements $\sigma, \tau \in S_n$, show that $\sigma\tau\sigma^{-1}\tau^{-1} \in A_n$

Joe Starr

We have previously shown that parity of a Permutation and its inverse are equal. We have also shown that parity of permutations follows normal addition rules for parity. So we observe $\sigma\tau\sigma^{-1}\tau^{-1}$ is 2 times the parity of sigma plus two times the parity of tau. Making the parity of $\sigma\tau\sigma^{-1}\tau^{-1}$ even as desired.

18. Let S be an infinite set. Let H be the set of all elements $\sigma \in \mathrm{Sym}(S)$ such that $\sigma(x) = x$ for all but finitely many $x \in S$. Prove that H is a subgroup of $\mathrm{Sym}(S)$

Joe Starr

Inverses: We observe that σ has k elements such that $\sigma(x) \neq x$. This means that for some $\sigma(x_i) = x_j$, we select σ^{-1} such that $\sigma^{-1}(x_j) = x_i$. We see that

Closure: We select $\sigma_1 and \sigma_2$, we observer that they have k_1 and k_2 elemetns with $\sigma(x) \neq x$. If we assume in the worst case that these two mappings are disjoint sets of x_i's we sill have the union of countable sets which we know to be countable.

3.7 Homomorphism

7. Define $\phi : \mathbf{C}^\times \to \mathbf{R}^\times$ by $\phi(a+bi) = a^2 + b^2$, for all $a + bi \in \mathbf{C}^\times$. Show that ϕ is a homomorphism.

Joe Starr

9. Which of the following functions are homomorphisms?

(a) $\phi : \mathbf{R}^\times \to \mathrm{GL}_2(\mathbf{R})$ defined by $\phi(a) = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$

(b) $\phi : \mathbf{R} \to \mathrm{GL}_2(\mathbf{R})$ defined by $\phi(a) = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}$

(c) $\phi : M_2(\mathbf{R}) \to \mathbf{R}$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a$

(d) $\phi : \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^\times$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ab$

(e) $\phi : \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d$

(f) $\phi : \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^\times$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$

Joe Starr

10. Let $\phi : G_1 \to G_2$ and $\theta : G_2 \to G_3$ be group homomorphisms. Prove that $\theta\phi : G_1 \to G_3$ is a homomorphism. Prove that $\ker(\phi) \subseteq \ker(\theta\phi)$

Joe Starr

13. Let G be a group, and let H be a normal subgroup of G. Show that for each $f \in G$ and $h \in H$ there exist h_1 and h_2 in H with $gh = h_1 g$ and $hg = gh_2$.

Joe Starr

15. Show that the only proper nontrivail normal subgroup of S_3 in the subgroup with three elements.

Joe Starr

17. Recall that the center of a group G is $\{x \in G | xg = gx \text{ for all } g \in G\}$. Prove that the center of any group is a normal subgroup.

Joe Starr

3.8 Cosets, Normal Subgroups, and Factor Groups

1. List all cosets in $\mathbf{Z}_{24}$ of each of the given subgroups.

   (a) $\langle [3] \rangle$

   (b) $\langle [16] \rangle$

Joe Starr

6. Let G be a group with subgroup H. Prove that there is a one-to-one correspondence between the left and right cosets of H. (Your proof must include the case in which G is infinite.)

Joe Starr

7. Prove that if N is a normal subgroup of G, and H is any subgroup of G, then $H \cap N$ is a normal subgroup of H

Joe Starr

9. Let G be a finite group, and let n be a divisor of $|G|$. Show that if H is the only subgroup of G of order n, then H must be normal in G.

Joe Starr

11. Let N be a normal subgroup of G. Show that the order of any coset aN in G/N is a divisor of $o(a)$, when $o(a)$ is finite.

Joe Starr

14. Let N be a subgroup of the center of G. Show that if G/N is a cyclic group, then G myst be abelian.

Joe Starr

28. Consider the additive groups $\mathbb{Q}$ and $\mathbb{Z}$. Show that $\phi : \mathbb{Q} \to \mathbb{Z}$ is any group homomorphism, then $\phi(r) = 0$ for all $r \in Q$.

Joe Starr

30. Consider the additive groups $\mathbb{Z}_2$ and $\mathbb{Q}$. Show that $\phi : \mathbb{Z}_2 \to \mathbb{Q}$ is any group homomorphism, then $\phi(x) = 0$ for all $x \in \mathbb{Z}_2$.

Joe Starr

4 Polynomials

4.1 Fields; Roots of Polynomials

3. For $f(x) = 2x^3 + x^2 - 2x + 1$, use the method of Theorem 4.1 .9 to write $f(x) = q(x)(x - 1) + f(1)$

Joe Starr

9. Show that if c is any element of the field F and $k > 2$ is an odd integer, then $x + c$ is a factor of $x^k + c^k$.

Joe Starr

11. Let a be a nonzero element of a field F. Show that $\left(a^{-1}\right)^{-1} = a$ and $(-a)^{-1} = -a^{-1}$.

Joe Starr

13. Show that the set $\mathbb{Q}\left(\sqrt{3}\right) = \left\{a + b\sqrt{3} | a,\ b \in \mathbb{Q}\right\}$ is closed under addition, subtraction, multiplication, and division.

Joe Starr

15. Show that the set of matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where $a, b \in \mathbb{R}$, is a field under the operations of matrix addition and multiplication.

Joe Starr

16. Show that the set of matrices of the form $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$, where $a, b \in \mathbb{R}$, is a field under the operations of matrix addition and multiplication.

Joe Starr

4.2 Factors

1. Use the division algorithm to find the quotient and remainder when $f(x)$ is divided by $g(x)$ over the field of rational numbers $\mathbf{Q}$.

(a) $f(x) = 2x^4 + 5x^3 - 7x^2 + 4x + 8 \quad g(x) = 2x - 1$

(b) $f(x) = 2x^7 - 5x^6 + 5x^5 - x^3 - x^2 + 4x - 5 \quad g(x) = x^2 - x + 1$

(c) $f(x) = x^5 + 1 \quad g(x) = x + 1$

(d) $f(x) = 2x^4 + x^3 - 6x^2 - x + 2 \quad g(x) = 2x^2 - 5$

Joe Starr

3. Find the greatest common divisor of $f(x)$ and $f'(x)$, over $\mathbf{Q}$

(a) $f(a)f(x) = x^4 - x^3 - x + 1$

(b) $f(x) = x^3 - 3x - 2$

(c) $f(x) = x^3 + 2x^2 - x - 2$

(d) $f(x) = x^4 + 2x^3 + 3x^2 + 2x + 1$

Joe Starr

9. Let $a \in \mathbf{R}$, and let $f(x) \in \mathbf{R}[x]$, with derivative $f'(x)$. Show that the remainder when $f(x)$ is divided by $(x-a)^2$ is $f'(a)(x-a) + f(a)$

Joe Starr

17. Show that for any real number $a \neq 0$, the polynomial $x^n - a$ has no multiple roots in R.

Joe Starr

4.3 Existence of Roots

1. Let F be a field. Given $p(x) \in F[x]$, prove that congruence modulo $p(x)$ defines an equivalence relation on $F[x]$.

Joe Starr

2. F Prove Proposition 4.3.4.

Joe Starr

3. Let E be a field, and let F be a subfield of E. Prove that the multiplicative identity of F must be the same as that of E

Joe Starr

12. Prove that $\mathbf{Q}[x]/\langle x^2 - 2\rangle$ is isomorphic to $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbf{Q}\}$, which was shown to be a field in Example 4.1 .1

Joe Starr

25. For which values of $k = 2, 3, 5, 7, 11$ is $\mathbf{Z}_k[x]/\langle x^2 + 1\rangle$ a field? Show your work.

Joe Starr

4.4 Polynomials over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$

1. let $f(x), g(x) \in \mathbf{Z}[x]$, and suppose that $g(x)$ is monic. Show that there exist unique polynomials $q(x), r(x) \in \mathbf{Z}[x]$ with $f(x) = q(x)g(x) + r(x)$, where either $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$

Joe Starr

6. Use Eisenstein's criterion to show that each of these polynomials is irreducible over the field of rational numbers. (You may need to make a substitution.)

(a) $x^4 + 1$ (substitute $x + 1$)

(b) $x^6 + x^3 + 1$ (substitute $x + 1$)

(c) $x^3 + 3x^2 + 5x + 5$

(d) $x^3 - 3x^2 + 9x - 10$

Joe Starr

8. Let $f(x) = x^2 + 100x + n$

(a) Give an infinite set of integers n such that $f(x)$ is reducible over $\mathbf{Q}$

(b) Give an infinite set of integers n such that $f(x)$ is irreducible over $\mathbf{Q}$

Joe Starr

5 Commutative Rings

5.1 Commutative Rings; Integral Domains

6. Show that no proper nontrivial subset of Z can form a ring under the usual operations of addition and multiplication.

Joe Starr

11. Let R be a commutative ring such that $a^2 = a$ for all $a \in R$. Show that $a + a = 0$ for all $a \in R$

Joe Starr

15. Let I be any set and let R be the collection of all subsets of I. Define addition and multiplication of subsets $A, B \subseteq I$ as follows:

$$A + B = A \cup B \quad \text{and} \quad A \cdot B = A \cap B$$

Is R a commutative ring under this addition and multiplication?

Joe Starr

20. Give addition and multiplication tables for $\mathbf{Z}_2 \oplus \mathbf{Z}_2$

Joe Starr

22. Find all units of the following rings.

(a) $\mathbf{Z} \oplus \mathbf{Z}$

(b) $\mathbf{Z}_4 \oplus \mathbf{Z}_9$

Joe Starr

5.2 Ring Homomorphisms

1. Let R be a commutative ring, and let D be an integral domain. Let $\phi : R \to D$ be a nonzero function such that $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$, for all $a, b \in R$. Show that ϕ is a ring homomorphism.

Joe Starr

4. Show that taking complex conjugates defines an automorphism of $\mathbf{C}$. That is, for $z \in \mathbf{C}$, define $\phi(z) = \bar{z}$, and show that ϕ is an automorphism of $\mathbf{C}$

Joe Starr

9. Define $\phi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}[\sqrt{2}]$ by $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$, for all $m, n \in \mathbf{Z}$. Show that ϕ is an automorphism of $\mathbf{Z}[\sqrt{2}]$

Joe Starr

21. Are $\mathbb{Z}_9$ and $\mathbb{Z}_3 \bigoplus \mathbb{Z}_3$ isomorphic as rings?

Joe Starr

5.3 Ideals and Factor Rings

1. Give a multiplication table for the ring $\mathbb{Z}_2[x] \Big/ \langle x^2 + 1 \rangle$

Joe Starr

4. Give the multiplication table for the ring $\mathbb{Z}_3[x] \Big/ \langle x^2 - 1 \rangle$

Joe Starr

10. Show that if R is a finite ring, then every prime ideal of R is maximal.

Joe Starr

16. Let R be a commutative ring with ideals I, J. Let

$$I + J = \{x \in R | x = a + b \text{ for some } a \in I, b \in J\}$$

(a) Show that $I + J$ is an ideal.

(b) Determine $n\mathbf{Z} + m\mathbf{Z}$ in the ring of integers.

Joe Starr

5.4 Quotient Fields

8. Let p be a prime number, and let $D = \{m/n | m, n \in \mathbf{Z} \text{ and } pXn\}$. Verify that D is an integral domain and find $Q(D)$

Joe Starr

10. Considering $\mathbf{Z}[x]$ as a subring of $\mathbf{Q}[x]$, show that both rings have the same quotient field.

Joe Starr

12. F Show that if P is a prime ideal of D, then $D_P = \{a/b \in Q(D) | b \notin P\}$ is an integral domain with $D \subseteq D_P \subseteq Q(D)$

Joe Starr

6 Section

I <3 my Wayne State Libraries! Do you?

6.1 A Subsection

7 Section

I <3 my Wayne State Libraries! Do you?

7.1 A Subsection

8 Section

I <3 my Wayne State Libraries! Do you?

8.1 A Subsection

9 Section

I <3 my Wayne State Libraries! Do you?

9.1 A Subsection

10 Section

I <3 my Wayne State Libraries! Do you?

10.1 A Subsection

11 General Proofs