First Homework Solutions

1. **1.1.9(b) on page 22** Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Prove that the nonzero elements of G form a group under multiplication.

   If $x, y \in G$ then we may write $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ where $a, b, c, d \in \mathbb{Q}$, and then $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$. Also if $x, y \neq 0$, then $xy \neq 0$. It follows that multiplication is a binary operation on $G \setminus 0$. Also multiplication is associative and the identity is 1. Finally we need to check for inverses. If $a + b\sqrt{2} \in G \setminus 0$, then the inverse will be $1/(a + b\sqrt{2})$; the only problem we might have is that this is not obviously in $G \setminus 0$. However by multiplying top and bottom by $a - b\sqrt{2}$, this is

   $$\frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2}.$$

   Since $a^2 - 2b^2$ is a nonzero rational number, it is now clear that the inverse is in $G \setminus 0$ (if $a^2 - 2b^2 = 0$, then $\sqrt{2} \in \mathbb{Q}$) and the result follows.

2. **1.1.14 on page 22** Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}$, $\overline{-1}$, $\overline{5}$, $\overline{13}$, $\overline{-13}$, $\overline{17}$.

   Answer: 1,2,6,3,6,2. I won't give explanations for all the answers here, just for $\overline{5}$. We have modulo 36, $5^1 = 5$, $5^2 = 25$, $5^3 = 17$, $5^4 = 13$, $5^5 = 29$, $5^6 = 1$. Therefore the least positive power of $\overline{5}$ which is the identity is 6, consequently the order of $\overline{5}$ is 6.

3. **1.1.25 on page 22** Prove that if G is a group and $x^2 = 1$ for all $x \in G$, then G is abelian.

   Let $x, y \in G$. Then $x^2 = y^2 = (xy)^2 = 1$. Therefore

   $$x^2y^2 = 1 = (xy)^2 = xyxy.$$

   Multiplying by x^{-1} on the left and y^{-1} on the right, we obtain $xy = yx$ as required.

Second Homework Solutions

1. **2.1.10(a) on page 48** Prove that if H and K are subgroups of the group G, then so is $H \cap K$.

   Let e be the identity of G. Then $e \in H, K$ because H and K are subgroups of G, consequently $e \in H \cap K$. Next let $x, y \in H \cap K$. Then $xy \in H$ because $H \leq G$ and $xy \in K$ because $K \leq G$. Therefore $xy \in H \cap K$. Finally $x^{-1} \in H$ and K because H and K are subgroups of G, and we deduce that $x^{-1} \in H \cap K$. It now follows that $H \cap K$ is a subgroup of G as required.

2. **1.2.3 on page 27** Use the standard generators and relations to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

   Each element of D_{2n} can be written uniquely in the form r^i or sr^i, where $0 \leq i \leq n-1$ (see page 25). The elements r^i are of course powers of r, so we need to prove that sr^i has order 2. Since $sr^i \neq e$, it will be sufficient to show that $(sr^i)^2 = e$; we shall show that this is true for all i. We have $(sr^i)^2 = sr^i sr^i$. Now the relation $rs = sr^{-1}$ applied i times shows that $r^i s = sr^{-i}$, consequently $(sr^i)^2 = ssr^{-i}r^i = s^2 r^{-i+i} = ee = e$, which is what is required.

   Finally we need to show that D_{2n} is generated by the two elements s and sr, both of which have order two. That they both have order two follows from the previous paragraph. Also every element of D_{2n} can be written as a product of r, s, r^{-1}, s^{-1}, and since $r = s^{-1}(sr)$, we see that every element can be written as a product of $s, (sr), s^{-1}, (sr)^{-1}$. This establishes that D_{2n} is generated by s and sr.

3. **1.2.10 on page 28** Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Prove that $|G| = 24$.

   We may move a face to any one of the other 6 faces. Once a face is fixed we may rotate through it through $\pi/2$, which gives another 4 possibilities, and then we can no longer perform anymore motions. Therefore $|G| = 6 * 4 = 24$.

   Remark: if you were allowed to do the rigid motions in $\mathbb{R}^4$, then you could do a reflection and the answer would be instead 48.

4. **1.3.2 on page 33** (first three permutations only). Let σ be the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix}$$

   and let τ be the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{pmatrix}.$$

Find the cycle decompositions of each of the following permutations: σ, τ, σ^2.

$\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$
$\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$
$\sigma^2 = (1\ 5)(13\ 10)\ (3\ 8\ 15)(4\ 11\ 12)(14\ 7\ 9)$

5. **1.3.19 on page 34** Find all numbers n such that S_7 contains an element of order n.

   We have the following table, where we have listed all possible cycle shapes for elements of S_7 with the corresponding orders.

(1)	1	(1 2)(3 4 5)	6
(1 2)	2	(1 2)(3 4 5 6)	4
(1 2 3)	3	(1 2)(3 4 5 6 7)	10
(1 2 3 4)	4	(1 2 3)(4 5 6)	3
(1 2 3 4 5)	5	(1 2 3)(4 5 6 7)	12
(1 2 3 4 5 6)	6	(1 2)(3 4)(5 6)	2
(1 2 3 4 5 6 7)	7	(1 2)(3 4)(5 6 7)	6
(1 2)(3 4)	2		

   Thus the orders of the elements of S_7 are 1,2,3,4,5,6,7,10,12.

6. **1.4.3 on page 35** Show that $\mathrm{GL}_2(\mathbb{F}_2)$ is nonabelian.

   Let $a = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$ and $b = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$. Note that $a, b \in \mathrm{GL}_2(\mathbb{F}_2)$. Since $ab = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}$ and $ba = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$, it follows that $ab \neq ba$ and we have proved that $\mathrm{GL}_2(\mathbb{F}_2)$ is nonabelian.

Third Homework Solutions

1. 1.5.2 on page 36. Write out the group table for Q_8.

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	$-i$	i
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

2. 1.6.7 on page 40. Prove that D_8 and Q_8 are not isomorphic.

   The group D_8 has one element of order 1, two elements of order 4, and five elements of order 2. In fact if we write $D_8 = \{r,s \mid r^4 = s^2 = e, rs = sr^{-1}\}$, so that the elements of D_8 are r^i and sr^i where $i = 0,1,2,3$, then r^0 has order 1, r and r^3 have order 4, and sr^i (for $i = 0,1,2,3$) and r^2 have order 2. On the other hand Q_8 has one element of order 1, one element of order 2 (namely -1), and six elements of order 4. If D_8 and Q_8 were isomorphic, then they would have the same number of elements of order 2 (and also the same number of elements of order 4); since this is not the case, we see that D_8 and Q_8 are not isomorphic.

   It is worth remarking that although D_8 and Q_8 are not isomorphic, the sets of numbers n for which they have an element of order n are the same, namely the set whose elements are 1,2,4.

3. 1.7.14 on page 45. Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g,a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

   The second axiom $1.a = a$ is certainly true; however the first axiom fails if G is non-abelian. To be an action, we require $(hg) \cdot a = h \cdot (g \cdot a)$ for all $g,h \in G$ and $a \in A$, that is $a(hg) = (ag)h$. However this is true if and only if $hg = gh$ for all $g,h \in G$, so we do not have an action if G is nonabelian.

4. 2.2.3 on page 52. Prove that if A and B are subsets of the group G with $A \subseteq B$, then $\mathrm{C}_G(B)$ is a subgroup of $\mathrm{C}_G(A)$.

   The centralizer of any subset is always a subgroup, so we only need to prove containment. Let $x \in \mathrm{C}_G(B)$. This means that x commutes with all elements of B. Since $A \subseteq B$, we immediately see that x commutes with all elements of A and we conclude that $x \in \mathrm{C}_G(A)$ as required.

Fourth Homework Solutions

1. 2.3.6 on page 60. In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \overline{a} \rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

   Since 48 = 3 *16, 3 has two divisors and 16 has five divisors, we see that there are 2*5 = 10 subgroups.

   $\langle \overline{0} \rangle = \{\overline{0}\}$ Order 1

   $\langle \overline{1} \rangle = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{47}\}$ order 48

   $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \ldots, \overline{46}\}$ order 24

   $\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \ldots, \overline{45}\}$ order 16

   $\langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}, \ldots, \overline{44}\}$ order 12

   $\langle \overline{6} \rangle = \{\overline{0}, \overline{6}, \overline{10}, \ldots, \overline{42}\}$ order 8

   $\langle \overline{8} \rangle = \{\overline{0}, \overline{8}, \overline{12}, \ldots, \overline{40}\}$ order 6

   $\langle \overline{12} \rangle = \{\overline{0}, \overline{12}, \overline{24}, \overline{36}\}$ order 4

   $\langle \overline{16} \rangle = \{\overline{0}, \overline{16}, \overline{32}\}$ order 3

   $\langle \overline{24} \rangle = \{\overline{0}, \overline{24}\}$ order 2

   Then we have
   $\langle \overline{1} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{11} \rangle = \langle \overline{13} \rangle = \langle \overline{17} \rangle = \langle \overline{19} \rangle = \langle \overline{23} \rangle = \langle \overline{25} \rangle = \langle \overline{29} \rangle = \langle \overline{31} \rangle = \langle \overline{35} \rangle = \langle \overline{37} \rangle = \langle \overline{41} \rangle = \langle \overline{43} \rangle = \langle \overline{47} \rangle$

   $\langle \overline{2} \rangle = \langle \overline{10} \rangle = \langle \overline{14} \rangle = \langle \overline{22} \rangle = \langle \overline{26} \rangle = \langle \overline{34} \rangle = \langle \overline{38} \rangle = \langle \overline{46} \rangle$

   $\langle \overline{3} \rangle = \langle \overline{9} \rangle = \langle \overline{15} \rangle = \langle \overline{21} \rangle = \langle \overline{27} \rangle = \langle \overline{33} \rangle = \langle \overline{39} \rangle = \langle \overline{45} \rangle$

   $\langle \overline{4} \rangle = \langle \overline{20} \rangle = \langle \overline{28} \rangle = \langle \overline{44} \rangle$

   $\langle \overline{6} \rangle = \langle \overline{18} \rangle = \langle \overline{30} \rangle = \langle \overline{42} \rangle$

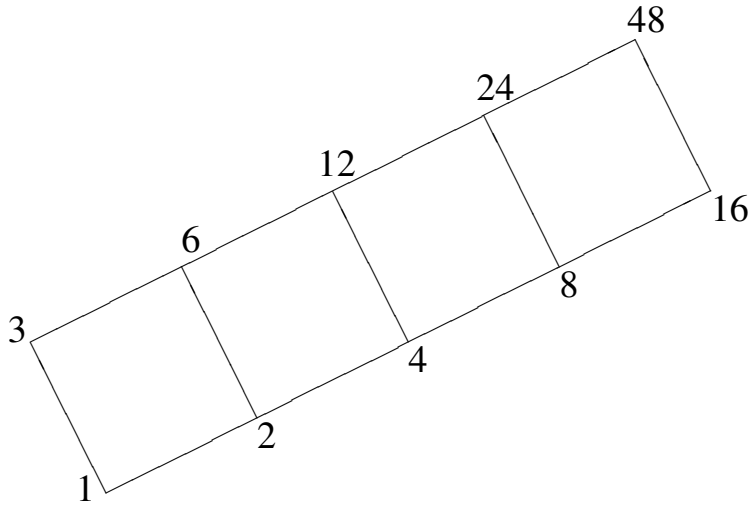
   $\langle \overline{8} \rangle = \langle \overline{40} \rangle$

   $\langle \overline{12} \rangle = \langle \overline{36} \rangle$

   $\langle \overline{16} \rangle = \langle \overline{32} \rangle$

   $\langle \overline{0} \rangle, \langle \overline{24} \rangle$ are on their own.

   The lattice of subgroups looks like (where we have labeled each subgroup with its order)



2. 2.4.3 on page 65. Prove that if H is an abelian subgroup of a group G, then $\langle H, \mathrm{Z}(G)\rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, \mathrm{C}_G(H)\rangle$ is not abelian.

   Set $Z = \mathrm{Z}(G)$. Then from the ungraded HW of February 15, every element of $\langle H, \mathrm{Z}(G)\rangle$ can be written in the form hx where $h \in H$ and $x \in \mathrm{Z}(G)$. Suppose we have two elements hx and ky of $\langle H, \mathrm{Z}(G)\rangle$; we need to prove that they commute. This is indeed the case because

   $$(hx)(ky) = hkxy = khxy = (kx)(hy).$$

   For the explicit example, one possibility is $H = 1$ and $G = S_3$. Then $\mathrm{C}_G(H) = G$, because in any group, then centralizer of the trivial subgroup 1 is the whole group. Thus in this case $\langle H, C_G(H)\rangle = S_3$, which is nonabelian.

3. Since θ and ϕ are reflections, they have order 2, consequently $|\langle\theta\rangle| = |\langle\phi\rangle| = 2$. Finally we show that $\theta\phi$ has infinite order; since $\theta\phi \in \langle\theta, \phi\rangle$, this will immediately imply that $\langle\theta, \phi\rangle$ also has infinite order. The formulae for θ and ϕ are $\theta(x,y) = (-x,y)$ and $\phi(x,y) = (2-x,y)$. Therefore $\theta\phi(x,y) = (x-2,y)$, which is translation of 2 to the left. It follows that $\theta\phi$ has infinite order as required.

4. 3.1.24 on page 88. Prove that if $N \lhd G$, then $N \cap H \lhd H$.

   Certainly $N \cap H \leq H$ (the intersection of any number of subgroups is a subgroup). We need to prove normality, so let $h \in H$ and $x \in N \cap H$. Then $hxh^{-1} \in N$ because $N \lhd G$, and $hxh^{-1} \in H$ because $h, x \in H \leq G$. Therefore $hxh^{-1} \in N \cap H$ for all $h \in H$ and $x \in N \cap H$ and it follows that $N \cap H \lhd H$ as required.

January 19, Ungraded Homework

Exercise 1.1.5 on page 21 Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \ldots, \overline{n-1}\}$. Suppose $\mathbb{Z}/n\mathbb{Z}$ is a group. Then it must have an identity e. We now have $e = e\bar{1} = \bar{1}$, so the identity is $\bar{1}$. Let x be the inverse for $\bar{0}$. Then $e = x\bar{0} = \bar{0}$. We conclude that $\bar{1} = \bar{0}$, which is a contradiction, unless $n = 1$.

Exercise 1.1.8 on page 22 Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

(b) Prove that G is not a group under addition.

(a) Note that multiplication defines a binary operation on G, because if $x, y \in G$, then $x^m = 1$ and $y^n = 1$ for some $m, n \in \mathbb{Z}^+$, and then we have $(xy)^{mn} = 1$, which shows that $xy \in G$. Also multiplication is associative and the identity is 1; note that $1 \in G$. Finally if $z \in G$, then it has an inverse z^{-1}; again note that $z^{-1} \in G$ because if $z^n = 1$, then $(z^{-1})^n = (z^n)^{-1} = 1$.

(b) Suppose G is a group under addition. Let $e \in G$ be the identity. Then $e + 1 = 1$, so $e = 0$. But $0 \notin G$ and we have the required contradiction.

Exercise 1.1.15 on page 22 Prove that $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$ for all $a_1, \ldots, a_n$ in the group G.

Let $x = a_1 a_2 \ldots a_n$ and $y = a_n^{-1} \ldots a_1^{-1}$. We need to prove that $y = x^{-1}$, equivalently $xy = yx = e$. However

$$\begin{aligned} xy &= a_1 a_2 \ldots a_n a_n^{-1} \ldots a_1^{-1} \\ &= a_1 a_2 \ldots a_{n-1} a_{n-1}^{-1} \ldots a_1^{-1} \\ &= a_1 a_2 \ldots a_{n-2} a_{n-2}^{-1} \ldots a_1^{-1} = \cdots = e. \end{aligned}$$

Similarly $yx = e$ and the result is proven.

Remark In a group, $xy = e$ implies $yx = e$, but this is not true in general (i.e. if we are not working in a group).

Exercise 1.1.12 on page 22 Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$.

$(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. The orders are 1,2,2,2 respectively; for example $\overline{5}$ has order 2 because $\overline{5} \neq \overline{1}$, yet $\overline{5}^2 = \overline{25} = \overline{1}$. Finally note that $\overline{-1} = \overline{11}$, $\overline{-7} = \overline{5}$.

Exercise 1.1.30 on page 23 Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

$(a,1)(1,b) = (a,b) = (1,b)(a,1)$, so $(a,1)$ and $(1,b)$ commute. Let $p = |a|$, $q = |b|$, $l = [p,q]$. Then

$$(a,b)^l = (a^l, b^l) = ((a^p)^{l/p}, (b^q)^{l/q}) = (1^{l/p}, 1^{l/q}) = (1,1) = 1.$$

This shows that the order of (a,b) divides l. On the other hand if m is a positive integer and $(a,b)^m = 1$, then $a^m = b^m = 1$, consequently $p,q \Big| m$. Therefore $l \Big| m$ and we are finished.

January 24, Ungraded Homework

Exercise 1.2.1 on page 27 Compute the orders of each of the elements in the following groups.

(a) D_6

(b) D_8

(c) D_{10}

We shall only give details for D_{10}.

(a) 1 has order 1; r, r^2 have order 3; and s, sr, sr^2 have order 2.

(b) 1 has order 1; r, r^3 have order 4; r^2 and s, sr, sr^2, sr^3 have order 2.

(c) 1 has order 1; r, r^2, r^3, r^4 have order 5; and s, sr, sr^2, sr^3, sr^4 have order 2.

Recall that every element of D_{10} can be written uniquely in the form $s^i r^j$ where $i = 0, 1$ and $j = 0, 1, 2, 3, 4$. The order of 1 being 1 is obvious. Also $(r^i)^5 = r^{5i} = (r^5)^i = 1^i = 1$, so the order of r^i divides 5. Since 5 is a prime number, it follows that if $i = 1, 2, 3, 4$, then the order of r^i is 5. Next $sr^i \neq 1$ $(i = 0, 1, 2, 3, 4)$, so if we can prove that $(sr^i)^2 = 1$, then it would follow that $|sr^i| = 2$ and we would be finished. However by using $rs = sr^{-1}$ i-times,

$$(sr^i)^2 = s(r^i s)r^i = ssr^{-i}r^i = s^2 = 1$$

as required.

Exercise 1.2.2 on page 27 Use generators and relations to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Recall that every element of D_{2n} can be written in the form r^i or sr^i. Therefore we may assume that $x = sr^i$. Then

$$rx = rsr^i = sr^{-1}r^i = sr^{i-1} = sr^i r^{-1} = xr^{-1}.$$

Exercise 1.2.9 on page 28 Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Let A, B, C, D denote the vertices of the tetrahedron. Obviously any symmetry must send vertices to vertices, and also any symmetry is determined by its affect on the vertices of the tetrahedron. By rotating about the line through D perpendicular to the face ABC, we see that we can send A to A, B or C, and then by rotating about another line which goes through a vertex and is perpendicular to the opposite face, we see that we can send A to D as well.

Once the position of A is decided, B can be sent to 3 possible vertices (it cannot be sent to where A is). Once the positions of A and B are determined, then so are the positions of C and D, and hence of the whole tetrahedron. (Note however if we could go into four dimensions, then a reflection in the plane which goes through AB and the midpoint of CD would interchange C and D; however this cannot be brought about by moving the tetrahedron in three dimensions). Thus G has order $4*3=12$.

Exercise 2.1.1 on page 48 Let G be a group. In each of (a)–(e) prove that the specified subset is a subgroup of the given group.

(a) the set of complex numbers of the form $a+ai$, $a \in \mathbb{R}$ (under addition)

(b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)

(c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)

(d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)

(e) the set of nonzero real numbers whose square is a rational number (under multiplication).

Let G denote the relevant set which needs to be shown a subgroup.

(a) If $x,y \in G$, then we may write $x=a+ai$, $y=b+bi$ where $a,b \in \mathbb{R}$ and we have $x+y=(a+b)+(a+b)i$, which shows that addition is a binary operation (we have closure). Also addition is associative. The identity is 0 and the inverse of x is $-a+(-a)i$.

(b) If $x,y \in G$, then $|xy|=|x||y|=1*1=1$, so multiplication is a binary operation. Also multiplication is associative and the identity is 1. Finally the inverse of x is $1/x$ (note that $1/x \in G$ because $|1/x|=1/|x|=1$).

(c) Let $x,y \in G$. Then we may write $x=a/n$, $y=b/n$ where $a,b \in \mathbb{Z}$, and we have $x+y=a/n+b/n=(a+b)/n$, which shows that $x+y \in G$. Thus we have closure, and addition is a binary operation. Addition is associative and the identity is $0=0/n$. Finally the inverse of x is $-a/n$, which is also in G.

(d) Let $x,y \in G$. Then we may write $x=a/p$, $y=b/q$, where $p,q \in \mathbb{Z}$ are prime to n. We now have $x+y=(aq+bp)/pq$, which shows that $x+y \in G$ because pq is prime to n. Thus we have closure and we see that addition is an associative binary operation. The identity is $0=0/1$. Finally the inverse of x is $-a/p$, which is also in G.

(e) Let $x,y \in G$. Then $x^2 \in \mathbb{Q}$ and $y^2 \in \mathbb{Q}$, consequently $(xy)^2 \in \mathbb{Q}$ and we see that $xy \in G$. It follows that multiplication is an associative binary operation on G. The identity is 1, and the inverse of x is $1/x$ (note that if $x \neq 0$, then $x^2 \in \mathbb{Q} \Rightarrow (1/x)^2 \in \mathbb{Q}$).

Exercise 2.1.8 on page 48 Let H and K be subgroups of the group G. Prove that $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

First suppose $H \cup K$ is a subgroup and that there exists $h \in H \setminus K$ and $k \in K \setminus H$. Then $h, k \in H \cup K$, so $hk \in H \cup K$. On the other hand if $hk \in H$, then $k = h^{-1}(hk) \in H$, which is not true and we see that $hk \notin H$. Similarly $hk \notin K$. We now have a contradiction and we conclude that if $H \cup K$ is a subgroup, then either $H \subseteq K$ or $K \subseteq H$.

If either $H \subseteq K$ or $K \subseteq H$, then $H \cup K = K$ or H, in which case it is obvious that $H \cup K$ is a subgroup.

January 26, Ungraded Homework

Exercise 1.3.1 on page 32 Let σ be the permutation

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1.$$

Find the cycle decomposition of each of the following permutations σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

First we obtain the cycle decomposition for σ. We have $\sigma 1 = 3$, $\sigma 3 = 5$ and $\sigma 5 = 1$, which yields the cycle (1 3 5); and $\sigma 2 = 4$ and $\sigma 4 = 2$, which yields the cycle (2 4). Therefore the cycle decomposition of σ (i.e. σ written as a product of *disjoint* cycles) is (1 3 5)(2 4).

Next we find the cycle decomposition of τ. We have $\tau 1 = 5$ and $\tau 5 = 1$, which yields the cycle (1 5), and $\tau 2 = 3$ and $\tau 3 = 2$, which yields the cycle (2 3), and $\tau 4 = 4$, which yields the cycle (4). Normally one omits the 1-cycles. Therefore the cycle decomposition of τ is (1 5)(2 3).

The calculation of the cycle decompositions of the other elements can be facilitated by using the cycle decompositions of σ and τ from above. Thus σ^2 = (1 5 3), $\sigma\tau$ = (2 5 3 4), $\tau\sigma$ = (1 2 4 3), and (note $\tau^2 = e$) $\tau^2\sigma = \sigma$ = (1 3 5)(2 4).

Exercise 1.3.3 on page 33 Find the orders of the permutations computed in the previous exercise.

If a permutation is a product of disjoint cycles of lengths $\ell_1, \ldots, \ell_n$, then its order is the lowest common multiple $[\ell_1, \ldots, \ell_n]$ of these lengths. Thus σ has order $[3,2] = 6$, τ has order $[2,2]$, σ^2 has order 3, $\sigma\tau$ has order 4, $\tau\sigma$ has order 4, $\tau^2\sigma$ has order 6.

Exercise 1.3.5 on page 33 Find the order of (1 12 8 10 4)(2 13)(5 11 7)(6 9).

Since this element is written as a product of disjoint cycles, we may apply Exercise 1.3.15 on page 33. The answer is the lowest common multiple of 5,2,3,2 which is 30.

Exercise 1.3.9 on page 33 Let σ = (1 2 3 4 5 6 7 8 9 10 11 12), τ = (1 2 3 4 5 6 7 8), ω = (1 2 3 4 5 6 7 8 9 10 11 12 13 14). For which positive integers i is σ^i a 12-cycle, τ^i an 8-cycle, ω^i a 14-cycle?

First consider σ, which we may view as an element of S_{12}. Suppose $(i,12) = 1$ (that is, i is prime to 12). Then there exists $j \in \mathbb{Z}$ such that $ij \equiv 1 \mod 12$, so $ij = 1 + 12r$ for some $r \in \mathbb{Z}$. Then

$$(\sigma^i)^j = \sigma^{ij} = \sigma^{1+12r} = \sigma(\sigma^{12})^r = \sigma.$$

Since σ is a 12-cycle and $\sigma^i \in S_{12}$, it must be true that σ^i is also a 12-cycle (if you take a power of a permutation, here the j th power of σ^i, you cannot get longer cycles).

Conversely suppose $(i,12) \neq 1$, say $n \geq 2$ divides i and 12. Then

$$(\sigma^i)^{12/n} = \sigma^{12i/n} = (\sigma^{12})^{i/n} = 1^{i/n} = 1.$$

This tells us that the order of σ^i is at most $12/n$, so σ^i is not a 12-cycle (a 12-cycle has order 12). So the answer is that σ^i is a 12-cycle if and only if i is prime to 12 (this is OK even if $i \leq 0$).

The solution for τ and ω is similar; the answer is that τ^i is an 8-cycle if and only if $(i,8) = 1$, and that ω^i is a 14-cycle if and only if $(i,14) = 1$.

Exercise 1.3.15 on page 33 Prove that the order of an element in S_n is the lowest common multiple of the lengths of the cycles in its cycle decomposition.

Let π be the element in S_n, and let l indicate the lowest common multiple of the lengths of its cycles. Let $\gamma_1, \ldots, \gamma_r$ be these cycles. Then $\gamma_i^l = 1$ for all i and since the γ_i commute (here it is important that the γ_i commute) we have

$$\pi^l = \gamma_1^l \ldots \gamma_r^l = 1.$$

Therefore $|\pi| \leq l$. Conversely suppose $\pi^m = 1$ where $m \in \mathbb{Z}^+$. Then $\gamma_1^m \ldots \gamma_r^m = 1$. Moreover the numbers which the γ_i move are mutually disjoint, so the same is true of the γ_i^m, consequently we must have $\gamma_i^m = 1$ for all i. This shows that $m \geq l$ and we are finished.

Exercise 1.3.18 on page 34 Find all numbers n such that S_5 contains an element of order n. Again we use Exercise 1.3.15 on page 33. The method is to find all possible shapes for cycle decompositions of elements of S_5 We will omit all 1-cycles except in the case of the identity element, since these don't affect the permutation. Then the possible cycle decompositions are a 1-cycle, a 2-cycle, a 3-cycle, a 4-cycle, a 5-cycle, a 2-cycle times a 2-cycle, and a 2-cycle times a 3-cycle. The corresponding orders are 1,2,3,4,5,2,6. Therefore the numbers n for which S_n contains an element of order n are 1,2,3,4,5,6.

Exercises 1.4.1,2 on page 35 Prove that $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$, write out the elements of $\mathrm{GL}_2(\mathbb{F}_2)$, and compute the order of each element.

The group $\mathrm{GL}_2(\mathbb{F}_2)$ consists of 2 by 2 matrices which have entries in $\mathbb{Z}/2\mathbb{Z}$ and nonzero determinant, with the binary operation matrix multiplication. The identity of the group is the identity 2 by 2 matrix. We now write out the elements of the group and the corresponding orders (and of course, this also shows that $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$).

$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$ which has order 1,

$\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$ which has order 2,

$\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$ which has order 2,

$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{pmatrix}$ which has order 2,

$\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$ which has order 3,

$\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}$ which has order 3.

Exercise 1.5.1 on page 36 Compute the order of each of the elements in Q_8.

The order of 1 is 1, the order of -1 is 2, and the order of the other six elements is 4. We will just show that the order of i is 4. We have $i \neq 1$, $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$, $i^4 = (i^2)^2 = (-1)^2 = 1$. Thus i has order 4.

Exercise 1.6.1 on page 39 Let $\phi : G \to H$ be a homomorphism.

(a) Prove that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}^+$.

(b) Do part (a) for $n = -1$ and deduce that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}$.

(a) We prove this by induction on n; it is certainly true for $n = 1$. If it is true for $n = m$, then we know $\phi(x^m) = \phi(x)^m$, so

$$\phi(x^{m+1}) = \phi(x^m x) = \phi(x^m)\phi(x) = \phi(x)^m \phi(x) = \phi(x)^{m+1}.$$

This establishes the induction step and the result follows.

(b) We have

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

Therefore $\phi(x)^{-1} = \phi(x^{-1})$. To prove that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}$: this has been done for $n \in \mathbb{Z}^+$ in part(a), while for $n = 0$ both sides are e. Finally for $n < 0$, we have $-n \in \mathbb{Z}^+$, consequently

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

Exercise 1.6.2 on page 39 If $\phi : G \to H$ is an isomorphism, prove that $|\phi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if ϕ is only assumed to be a homomorphism?

Let $n = |x|$. Then

$$\phi(x)^n = \phi(x^n) = \phi(e) = e.$$

This shows that $|\phi(x)|$ divides n. Since ϕ is an isomorphism, it is bijective and therefore has an inverse, say θ, and θ will also be an isomorphism. Thus by replacing ϕ with θ and x with $\phi(x)$ in the above argument, we see that $|\theta(\phi(x))|$ divides $|\phi(x)|$, so n divides $|\phi(x)|$ because $\theta\phi(x) = x$. We conclude that $|\phi(x)| = n$ as required. It immediately follows that G and H have the same number of elements of order n for each $n \in \mathbb{Z}^+$.

If ϕ is only assumed to be a homomorphism, this is false in general. For example define $\phi: G \to H$ by $\phi(g) = e$ for all $g \in G$, and let $e \neq x \in G$. Then $|\phi(x)| = 1$ and $|x| \neq 1$.

Exercise 1.6.8 on page 40 Prove that if $n \neq m$, then S_n and S_m are not isomorphic.

$|S_n| = n!$ and $|S_m| = m!$, so if $n \neq m$ the two groups have different orders and so are not isomorphic.

Exercise 1.6.9 on page 40 Prove that D_{24} and S_4 are not isomorphic.

D_{24} has an element of order 12, namely r, which is rotation through $\pi/6$. On the other hand the elements of S_4 have order 1, 2, 3 or 4. This proves that D_{24} and S_4 are not isomorphic (the orders of elements of isomorphic groups are the same).

Exercise 1.7.8 on page 44 Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.

(a) Prove that this is a group action.

(b) Describe explicitly how the elements (1 2) and (1 2 3) act on the six 2-element subsets of $\{1,2,3,4\}$.

(a) Let $g, h \in S_A$. Then

$$\begin{aligned} g \cdot (h \cdot \{a_1, \ldots, a_k\}) &= g \cdot \{h(a_1), \ldots, h(a_k)\} = \{gh(a_1), \ldots, gh(a_k)\} \\ &= gh \cdot \{a_1, \ldots, a_k\} \end{aligned}$$

and

$$1 \cdot \{a_1, \ldots, a_k\} = \{1(a_1), \ldots, 1(a_k)\} = \{a_1, \ldots, a_k\}.$$

This proves that the above defines a group action.

(b) (1 2) induces the permutation
$(\{1\ 3\}\{2\ 3\})\ (\{1\ 4\}\{2\ 4\})$
(1 2 3) induces the permutation $(\{1\ 2\}\{2\ 3\}\{1\ 3\})(\{1\ 4\}\{2\ 4\}\{3\ 4\})$

Exercise 1.7.15 on page 45 Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action of G onto itself.

For $g, h \in G$, we have

$$g \cdot (h \cdot a) = g(ah^{-1}) = (ah^{-1})g^{-1} = a(gh)^{-1} = gh \cdot a$$

and $1 \cdot a = a(1^{-1}) = a$. This proves that we have a group action.

Exercise 2.1.2 on page 48 In each of (a)–(e) prove that the specified subset is *not* a subgroup of the given group:

(a) the set of 2-cycles in S_n for $n \geq 3$

(b) the set of reflections in D_{2n} for $n \geq 3$

(c) for n a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G \mid |x| = n\} \cup \{1\}$

(d) the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0

(e) the set of real numbers whose square is a rational number (under addition).

(a) (1 2)(2 3) = (1 2 3) which shows that the set is not closed under multiplication.

(b) Using the notation of the text book, we have $s(sr) = r$, so the product of the two reflections s, sr is a rotation, which is not a reflection.

(c) Write $n = pq$ where $1 < p, q \in \mathbb{Z}$ and let $x \in G$ be an element of order n. Then $x^p \neq 1$ and x^p has order q.

(d) Assuming the operation is addition, 1+1=2 shows that closure fails.

(e) $(\sqrt{2} + \sqrt{3})^2 \notin \mathbb{Q}$, so closure fails.

January 31, Ungraded Homework

Exercise 2.2.1 on page 52 Prove that $\mathrm{C}_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

By definition, $g \in \mathrm{C}_G(A)$ if and only if $gag^{-1} = a$ for all $a \in A$. Multiplying on the left by g^{-1} and on the right by g, we see that this is if and only if $a = g^{-1}ag$, which yields the required result.

Exercise 2.2.2 on page 52 Prove that $\mathrm{C}_G(\mathrm{Z}(G)) = G$ and deduce that $\mathrm{N}_G(\mathrm{Z}(G)) = G$.

Let $g \in G$. Then by definition of center, $gx = xg$ for all $x \in \mathrm{Z}(G)$. Therefore $g \in \mathrm{C}_G(\mathrm{Z}(G))$ and we have proven that $G \subseteq \mathrm{C}_G(\mathrm{Z}(G))$. The reverse inclusion, namely $\mathrm{C}_G(\mathrm{Z}(G)) \subseteq G$ is obvious, and it follows that $\mathrm{C}_G(\mathrm{Z}(G)) = G$, as required. Since the centralizer is always contained in the normalizer, we now see immediately that $\mathrm{N}_G(\mathrm{Z}(G)) = G$.

Exercise 2.2.5 on page 52 In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $\mathrm{C}_G(A) = A$ and $\mathrm{N}_G(A) = G$.

(a) $G = S_3$ and $A = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$.

(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.

(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

(a) Since the elements of A commute between themselves, we certainly have $A \subseteq \mathrm{C}_G(A)$. Thus to verify $\mathrm{C}_G(A) = A$, we need to show that each 2-cycle of G is not in $\mathrm{C}_G(A)$. Since $(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (1\ 3\ 2)$, this is indeed the case for $(1\ 2)$, and the argument for the other two 2-cycles is exactly similar. For $\mathrm{N}_G(A)$, we need to show $gAg^{-1} = A$ for all $g \in G$. For example with $g = (1\ 2)$, we have

$$\begin{aligned} g1g^{-1} &= (1\ 2)1(1\ 2)^{-1} = 1 \\ g(1\ 2\ 3)g^{-1} &= (1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (1\ 3\ 2) \\ g(1\ 3\ 2)g^{-1} &= (1\ 2)(1\ 3\ 2)(1\ 2)^{-1} = (1\ 2\ 3) \end{aligned}$$

so we are OK with $g = (1\ 2)$. We do a similar calculation with the other six possibilities. On the other hand our calculation is simplified if we use the result that for all $g \in S_n$ and $m \leq n$,

$$g(1\ 2\ \ldots\ m)g^{-1} = (g1\ g2\ \ldots\ gm);$$

in particular applying $g \ldots g^{-1}$ yields a permutation with the same cycle shape.

(b) As in (a), the elements of A commute between themselves, so we have $A \subseteq \mathrm{C}_G(A)$. For $\mathrm{N}_G(A)$, we need to show $gAg^{-1} = A$ for all $g \in G$. For example with $g = r$,

$$\begin{aligned} g1g^{-1} &= r1r^{-1} = 1 \\ gsg^{-1} &= rsr^{-1} = sr^2 \\ gr^2g^{-1} &= rr^2r^{-1} = r^2 \\ gsr^2g^{-1} &= rsr^2r^{-1} = s \end{aligned}$$

so we are OK with $g = r$. We do a similar calculation with the other seven possibilities for g (of course this calculation is particular simple in the case $g = 1$).

(c) This is similar to (b); however the calculations can be simplified considerably if we assume the theorem that every subgroup of index 2 is normal, which we will cover soon in class. Since $|A| = 5$ and $|D_{10}| = 10$, we see that A has index 2 in G and hence $A \lhd G$. Therefore $\mathrm{N}_G(A) = G$. Since the elements of A commute among themselves, we certainly have $A \subseteq \mathrm{C}_G(A)$. Suppose sr^i commutes with r. Then $sr^i r = rsr^i = sr^{-1}r^i$ and we see that $r^2 = 1$, which is not the case. Therefore $sr^i \notin \mathrm{C}_G(A)$ for all i and we deduce that $\mathrm{C}_G(A) = A$, as required.

Exercise 2.2.10 on page 53 Let H be a subgroup of order 2 in G. Show that $\mathrm{N}_G(H) = \mathrm{C}_G(H)$. Deduce that if $\mathrm{N}_G(H) = G$, then $H \leq \mathrm{Z}(G)$.

We always have $\mathrm{C}_G(H) \subseteq \mathrm{N}_G(H)$. Conversely suppose $g \in \mathrm{N}_G(H)$. Since $|H| = 2$, we may write $H = \{1, x\}$ where $1 \neq x \in H$. If $h \in H$, then $h = 1$ or x. If $h = 1$, then obviously $ghg^{-1} = 1 = h$. On the other hand if $h = x$, then $ghg^{-1} = 1$ or x because $g \in \mathrm{N}_G(H)$. But if $gxg^{-1} = 1$, then by multiplying on the left by g^{-1} and on the right by g, we obtain $x = 1$ which is a contradiction. Therefore $gxg^{-1} = x$ and we conclude that $ghg^{-1} = h$ for all $h \in H$. This finishes the proof that $\mathrm{C}_G(H) = \mathrm{N}_G(H)$. Finally if in addition $\mathrm{N}_G(H) = G$, then we see that $\mathrm{C}_G(H) = G$, so $ghg^{-1} = h$ for all $g \in G$ and $h \in H$. This shows that $h \in \mathrm{Z}(G)$ for all $h \in H$ and we have proven that $H \leq \mathrm{Z}(G)$ as required.

February 2, Ungraded Homework

Exercise 2.3.1 on page 60 Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

The problem is equivalent to finding all the subgroups and containments between them for $\mathbb{Z}/45\mathbb{Z}$. For each positive integer n dividing 45, there is a unique subgroup of order n; this subgroup is $\langle \overline{45/n} \rangle$, the cyclic group with generator $\overline{45/n}$. Therefore the subgroups of $\mathbb{Z}/45\mathbb{Z}$ are $\langle \overline{1} \rangle$, $\langle \overline{3} \rangle$, $\langle \overline{5} \rangle$, $\langle \overline{9} \rangle$, $\langle \overline{15} \rangle$, $\langle \overline{45} \rangle$.

For the containments, we have $\langle \overline{a} \rangle \subseteq \langle \overline{b} \rangle$ if and only if $b \big| a$ (this only works when $a, b \big| 45$). Thus we have

$\langle \overline{45} \rangle$ is contained in $\langle \overline{1} \rangle$, $\langle \overline{3} \rangle$, $\langle \overline{5} \rangle$, $\langle \overline{9} \rangle$, $\langle \overline{15} \rangle$, $\langle \overline{45} \rangle$.
$\langle \overline{15} \rangle$ is contained in $\langle \overline{1} \rangle$, $\langle \overline{3} \rangle$, $\langle \overline{5} \rangle$, $\langle \overline{15} \rangle$.
$\langle \overline{9} \rangle$ is contained in $\langle \overline{1} \rangle$, $\langle \overline{3} \rangle$, $\langle \overline{9} \rangle$.
$\langle \overline{5} \rangle$ is contained in $\langle \overline{1} \rangle$, $\langle \overline{5} \rangle$.
$\langle \overline{3} \rangle$ is contained in $\langle \overline{1} \rangle$, $\langle \overline{3} \rangle$.
$\langle \overline{1} \rangle$ is contained in $\langle \overline{1} \rangle$.

For the cyclic subgroup of order 45 with generator x, replace $\overline{n}$ with x^n everywhere. Thus, for example, the subgroups of $\langle x \rangle$ are $\langle x \rangle$, $\langle x^3 \rangle$, $\langle x^5 \rangle$, $\langle x^9 \rangle$, $\langle x^{15} \rangle$, $\langle x^{45} \rangle$. The last one is of course 1 (the subgroup consisting of just the identity).

Exercise 2.3.3 on page 60 Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

$\mathbb{Z}/48\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{47}\}$. Also $\overline{a}$ is a generator of $\mathbb{Z}/48\mathbb{Z}$ if and only if $|\overline{a}| = 48$, and $|\overline{a}| = 48/(48,a)$. Thus $\overline{a}$ is a generator of $\mathbb{Z}/48\mathbb{Z}$ if and only if $(a,48) = 1$. Therefore the generators of $\mathbb{Z}/48\mathbb{Z}$ are

$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$	$\overline{13}$	$\overline{17}$	$\overline{19}$	$\overline{23}$
$\overline{25}$	$\overline{29}$	$\overline{31}$	$\overline{35}$	$\overline{37}$	$\overline{41}$	$\overline{43}$	$\overline{47}$

Exercise 2.3.10 on page 60 What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements and their orders in $\langle \overline{30} \rangle$.

The order of $\overline{1}$ in $\mathbb{Z}/54\mathbb{Z}$ is 54. Since $\overline{30} = \overline{1}^{30}$, we see that (see Proposition 5 on page 57) that $|\overline{30}| = 54/(54,30)$. The greatest common divisor of 54 and 30 is 6, hence the order of $\overline{30}$ is 9.

Now we find the orders of all the elements in $\langle \overline{30} \rangle$. Since the order of $\overline{30}$ is 9 (from the previous paragraph), $|\langle \overline{30} \rangle| = 9$, which means that the elements of $\langle \overline{30} \rangle$ are $\overline{30}^0$, $\overline{30}^1$, $\overline{30}^2$, $\overline{30}^3$, $\overline{30}^4$, $\overline{30}^5$, $\overline{30}^6$, $\overline{30}^7$, $\overline{30}^8$. Remembering that the operation is modular addition, these elements are $\overline{0}$, $\overline{30}$, $\overline{6}$, $\overline{36}$, $\overline{12}$, $\overline{42}$, $\overline{18}$, $\overline{48}$, $\overline{24}$ respectively. The corresponding orders are $9/(9,0)$, $9/(9,1)$, $9/(9,2)$, $9/(9,3)$, $9/(9,4)$, $9/(9,5)$, $9/(9,6)$, $9/(9,7)$, $9/(9,8)$. Putting this altogether in a table, we obtain the following result:

element	$\overline{0}$	$\overline{30}$	$\overline{6}$	$\overline{36}$	$\overline{12}$	$\overline{42}$	$\overline{18}$	$\overline{48}$	$\overline{24}$
order	1	9	9	3	9	9	3	9	9

February 7, Ungraded Homework

Exercise 2.3.12 on page 60 Prove that the following groups are *not* cyclic.

(a) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$

(c) $\mathbb{Z} \times \mathbb{Z}$

(a) $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$, so if the group was cyclic, it would have an element of order 4. This is not the case because all nonidentity elements have order 2.

(b) Since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ is infinite, if it is also cyclic, it must be isomorphic to $\mathbb{Z}$. However the given group has an element of order 2, namely $(\bar{1}, 0)$, whereas all nonidentity elements of $\mathbb{Z}$ have infinite order.

(c) Suppose $\mathbb{Z} \times \mathbb{Z}$ is cyclic. Then it would have a generator (a,b), where $a,b \in \mathbb{Z}$. This would mean that every element of the group could be written as (na,nb) for some $n \in \mathbb{Z}$. Thus there would be $p,q \in \mathbb{Z}$ such that $(pa,pb) = (1,0)$ and $(qa,qb) = (0,1)$. The we have $pa = 1$ and $qb = 1$, so $p,q \neq 0$, and then $pb = 0$ and $qa = 0$ yields $a = b = 0$ and we have a contradiction.

Exercise 2.3.15 on page 60 Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

$\mathbb{Z} \times \mathbb{Z}$ is a subgroup of $\mathbb{Q} \times \mathbb{Q}$. From the previous problem $\mathbb{Z} \times \mathbb{Z}$ is not cyclic, which proves the result because subgroups of cyclic groups are cyclic.

Exercise 2.3.18 on page 60 Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $\mathbb{Z}/n\mathbb{Z} = \langle x \rangle$ to H such that $x \mapsto h$.

Suppose $\theta \colon \mathbb{Z}/n\mathbb{Z} \to H$ is a homomorphism with $\theta x = h$. Then $\theta(x^i) = h^i$ because θ is a homomorphism, and since every element of $\mathbb{Z}/n\mathbb{Z}$ can be written in the form x^i, we see that θ (if it exists) must be unique.

Now we must show that θ exists. We define $\theta(x^i)$ to be h^i. This is clearly a homomorphism; the only possible problem is whether θ is well defined. We need to show that if $x^i = x^j$, then the two possibilities for θ, namely h^i and h^j, are in fact the same. However if $x^i = x^j$, then $x^{i-j} = 1$, hence $n | i-j$ because x has order n. Therefore $h^{i-j} = 1$ because $h^n = 1$ and we deduce that $h^i = h^j$ as required.

Exercise 2.4.2 on page 65 Prove that if A is a subset of B, then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.

By definition, $\langle B \rangle$ is a subgroup of G which contains B and in particular contains A. Again by definition, we deduce that $\langle B \rangle$ contains $\langle A \rangle$. For the final sentence, we could let G be any group, B to be the whole of G and A to be the nonidentity elements of G. Then $\langle A \rangle = \langle B \rangle = G$.

Exercise 2.4.6 on page 65 Prove that the subgroup of S_4 generated by (1 2) and (1 2)(3 4) is a noncyclic group of order 4.

Let $H = \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$. It is easily checked that H is a subgroup of S_4. Clearly it contains (1 2) and (1 2)(3 4), and it has order 4. Finally it is noncyclic because it has no element of order 4; in fact every nonidentity element has order 2.

Exercise 3.1.1 on page 85 Let $\phi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\phi^{-1}(E) \leq G$ (i.e. the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \lhd H$, prove that $\phi^{-1}(E) \lhd G$. Deduce that $\ker\phi \lhd G$.

Since E is nonempty, it is clear that $\phi^{-1}(E)$ is also nonempty. Next let $x, y \in \phi^{-1}(E)$. Then $\phi(x), \phi(y) \in E$, hence $\phi(xy) = \phi(x)\phi(y) \in E$. Finally let $x \in \phi^{-1}(E)$. Then $\phi(x^{-1}) = \phi(x)^{-1} \in E$ and it now follows that $\phi^{-1}(E) \leq G$.

Suppose in addition that H is normal in G. Let $g \in G$ and $x \in \phi^{-1}(E)$. We need to show that $gxg^{-1} \in \phi^{-1}(E)$, equivalently that $\phi(gxg^{-1}) \in E$. Since ϕ is a homomorphism, $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1}$, and this last element is in E because $E \lhd H$ and $\phi(x) \in E$. Finally it now follows that $\ker\phi \lhd G$, because we apply the above with $E = 1$; in this situation $\ker\phi = \phi^{-1}(1)$ and 1 is certainly a normal subgroup of H.

Let G be a group and let $H \leq G$. Prove that $\langle H, \mathrm{Z}(G)\rangle = H\,\mathrm{Z}(G)$.

Set $Z = \mathrm{Z}(G)$. Note that $HZ \leq G$. This is because

(i) $1 = 11$ and $1 \in H, Z$, so $1 \in HZ$.

(ii) Let hx and $ky \in HZ$, where $h, k \in H$ and $x, y \in Z$. Since every element of Z commutes with all elements of G, $(hx)(ky) = (hk)(xy) \in HZ$, so HZ is closed under multiplication.

(iii) Let $hz \in HZ$, where $h \in H$ and $z \in Z$. Since z commutes with h, we have $(hz)^{-1} = (zh)^{-1} = h^{-1}z^{-1} \in HZ$, so HZ is closed under taking inverses.

We deduce that $HZ \supseteq \langle H, Z\rangle$. On the other hand if K is a subgroup containing H, Z, then it must contain HZ and we conclude that $\langle H, Z\rangle = HZ$.

February 9, Ungraded Homework

Exercise 3.1.4 on page 85 Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

If α is positive, this is proved by induction. The result is certainly true if $\alpha = 0$ (both sides are then the identity N); if it is true for $\alpha = s$, then we have

$$(gN)^{s+1} = (gN)(gN)^s = gN(g^sN) = g^{s+1}N$$

as required. On the other hand if α is negative, then $-\alpha$ is positive and we have

$$(gN)^\alpha = ((gN)^{-1})^{-\alpha} = (g^{-1}N)^{-\alpha} = (g^{-1})^{-\alpha}N = g^\alpha N$$

and we are finished.

Exercise 3.1.36 on page 89 Prove that if $G/\mathrm{Z}(G)$ is cyclic, then G is abelian.

Write $Z = \mathrm{Z}(G)$. If G/Z is cyclic, then $G/Z = \langle xZ \rangle$ for some $x \in G$. This means that the left cosets of Z in G are of the form x^aZ for some $a \in \mathbb{Z}$ and $z \in Z$. Therefore every element of G is of the form x^az. Suppose we have another such element, say x^bw (so $w \in Z$). Then

$$(x^az)(x^bw) = zwx^ax^b = wzx^bx^a = (wx^b)(zx^a),$$

consequently any two elements of G commute and we have proven that G is abelian.

Exercise 3.1.22(a) on page 88 Prove that if H and K are normal subgroups of a group G, then their intersection $H \cap K$ is also a normal subgroup of G.

We have already proved previously that $H \cap K$ is a subgroup of G; see Exercise 2.1.10(a) on page 48. We now need to verify the normality condition: let $g \in G$. Then $gHg^{-1} = H$ and $gKg^{-1} = K$, consequently

$$g(H \cap K)g^{-1} \subseteq gHg^{-1} \cap gKg^{-1} = H \cap K.$$

Since N is a normal subgroup of G if and only if $N \leq G$ and $gNg^{-1} \subseteq N$ for all $g \in G$, the result is proven.

Let G be a group and let $H \leq G$. Prove that the formula $g \cdot (xH) = gxH$ for $g, x \in G$ defines an action of G on the left cosets of H in G.

We should note that the formula is well defined because if $xH = yH$, then

$$g \cdot (xH) = gxH = g(xH) = g(yH) = gyH = g \cdot (yH).$$

We now have

(i) $1 \cdot (xH) = 1xH = xH$.

(ii) If $g, k \in G$, then

$$g \cdot (k \cdot xH) = g \cdot (kxH) = gkxH = (gk) \cdot (xH).$$

This shows that we have an action, as required.

February 14, Ungraded Homework

Exercise 3.1.22(a) on page 88 Prove that if H and K are normal subgroups of a group G, then their intersection $H \cap K$ is also a normal subgroup of G.

We have already proved previously that $H \cap K$ is a subgroup of G; see Exercise 2.1.10(a) on page 48. We now need to verify the normality condition: let $g \in G$. Then $gHg^{-1} = H$ and $gKg^{-1} = K$, consequently

$$g(H \cap K)g^{-1} \subseteq gHg^{-1} \cap gKg^{-1} = H \cap K.$$

Since N is a normal subgroup of G if and only if $N \leq G$ and $gNg^{-1} \subseteq N$ for all $g \in G$, the result is proven.

Exercise 3.1.33 on page 88 Find all normal subgroups of D_8 and for each of these find the isomorphism type of its corresponding quotient.

We shall write $G = D_8 = \{r, s \mid r^4 = s^2 = e, rs = sr^{-1}\}$. Thus the elements of D_8 are r^i and sr^i for $i = 0, 1, 2, 3$. A very useful result (which we shall cover in class) is that if $H \leq G$ and $|G/H| = 2$, then $H \lhd G$.

Let $N \lhd G$. Then by Lagrange's theorem N must have order 1,2,4 or 8, so let us consider these four cases separately.

1. $|N| = 8$. Then $N = G$ and $G/N \cong 1$.

2. $|N| = 1$. Then $N = 1$ and $G/N \cong D_8$.

3. $|N| = 4$. Then $|G/N| = |G|/|N| = 8/4 = 2$. Any group of order 2 is cyclic and therefore isomorphic to $\mathbb{Z}/2\mathbb{Z}$, consequently $G/N \cong \mathbb{Z}/2\mathbb{Z}$. If we use the table on page 69, the subgroups of order 4 in D_8 are $\langle s, r^2 \rangle$, $\langle r \rangle$, $\langle rs, r^2 \rangle$. As remarked above these subgroups are normal because they have index two; however it is not difficult to check that these subgroups are normal directly.

4. $|N| = 2$. Then $N = \langle x \rangle$ where x is the unique nonidentity element of N, and $|x| = 2$. The elements of order 2 in D_8 are sr^i for $i = 1, 2, 3, 4$ and r^2.

   Suppose $x = sr^i$. Then $N = \{e, sr^i\}$ and $rNr^{-1} = \{e, rsr^ir^{-1}\} = \{e, sr^{-1}r^ir^{-1}\} = \{e, sr^{i-2}\}$. Thus $N \neq rNr^{-1}$ and we see that N is not normal in G.

   Now suppose $x = r^2$. It is easily checked that $gr^2g^{-1} = r^2$ for all $g \in G$, hence $gng^{-1} = n$ for all $n \in N$ and we deduce that $N \lhd G$. Also $(sr^iN)^2 = (sr^i)^2N = N$ and $(r^iN)^2 = (r^i)^2N = r^{2i}N = N$ or $r^2N = N$. Thus every element of G/N has order at most 2, hence $G/N \ncong \mathbb{Z}/4\mathbb{Z}$ and we deduce that $G/N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 3.2.1 on page 95 Which of the following are permissible orders for subgroups of a group of order 120: 1, 2, 5, 7, 15, 60, 240? For each permissible order, give the corresponding index.

By Lagrange's theorem, the given number has to divide 120 (the order of the group). So the permissible orders are 1, 2, 5, 15, 60. Perhaps it is worth noting that all these orders are possible if the group of order 120 is cyclic, because for such a group there is exactly one subgroup of order n for each positive integer n dividing 120. Finally the corresponding indexes are 120/1, 120/2, 120/5, 120/15, 120/60; that is 120, 60, 24, 8, 2.

Exercise 3.2.4 on page 95 Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $\mathrm{Z}(G) = 1$.

Write $Z = \mathrm{Z}(G)$. By Lagrange's theorem $|Z|\big||G|$, so $|Z| = 1, p, q$ or pq. If $|Z| = pq$, then $Z = G$ which shows that G is abelian (the center of a group is always abelian). Therefore we may assume that $|Z| = p$ or q; without loss of generality $|Z| = p$, and then it follows that $|G/Z| = |G|/|Z| = q$.

I claim that G/Z must be cyclic. Indeed let x be a nonidentity element of G/Z. Then $\langle x\rangle$ is a subgroup of G/Z which is not equal to 1. By Lagrange's theorem $|\langle x\rangle|\big|q$ and since q is prime, we see that $|\langle x\rangle| = q$. Therefore $\langle x\rangle = G/Z$ and it follows that G/Z is cyclic.

Since G/Z is cyclic (and Z is contained in the center of G), it follows that G is abelian (see Exercise 3.1.36) and the proof is complete.