Abstract Algebra Solutions

Research · August 2015

DOI: 10.13140/RG.2.1.2799.6004

Evan Oman

Black River Systems Co.

Evan Oman
MATH 5371
Joe Gallian
September 16, 2013

Homework 1

Gallian 2.6: In each case, perform the indicated operation:

a) In $\mathbb{C}^*$, $(7+5i)(-3+2i)$

$$\begin{aligned}(7+5i)(-3+2i) &= -21+14i-15i+10i^2\\ &= -21-i+10(-1)\\ &= -(i+31)\in\mathbb{C}^*\end{aligned}$$

b) In $GL(2,Z_{13})$, $\det\left[\begin{pmatrix}7 & 4\\ 1 & 5\end{pmatrix}\right]$

First recall the definition of the determinant of a 2 × 2 matrix:

$$\det\left[\begin{pmatrix}a & b\\ c & d\end{pmatrix}\right] = a\cdot d - b\cdot c$$

So in our case we would have:

$$\begin{aligned}\det\left[\begin{pmatrix}7 & 4\\ 1 & 5\end{pmatrix}\right] &= 7\cdot 5-4\cdot 1\\ &= 31\\ &\equiv_{13} 5\in Z_{13}\end{aligned}$$

c) In $GL(2,\mathbb{R})$, $\begin{pmatrix}6 & 3\\ 8 & 2\end{pmatrix}^{-1}$

Recall the definition of the inverse of a 2 × 2 matrix:

$$A^{-1} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1} = \frac{1}{\det A}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$$

So if we let $B = \begin{pmatrix}6 & 3\\ 8 & 2\end{pmatrix}$, we find that

$$\begin{aligned}\det[B] &= 6\cdot 2-8\cdot 3\\ &= 12-24\\ &= -12\in\mathbb{R}\end{aligned}$$

Therefore

$$\begin{aligned} B^{-1} &= \frac{-1}{12}\begin{pmatrix} 2 & -3 \\ -8 & 6 \end{pmatrix} \\ &= \begin{pmatrix} -\frac{1}{6} & \frac{1}{4} \\ \frac{2}{3} & -\frac{1}{2} \end{pmatrix} \in GL(2,\mathbb{R}) \end{aligned}$$

d) In $GL\,(2, Z_{13})$, $\begin{pmatrix} 6 & 3 \\ 8 & 2 \end{pmatrix}^{-1}$

Here we use the same formula but since the entries are elements of Z_{13}, we must adjust the values according to this new modulus. So from part **c)**: $\det[B] = -12 \equiv_{13} 1$.

So our inverse becomes:

$$\begin{aligned} B^{-1} &= \frac{1}{1}\begin{pmatrix} 2 & -3 \\ -8 & 6 \end{pmatrix} \\ &\equiv_{13} \begin{pmatrix} 2 & 10 \\ 5 & 6 \end{pmatrix} \in GL(2, Z_{13}) \end{aligned}$$

■

Gallian 2.20: For any integer $n > 2$, show that there are at least 2 elements in $U(n)$ that satisfy $x^2 = 1$.

Let $n \in \mathbb{Z}$ such that $n > 2$. Then we know that that $U(n)$, the group of integers modulo n under multiplication, contains only the elements which are relatively prime to n. So we can write

$$U(n) = \{x \mod n |\ \gcd(n, x) = 1\}$$

So clearly $1 \in U(n)$ because the $\gcd(n, 1) = 1$(which is true for any number) and because $1 = e$ under multiplication which must be an element of $U(n)$ by $U(n)$ being a group.
Then since 1 is the identity it follows that $(1)^2 = 1$ giving one element satisfying $x^2 = 1$.
The next element we will consider is $n - 1$. By Lemma 0.1 we know that n and $(n - 1)$ are relatively prime so $n - 1 \in U(n)$.
Then squaring $(n - 1)^2$ yields:

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

Therefore we have found two elements that satisfy $x^2 = 1$, guaranteeing at least 2 elements $\forall U(n)$.

Lemma 0.1
Let $n \in \mathbb{Z}$ such that $n > 2$. Assume by contradiction that $n, n - 1$ are not relatively prime.

Then $\exists a \in \mathbb{N}\backslash\{1\}$ such that $a|n$ and $a|(n-1)$ which is to say that $\exists l, m \in \mathbb{N}\{1\}$ such that $m \cdot a = n$ and $l \cdot a = (n-1)$.

Rearranging we have $ma = la + 1 \Rightarrow a = \dfrac{1}{m-l}$.

However since $a, l, m \in \mathbb{N}\backslash\{1\}$, we arrive at a contradiction. Therefore we conclude that $n, n-1$ must be relatively prime for $n > 2$.

■

Gallian 2.34: Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

$(\Rightarrow)$

Assume $(ab)^2 = a^2b^2$.

Then

$$\begin{aligned}(ab)^2 = a^2b^2 &\Rightarrow abab = a^2b^2 \\ &\Rightarrow a^{-1}abab = a^{-1}a^2b^2 \\ &\Rightarrow bab = ab^2 \\ &\Rightarrow babb^{-1} = ab^2b^{-1} \\ &\Rightarrow ba = ab\end{aligned}$$

Therefore $(ab)^2 = a^2b^2 \Rightarrow ab = ba$.

$(\Leftarrow)$

Assume $ab = ba$.

Then

$$\begin{aligned}ab = ba &\Rightarrow a(ab) = a(ba) \\ &\Rightarrow a^2b = aba \\ &\Rightarrow (a^2b)b = (aba)b \\ &\Rightarrow a^2b^2 = (ab)^2\end{aligned}$$

Therefore $ab = ba \Rightarrow (ab)^2 = a^2b^2$.

Then since we have proven both directions we can conclude that $(ab)^2 = a^2b^2$ iff $ab = ba$. ■

Gallian 2.42: Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n such that $F_1F_2 = F_2F_1$. Prove that $F_1F_2 = R_{180}$.

Let $F_1, F_2 \in D_n$ be distinct reflections and assume $F_1 \neq F_2$ and $F_1F_2 = F_2F_1$. Then since every flip is its own inverse,

$$(F_1F_2)(F_1F_2) = F_1F_2F_1F_2 = F_2F_1F_1F_2 = F_2R_0F_2 = R_0$$

which is to say that $(F_1F_2)^2 = R_0$ or equivalently $(F_1F_2)^{-1} = F_1F_2$.

Then since F_1F_2 is a composition of flips, it represents some manipulation of the front side of our regular n-gon. Therefore F_1F_2 can be written as a rotation in the form of R_x.
Then since $F_1F_2 = R_x$, $(F_1F_2)^2 = R_0 \Rightarrow (R_x)^2 = R_0$.
Then by Lemma 0.2, we know that $F_1F_2 \neq R_0$ so the only other rotation who is its own inverse is R_{180}.
Therefore we conclude that $R_x = R_{180}$ and ultimately that $F_1F_2 = R_{180}$. ■

Lemma 0.2
Let $F_1, F_2 \in D_n$ and assume that $F_1 \neq F_2$.
Now assume by contradiction that $F_1F_2 = R_0$. Then left multiplying by F_1^{-1} we see that

$$F_1F_2F_2^{-1} = F_2^{-1}$$

Then since F_2 is a flip, $F_2 = F_2^{-1}$.
Therefore we are left with $F_1 = F_2$ which contradicts our premise that F_1, F_2 are distinct flips. Ergo $F_1F_2 \neq R_0$.

Gallian 2.44: Let R be a fixed rotation and F any fixed reflection in a dihedral group. Prove that $FR^kF = R^{-k}$. Why does this imply that D_n is non-Abelian?

Let $F, R \in D_n$.
Now consider the element FR^k(which is in D_n by closure of composition). Since the result of this composition is the reverse face of the regular n-gon, we can say that it is equivalent to some flip of the original shape.
Then, since FR^k is a flip, we know that $(FR^k)(FR^k) = R_0$ because every flip in D_n is its own inverse.
So

$$\begin{aligned}(FR^k)(FR^k) = R_0 &\Rightarrow \left(FR^k\right)\left(FR^k\right)R^{-k} = (R_0)\,R^{-k}\\ &\Rightarrow FR^kF = R^{-k}\end{aligned}$$

Therefore $\forall F, R \in D_n$, $FR^kF = R^{-k}$.
To see that this implies that D_n is non-Abelian, we assume by contradiction that every element commutes. Then using the above equality,

$$\begin{aligned}FR^kF = R^{-k} &\Rightarrow FR^kFR^k = R_0\\ &\Rightarrow FFR^kR^k = R_0\\ &\Rightarrow \left(R^k\right)^2 = R_0\end{aligned}$$

However this last line is only true for R_0 and R_{180} but since $R \in D_n$ was arbitrary, we arrive at a contradiction.
Therefore D_n is non-Abelian. ■

Gallian 2.50: In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 4. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

Let G be an arbitrary finite group. Then we can say that there are two basic cases:

Case 1: $\neg \exists x \in G : x \neq e$ and $x^5 = e$

In this case we say that there are no elements which satisfy the equation. So, since $4 \cdot 0 = 0$, we say that there is a multiple of 4 elements which satisfy the equation $x^5 = e$.

Case 2: $\exists x_1, \ldots, x_n \in G : x_i \neq e$ and $x_i^5 = e$ where $n \geq 1$

Consider some $x_i \in G$ where $x_i^5 = e$. Then we know that $x_i^2 \in G$ by closure and that

$$(x_i^2)^5 = (x_i^5)^2 = e^2 = e$$

To see that $x_i^2 \neq x_i$ it is clear that

$$x_i^2 = x_i \Rightarrow x_i = e$$

which is a contradiction. So x_i^2 is a new, unique element which satisfies $x^5 = e$.
Now consider the element x_i^3(which is in G by closure) where $x_i^3 \neq x_i^2$ because $x_i^3 = x_i^2 \Rightarrow x_i = e$(a contradiction). Then we have

$$(x_i^3)^5 = (x_i^5)^3 = e^3 = e$$

so x_i^3 is a new, unique element which satisfies $x^5 = e$.
Now consider the element x_i^4(which is in G by closure) where $x_i^4 \neq x_i^3$ because $x_i^4 = x_i^3 \Rightarrow x_i = e$(a contradiction). Then we have

$$(x_i^4)^5 = (x_i^5)^4 = e^4 = e$$

so x_i^4 is a new, unique element which satisfies $x^5 = e$.
However if we consider x_i^5, we already have $x_i^5 = e$ so this would not add to the list of nonidentity elements.
Additionally x_i^m where $m > 4$ would also not add to the list because these would be repeats of elements already found.
For example $x_i^6 = x_i x_i^5 = x_i e = x_i$. Hence we take x_i^m as $x_i^{m \mod 5}$.
Therefore for each x_i where $x_i^5 = e$ there are 3 additional elements(x_i^2, x_i^3, x_i^4) that also satisfy $x^5 = e$.
Consequently if $\exists x_1, \ldots, x_n \in G : x_i \neq e$ and $x_i^5 = e$ where $n \geq 1$ then we can say that the total number of elements that satisfy $x^5 = e$ would be $4 \cdot n$ which is clearly a multiple of 4.

If the finite condition were to be removed we would simply have an additional case where there are $x_1, x_2, \ldots \in G : x_i \neq e$ and $x_i^5 = e$. Here we would say that there are an infinite number of solutions to $x^5 = e$. ■

Evan Oman
MATH 5371
Joe Gallian
September 25, 2013

Homework 2

Gallian 3.26 Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

Let G be an arbitrary group.
Now assume $a, b \in G$ such that $a^2 = b^2 = e$ and $ab = ba$ so it has two elements of order 2 that commute.
Now consider $H = \langle a, b\rangle = \{e, a, b, ab\}^* \subseteq G$. First we know that H is non-empty and contains an identity.
Then to see that H is closed consider the multiplication of any two elements, any combination of elements would be equivalent to one of the existing elements because

$$\cdots a^{-3} = a^{-1} = a^1 = a^3 \cdots$$
$$\cdots b^{-3} = b^{-1} = b^1 = b^3 \cdots$$
$$\cdots (ab)^{-3} = (ab)^{-1} = (ab)^1 = (ab)^3 \cdots$$

since the elements a, b commute and are of order 2.
Then we can see that inverses exist for each element:

- $e^{-1} = e$
- $a^{-1} = a$
- $b^{-1} = b$
- $(ab)^{-1} = ab$

Therefore since H is closed, has inverses and identity, we say that H is a subgroup of G.
Then since $|H| = |\langle a, b\rangle| = 4$ we can say that for any group G where $a, b \in G$ such that $a^2 = b^2 = e$ and $ab = ba$, there exists a subgroup H where $|H| = 4$, namely, $H = \langle a, b\rangle$. ■

Gallian 3.28 Suppose that H is a proper subgroup of Z under addition and H contains 18,30, and 40. Determine H.

The proper subgroups of $\mathbb{Z}$ come in the form $\langle n\rangle$ where $\langle n\rangle$ is the set of all multiples of n. We can see that these are subgroup of $\mathbb{Z}$ because under addition, the operation of a multiple of n with another multiple of n necesarily produces another multiple of n. So we need to find the subgroup of $\mathbb{Z}$ containing 18, 30, and 40. Then since $gcd(18, 30, 40) = 2$ we say that the proper subgroup containing these elements is $\langle 2\rangle \leq \mathbb{Z}$. ■

[*] Note that $ab = ba$ so we write ab once.

Gallian 3.30 Prove that the dihedral group of order 6 does not have a subgroup of order 4.

Consider some subset H of the group D_3 where $|H| = 4$ andf $R_0 \in H$. Then H the only possibilities for H would be one of the following cases:

- Case 1: $H_1 = \{R_0, F_1, F_2, F_3\}$

  Since $F_1F_2 = R_{120} \notin H$, we know that H is not closed under the operation of composition so we know that it can not be a subgroup of G.

- Case 2: $H_2 = \{R_0, R_{120}, R_{240}, F_n\}$

  Because $F_nR_{120} = F_m$ where $F_m \neq F_n$, $F_m \notin H$ which implies that H is not closed. Therefore it can not be a subgroup of G.

- Case 2: $H_3 = \{R_0, R_x, F_n, F_m\}$

  If we consider the element $R_x \in H$ we know that $R_x^2 = R_{2\cdot x} \neq R_x$[†] so clearly $R_x^2 \notin H$ so again H is not closed and consequently not a group.

So every possible subset of D_3 with order 4 is not closed and fails to satisfy the subgroup criteria. Therefore D_3 has no subgroups of order 4. ∎

Gallian 3.32 If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?

Let G be a group and assume $H, K \leq G$. Then we can see that there are two possibilities for $H \cap K$:

- Case 1: $H \cap K = \{e\}$

  Assume $H \cap K = \{e\}$. Then $H \cap K$ would be the trivial subgroup which is by definition a subgroup of G. So $H \cap K \leq G$.

- Case 2: $H \cap K$ is nontrivial.

  Assume $H \cap K$ is a nontrivial set. Then since H, K are subgroups we know that $e \in H$ and $e \in K$ so $e \in H \cap K$ which implies that $H \cap K$ is non-empty.

  Now assume $a, b \in H \cap K$. Then since $H \cap K$ is defined as all elements that are in H **and** K we know that $a, b \in H$ and $a, b \in K$. Then since H and K are subgroups, $ab^{-1} \in H$ and $ab^{-1} \in K$. Therefore $ab^{-1} \in H \cap K$.

  Therefore $H \cap K$ passes the one-step subgroup test and consequently $H \cap K \leq G$.

So we conclude that for all $H, K \leq G$, $H \cap K \leq G$. ∎

[†] Since we are working in D_3 the possibilities here for x are 120 and 240 which when doubled do not equal themselves modulo 360

Gallian 3.34 Let G be a group, and let $a \in G$. Prove that $C(a) = C\left(a^{-1}\right)$

Let G be a group and let $a \in G$.
First recall that the definition of the centralizer of an element a in G:

$$C(a) = \{g \in G | ga = ag\}$$

Assume $c \in C(a)$ such that c is arbitrary. So we have:

$$\begin{aligned} ca = ac &\Rightarrow (ca)a^{-1} = (ac)a^{-1} \text{ (right multiply by } a^{-1}) \\ &\Rightarrow c = aca^{-1} \\ &\Rightarrow a^{-1}(c) = a^{-1}(aca^{-1}) \text{ (left multiply by } a^{-1}) \\ &\Rightarrow a^{-1}c = ca^{-1} \end{aligned}$$

So $c \in C\left(a^{-1}\right)$ and since c was arbitrary, $C\left(a\right) \subseteq C\left(a^{-1}\right)$.
Now assume $d \in C\left(a^{-1}\right)$ such that d is arbitrary. So we have:

$$\begin{aligned} da^{-1} = a^{-1}d &\Rightarrow (da^{-1})a = (a^{-1}d)a \text{ (right multiply by } a) \\ &\Rightarrow d = a^{-1}da \\ &\Rightarrow a(d) = a(a^{-1}da) \text{ (left multiply by } a) \\ &\Rightarrow ad = da \end{aligned}$$

So $d \in C\left(a\right)$ and since d was arbitrary, $C\left(a^{-1}\right) \subseteq C\left(a\right)$.
Therefore $C(a)$ and $C\left(a^{-1}\right)$ are inverses of each other so we can conclude that $C(a) = C\left(a^{-1}\right)$. ■

Gallian 3.68 Let $H = \{A \in GL\left(2, \mathbb{R}\right) | \det A \text{ is an integer power of } 2\}$. Show that H is a subgroup of $GL\left(2, \mathbb{R}\right)$.

Let $H = \left\{A \in GL\left(2, \mathbb{R}\right) | \det A = 2^l \text{ where } l \in \mathbb{Z}\right\}$.
Then $I \in H$ because

$$\det\left[\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right)\right] = 1 \cdot 1 - 0 \cdot 0 = 1 = 2^0$$

So I has a determinant which is a integer power of 2. Therefore H is non-empty.
Now assume $A, B \in H$ where

$$A = \left(\begin{array}{cc} a_1 & a_2 \\ a_3 & a_4 \end{array}\right) \text{ and } B = \left(\begin{array}{cc} b_1 & b_2 \\ b_3 & b_4 \end{array}\right)$$

Then by definition of H,

$$\begin{aligned} \det A = a_1 \cdot a_4 - a_2 \cdot a_3 = 2^n \text{ where } n \in \mathbb{Z} \\ \det B = b_1 \cdot b_4 - b_2 \cdot b_3 = 2^m \text{ where } m \in \mathbb{Z} \end{aligned}$$

Then to see that $AB^{-1} \in H$, we first find B^{-1} which is defined as:

$$B^{-1} = \frac{1}{\det B} \left(\begin{array}{cc} b_4 & -b_2 \\ -b_3 & b_1 \end{array} \right)$$

Then calculating AB^{-1} we find that:

$$\begin{aligned} AB^{-1} = C &= \left(\left(\begin{array}{cc} a_1 & a_2 \\ a_3 & a_4 \end{array} \right) \right) \cdot \left(\frac{1}{\det B} \left(\begin{array}{cc} b_4 & -b_2 \\ -b_3 & b_1 \end{array} \right) \right) \\ &= \frac{1}{\det B} \left(\begin{array}{cc} a_1 & a_2 \\ a_3 & a_4 \end{array} \right) \cdot \left(\begin{array}{cc} b_4 & -b_2 \\ -b_3 & b_1 \end{array} \right) \\ &= \frac{1}{\det B} \left(\begin{array}{cc} b_4a_1 - b_3a_2 & a_2b_1 - a_1b_2 \\ a_3b_4 - a_4b_3 & a_4b_1 - a_3b_2 \end{array} \right) \end{aligned}$$

Then to see that $AB^{-1} = C \in H$ we must calculate the determinant of C:

$$\begin{aligned} \det C &= \det \left[\frac{1}{\det B} \left(\begin{array}{cc} b_4a_1 - b_3a_2 & a_2b_1 - a_1b_2 \\ a_3b_4 - a_4b_3 & a_4b_1 - a_3b_2 \end{array} \right) \right] \\ &= \left(\frac{1}{\det B} \right)^2 \cdot \det \left[\left(\begin{array}{cc} b_4a_1 - b_3a_2 & a_2b_1 - a_1b_2 \\ a_3b_4 - a_4b_3 & a_4b_1 - a_3b_2 \end{array} \right) \right] \text{ (since we have a } 2 \times 2 \text{ matrix)} \\ &= \left(\frac{1}{\det B} \right)^2 \cdot \left[(b_4a_1 - b_3a_2) \cdot (a_4b_1 - a_3b_2) - (a_2b_1 - a_1b_2) \cdot (a_3b_4 - a_4b_3) \right] \\ &= \left(\frac{1}{\det B} \right)^2 \cdot \left[b_4a_1a_4b_1 - b_4a_1a_3b_2 - b_3a_2a_4b_1 + b_3a_2a_3b_2 - (a_2b_1a_3b_4 - a_2b_1a_4b_3 - a_1b_2a_3b_4 + a_1b_2a_4b_3) \right] \\ &= \left(\frac{1}{\det B} \right)^2 \cdot \left[a_1a_4b_1b_4 + a_2a_3b_2b_3 - a_2a_3b_1b_4 - a_1a_4b_2b_3 \right] \\ &= \left(\frac{1}{\det B} \right)^2 \cdot \left[a_1a_4 \left(b_1b_4 - b_2b_3 \right) - a_2a_3 \left(b_1b_4 - b_2b_3 \right) \right] \\ &= \left(\frac{1}{\det B} \right)^2 \cdot (a_1a_4 - a_2a_3) \cdot (b_1b_4 - b_2b_3) \\ &= \left(\frac{1}{\det B} \right)^2 \cdot (\det A) \cdot (\det B) \\ &= \frac{\det A}{\det B} = \frac{2^n}{2^m} = 2^{n-m} \end{aligned}$$

Then since $n - m \in \mathbb{Z}$ we can say that $\det [C] = \det [AB^{-1}]$ is equal to an integer power of 2 and consequently $AB^{-1} \in H$.

Therefore we have satisfied the conditions of the one-step subgroup test and consequently H is a subgroup of G. ■

Evan Oman
Graduate Student
MATH 5371
Joe Gallian
October 7, 2013

Homework 3

Gallian 4.18: If a cyclic group has an element of infinite order, how many elements of finite order does it have?

Let G be a cyclic group generated by some $g \in G$ such that $\langle g \rangle = G$.
Now assume that $\exists a \in G$ such that $|a| = \infty$.
Then by closure we know that $|G| = \infty$ and additionally, by Corollary 1 of Theorem 4.2, that $|G| = |\langle g \rangle| = |g|$. Thus in our case $|g| = \infty$.
Then since G is cyclic we know that every element of G can be written as g^n where $n \in \mathbb{Z} \setminus \{0\}$.
Now consider some $b \in G$ and assume that $b \neq e$ and $b^m = e$ where $m \in \mathbb{Z} \setminus \{0\}$ such that b has finite order.
Then we have $b^m = (g^n)^m = e$ so $|g| \leq n \cdot m$ by Corollary 2 of Theorem 4.1 which says $a^k = e \Rightarrow$ that $(|a|)|k$ which, by extension, says that $|a| \leq k$.
However this is a contradiction because $|a| = \infty$ and there are no $m, n \in \mathbb{Z}$ where $n \cdot m \geq \infty$.
Therefore there are no non-identity elements in G with finite order. If we consider e however we see that $|e| = 1$ which is finite. So we conclude that any cyclic group G with an element of infinite order has only one element[*] of finite order: the identity. ■

Gallian 4.36: Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

$(\Rightarrow)$
Let G be a finite group and assume that G is the union of all of its subgroups. Now assume by contradiction that G is cyclic such that $\exists g \in G$ such that $\langle g \rangle = G$.
Then we can consider 3 different cases:

1. $G = \{e\}$

   We can see that $\{e\}$ is a cyclic group but has no proper subgroups. Therefore we contradict our premise that G is the union of all of its proper subgroups so in this case G can not be cyclic.

2. $|G| = n$ where n is prime

   Assume that $|G| = n$ where n is prime. Then since G is cyclic, by Theorem 4.4 we know that the number of elements in G with order n would be equal to $n - 1$ because $\phi(n) = n - 1$ when n is prime. So every element g_i would have order n.

[*] Since there can only be one identity

Then we can say that each $g_i \in G$ would be a generator of G because each $\langle g_i \rangle$ would have order n(which is to say that they generate n elements).

Thus we conclude that the only proper subgroup of G would be the trivial subgroup $\{e\}$, which, when unioned with itself, is clearly not equal to G.

Therefore our assumption that G is cyclic has contradicted our premise that G is the union of all its proper subgroups. Thus in this case G can not be cyclic.

3. $\underline{|G| = n \text{ where } n \text{ is composite}}$

   Assume that $|G| = n$ where n is composite. Then by theorem 4.3 we know that G has exactly 1 subgroup of order $k \in \mathbb{Z}$ where k is a divisor of n, namely, $\left\langle g^{\frac{n}{k}} \right\rangle$.

   Thus in this case there are $n - \phi(n) - 1$ proper subgroups of G because this represents the number of elements whose powers are not relatively prime to n, the order of G.

   However when we consider some such subgroup

   $$\left\langle g^{\frac{n}{k}} \right\rangle = \left\{ e, g^{\frac{n}{k}}, g^{\frac{2n}{k}}, \dots, g^{\frac{k \cdot n - 1}{k}} \right\}$$

   we see that the power of each element is not relatively prime to n because it each power is a divisor of n.

   Thus these subgroups will never contain an element $a^l \in G$ where l is relatively prime to n because no divisor of n can be relatively prime to n.

   Then we can see that proper subgroups of the form $\left\langle g^{\frac{n}{k}} \right\rangle$ are the only proper subgroups of G by a similar argument as the case where n is prime because any element g^l where l is relatively prime to n would be a generator of the entire group G and would therefore not be a proper subgroup.

   Therefore the union of these proper subgroups do not form G because powers of our generator g that are relatively prime to n would never be generated. So G would not equal the union of its proper subgroups and we contradict our premise so in this case G can not be cyclic.

Thus in each case we arrive at a contradiction so we conclude that if G is the union of all its subgroups, G must not be cyclic.
$(\Leftarrow)$
Let G be a finite group and assume that G is not cyclic.
Then we can say that $\forall g_i \in G$, $\langle g_i \rangle \neq G$. Then we know that $\langle g_i \rangle \subset G$ and by Theorem 3.4, $\langle g_i \rangle$ is a proper subgroup of G.
Therefore we can see that

$$\bigcup_{i=0}^{n-1} \langle g_i \rangle = G$$

because each $\langle g_i \rangle$ contains at least g_i and never all of G.
Ergo if G is finite and not cyclic it is equal to the union of all of its proper subgroups. ∎

Gallian 4.44: Let F and F' be distinct reflections in D_{21}. What are the possibilities for $|FF'|$.

Let $F, F' \in D_{21}$. Then since $F \neq F'$, we can say that $FF' = R_x \neq R_0$ where R_x is some rotation in D_{21}.
So we have $|FF'| = |R_x|$. Then we can rewrite R_x as $R^k_{\frac{360}{21}}$ where $0 < k < 21$ because $\forall R_x \in D_{21}$, $R_x \in \left\langle R_{\frac{360}{21}} \right\rangle$.
Then by Theorem 4.2. we know that given some a where $|a| = n$, $|a^k| = \dfrac{n}{\gcd(n,k)}$.
So in our case we know that $\left| R_{\frac{360}{21}} \right| = 21$ so we have $\left| R^k_{\frac{360}{21}} \right| = \dfrac{21}{\gcd(21,k)}$.
Therefore we can case out the possible orders of $R^k_{\frac{360}{21}} = R_x = FF'$ in the table below:

k	Order of $R^k_{\frac{360}{21}} = FF'$
3,6,9,12,15,18	7
7,14	3
Otherwise	21

Table 1: Possible orders of $FF' \in D_{21}$

■

Gallian 4.50: Prove or disprove that $H = \{n \in \mathbb{Z} | n \text{ is divisible by both 8 and 10}\}$ is a subgroup of $\mathbb{Z}$.

Let $H \subset \mathbb{Z}$ be defined as the the set above. First, we know that the elements of H will take the form of $m \cdot l$ where $l = \operatorname{lcm}(8,10) = 40$.
So we have the set $H = \{40 \cdot m | m \in \mathbb{Z}\}$ which is clearly equal to $\langle 40 \rangle \subset \mathbb{Z}$.
Then by Theorem 3.4, we know that $\langle 40 \rangle < \mathbb{Z}$ so we conclude that $H = \langle 40 \rangle$ is a subgroup of $\mathbb{Z}$. ■

Gallian 4.64: Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$

Let G be a group and assume that $a, b \in G$ such that $|a| = m$ and $|b| = n$ where $\gcd(m,n) = 1$ (which is to say that m, n are relatively prime).
Now suppose by contradiction that $\exists$ a non-identity element $c \in \langle a \rangle \cap \langle b \rangle$.
Then we can say that $a^j = c = b^k$ where $j, k \in \mathbb{Z}^+$. Then $\exists l > 1 \in \mathbb{Z}$ such that $|c| = l$. Note that $l > 1$ because we have defined c such that $c \neq e$. So:

$$\begin{aligned} \left(a^j\right)^l = c^l = e = c^l = \left(b^k\right)^l &\Rightarrow a^{j \cdot l} = e = b^{k \cdot l} \\ &\Rightarrow m = j \cdot l,\ n = k \cdot l \end{aligned}$$

where $m = |a|$ and $n = |b|$.
Then we have that m, n share a common factor l contradicting our premise that $\gcd(m,n) = 1$.
Therefore $\neg \exists c \in \langle a \rangle \cap \langle b \rangle$ where $c \neq e$ so we conclude that $\langle a \rangle \cap \langle b \rangle = \{e\}$. ■

Gallian 4.78: If n is odd, prove that D_n has no subgroup of order 4.

Consider the group D_n where n is odd. First we can note that there are n flips and n rotations. Then there are really only 4 possible forms of subsets of D_n with order 4 which include the identity(so we can check if these subsets can possibly be subgroups).

- $H_1 = \{e, R_x, R_y, R_z\}$

  Consider the subset H_1 of D_n where $H_1 = \{e, R_x, R_y, R_z\}$. Then we know that the subgroup of all rotations, $\left\langle R_{\frac{360}{n}} \right\rangle$, in D_n is cyclic. So in order for $H_1 \leq D_n$ it must also be a subgroup of $\left\langle R_{\frac{360}{n}} \right\rangle$.

  Then by Theorem 4.3, if $H_! \leq \left\langle R_{\frac{360}{n}} \right\rangle$, then $|H_1|$ must divide the order of $\left\langle R_{\frac{360}{n}} \right\rangle$. However since $\left|\left\langle R_{\frac{360}{n}} \right\rangle\right| = n$ where n is odd, clearly $|H_1| = 4$ does not divider any odd number n.

  Therefore the subset H_1 containing the identity and 3 rotations is not a subgroup of D_n.

- $H_2 = \left\{e, F^l, F^m, F^n\right\}$

  Consider the subset H_2 of D_n where $H_2 = \left\{e, F^l, F^m, F^n\right\}$. Clearly this subset is not a subgroup of D_n because, for example, $F^l F^m = R_x \notin H$ so the subset is not closed under composition.

  Thus H_2 is not a subgroup of D_n.

- $H_3 = \left\{e, F^l, F^m, R_x\right\}$

  Consider the subset H_3 of D_n where $H_3 = \left\{e, F^l, F^m, R_x\right\}$. However since n is odd, we know that $\neg\exists R_x^{-1} \in H_3$ because $R_{180} \notin D_n$ when n is odd. Thus for any $R_y \in D_n$, $R_y \neq R_y^{-1}$.

  Therefore H_3 is not a subgroup of D_n

- $H_4 = \left\{e, F^l, R_x, R_y\right\}$

  Consider the subset H_4 of D_n where $H_4 = \left\{e, F^l, R_x, R_y\right\}$. To show that this subset is not closed it suffices to show that $\{R_x, R_y\}$ is not closed.

  Clearly this subset is not closed because every subgroup(or equivalently closed subset for our purposes) of $\left\langle R_{\frac{360}{n}} \right\rangle$ must divide n(see the argument for H_1).

  Thus the subset $\{R_x, R_y\}$ is not a closed subset of $\left\langle R_{\frac{360}{n}} \right\rangle$ because $2 \nmid n$ when n is odd. So we can conclude that H_4 is not a closed subset of D_n because there are only the 2 rotations in H_4.

  Therefore H_4 is not a subgroup of D_n

Then since every identity containing subset of D_n with order 4 fails the subgroup criteria, we conclude that D_n contains no subgroup of order 4. ■

Evan Oman
Graduate Student
MATH 5371
Joe Gallian
October 7, 2013

Homework 3

Gallian 4.18: If a cyclic group has an element of infinite order, how many elements of finite order does it have?

Let G be a cyclic group generated by some $g \in G$ such that $\langle g \rangle = G$.
Now assume that $\exists a \in G$ such that $|a| = \infty$.
Then by closure we know that $|G| = \infty$ and additionally, by Corollary 1 of Theorem 4.2, that $|G| = |\langle g \rangle| = |g|$. Thus in our case $|g| = \infty$.
Then since G is cyclic we know that every element of G can be written as g^n where $n \in \mathbb{Z} \setminus \{0\}$.
Now consider some $b \in G$ and assume that $b \neq e$ and $b^m = e$ where $m \in \mathbb{Z} \setminus \{0\}$ such that b has finite order.
Then we have $b^m = (g^n)^m = e$ so $|g| \leq n \cdot m$ by Corollary 2 of Theorem 4.1 which says $a^k = e \Rightarrow$ that $(|a|)|k$ which, by extension, says that $|a| \leq k$.
However this is a contradiction because $|a| = \infty$ and there are no $m, n \in \mathbb{Z}$ where $n \cdot m \geq \infty$.
Therefore there are no non-identity elements in G with finite order. If we consider e however we see that $|e| = 1$ which is finite. So we conclude that any cyclic group G with an element of infinite order has only one element[*] of finite order: the identity. ■

Gallian 4.36: Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

$(\Rightarrow)$
Let G be a finite group and assume that G is the union of all of its subgroups. Now assume by contradiction that G is cyclic such that $\exists g \in G$ such that $\langle g \rangle = G$.
Then we can consider 3 different cases:

1. $\underline{G = \{e\}}$

   We can see that $\{e\}$ is a cyclic group but has no proper subgroups. Therefore we contradict our premise that G is the union of all of its proper subgroups so in this case G can not be cyclic.

2. $\underline{|G| = n \text{ where } n \text{ is prime}}$

   Assume that $|G| = n$ where n is prime. Then since G is cyclic, by Theorem 4.4 we know that the number of elements in G with order n would be equal to $n - 1$ because $\phi(n) = n - 1$ when n is prime. So every element g_i would have order n.

[*] Since there can only be one identity

Then we can say that each $g_i \in G$ would be a generator of G because each $\langle g_i \rangle$ would have order n(which is to say that they generate n elements).

Thus we conclude that the only proper subgroup of G would be the trivial subgroup $\{e\}$, which, when unioned with itself, is clearly not equal to G.

Therefore our assumption that G is cyclic has contradicted our premise that G is the union of all its proper subgroups. Thus in this case G can not be cyclic.

3. $\underline{|G| = n \text{ where } n \text{ is composite}}$

   Assume that $|G| = n$ where n is composite. Then by theorem 4.3 we know that G has exactly 1 subgroup of order $k \in \mathbb{Z}$ where k is a divisor of n, namely, $\left\langle g^{\frac{n}{k}} \right\rangle$.

   Thus in this case there are $n - \phi(n) - 1$ proper subgroups of G because this represents the number of elements whose powers are not relatively prime to n, the order of G.

   However when we consider some such subgroup

   $$\left\langle g^{\frac{n}{k}} \right\rangle = \left\{ e, g^{\frac{n}{k}}, g^{\frac{2n}{k}}, \ldots, g^{\frac{k \cdot n - 1}{k}} \right\}$$

   we see that the power of each element is not relatively prime to n because it each power is a divisor of n.

   Thus these subgroups will never contain an element $a^l \in G$ where l is relatively prime to n because no divisor of n can be relatively prime to n.

   Then we can see that proper subgroups of the form $\left\langle g^{\frac{n}{k}} \right\rangle$ are the only proper subgroups of G by a similar argument as the case where n is prime because any element g^l where l is relatively prime to n would be a generator of the entire group G and would therefore not be a proper subgroup.

   Therefore the union of these proper subgroups do not form G because powers of our generator g that are relatively prime to n would never be generated. So G would not equal the union of its proper subgroups and we contradict our premise so in this case G can not be cyclic.

Thus in each case we arrive at a contradiction so we conclude that if G is the union of all its subgroups, G must not be cyclic.
$(\Leftarrow)$
Let G be a finite group and assume that G is not cyclic.
Then we can say that $\forall g_i \in G$, $\langle g_i \rangle \neq G$. Then we know that $\langle g_i \rangle \subset G$ and by Theorem 3.4, $\langle g_i \rangle$ is a proper subgroup of G.
Therefore we can see that

$$\bigcup_{i=0}^{n-1} \langle g_i \rangle = G$$

because each $\langle g_i \rangle$ contains at least g_i and never all of G.
Ergo if G is finite and not cyclic it is equal to the union of all of its proper subgroups. ■

Gallian 4.44: Let F and F' be distinct reflections in D_{21}. What are the possibilities for $|FF'|$.

Let $F, F' \in D_{21}$. Then since $F \neq F'$, we can say that $FF' = R_x \neq R_0$ where R_x is some rotation in D_{21}.
So we have $|FF'| = |R_x|$. Then we can rewrite R_x as $R^k_{\frac{360}{21}}$ where $0 < k < 21$ because $\forall R_x \in D_{21}$, $R_x \in \left\langle R_{\frac{360}{21}} \right\rangle$.
Then by Theorem 4.2. we know that given some a where $|a| = n$, $|a^k| = \dfrac{n}{\gcd(n,k)}$.
So in our case we know that $\left|R_{\frac{360}{21}}\right| = 21$ so we have $\left|R^k_{\frac{360}{21}}\right| = \dfrac{21}{\gcd(21,k)}$.
Therefore we can case out the possible orders of $R^k_{\frac{360}{21}} = R_x = FF'$ in the table below:

k	Order of $R^k_{\frac{360}{21}} = FF'$
3,6,9,12,15,18	7
7,14	3
Otherwise	21

Table 1: Possible orders of $FF' \in D_{21}$

■

Gallian 4.50: Prove or disprove that $H = \{n \in \mathbb{Z} | n \text{ is divisible by both 8 and 10}\}$ is a subgroup of $\mathbb{Z}$.

Let $H \subset \mathbb{Z}$ be defined as the the set above. First, we know that the elements of H will take the form of $m \cdot l$ where $l = \operatorname{lcm}(8, 10) = 40$.
So we have the set $H = \{40 \cdot m | m \in \mathbb{Z}\}$ which is clearly equal to $\langle 40 \rangle \subset \mathbb{Z}$.
Then by Theorem 3.4, we know that $\langle 40 \rangle < \mathbb{Z}$ so we conclude that $H = \langle 40 \rangle$ is a subgroup of $\mathbb{Z}$. ■

Gallian 4.64: Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$

Let G be a group and assume that $a, b \in G$ such that $|a| = m$ and $|b| = n$ where $\gcd(m, n) = 1$ (which is to say that m, n are relatively prime).
Now suppose by contradiction that $\exists$ a non-identity element $c \in \langle a \rangle \cap \langle b \rangle$.
Then we can say that $a^j = c = b^k$ where $j, k \in \mathbb{Z}^+$. Then $\exists l > 1 \in \mathbb{Z}$ such that $|c| = l$. Note that $l > 1$ because we have defined c such that $c \neq e$. So:

$$\begin{aligned} \left(a^j\right)^l = c^l = e = c^l = \left(b^k\right)^l &\Rightarrow a^{j \cdot l} = e = b^{k \cdot l} \\ &\Rightarrow m = j \cdot l,\ n = k \cdot l \end{aligned}$$

where $m = |a|$ and $n = |b|$.
Then we have that m, n share a common factor l contradicting our premise that $\gcd(m, n) = 1$.
Therefore $\neg\exists c \in \langle a \rangle \cap \langle b \rangle$ where $c \neq e$ so we conclude that $\langle a \rangle \cap \langle b \rangle = \{e\}$. ■

Gallian 4.78: If n is odd, prove that D_n has no subgroup of order 4.

Consider the group D_n where n is odd. First we can note that there are n flips and n rotations. Then there are really only 4 possible forms of subsets of D_n with order 4 which include the identity(so we can check if these subsets can possibly be subgroups).

- $\underline{H_1 = \{e, R_x, R_y, R_z\}}$

  Consider the subset H_1 of D_n where $H_1 = \{e, R_x, R_y, R_z\}$. Then we know that the subgroup of all rotations, $\left\langle R_{\frac{360}{n}} \right\rangle$, in D_n is cyclic. So in order for $H_1 \leq D_n$ it must also be a subgroup of $\left\langle R_{\frac{360}{n}} \right\rangle$.

  Then by Theorem 4.3, if $H_! \leq \left\langle R_{\frac{360}{n}} \right\rangle$, then $|H_1|$ must divide the order of $\left\langle R_{\frac{360}{n}} \right\rangle$. However since $\left|\left\langle R_{\frac{360}{n}} \right\rangle\right| = n$ where n is odd, clearly $|H_1| = 4$ does not divider any odd number n.

  Therefore the subset H_1 containing the identity and 3 rotations is not a subgroup of D_n.

- $\underline{H_2 = \left\{e, F^l, F^m, F^n\right\}}$

  Consider the subset H_2 of D_n where $H_2 = \left\{e, F^l, F^m, F^n\right\}$. Clearly this subset is not a subgroup of D_n because, for example, $F^l F^m = R_x \notin H$ so the subset is not closed under composition.

  Thus H_2 is not a subgroup of D_n.

- $\underline{H_3 = \left\{e, F^l, F^m, R_x\right\}}$

  Consider the subset H_3 of D_n where $H_3 = \left\{e, F^l, F^m, R_x\right\}$. However since n is odd, we know that $\neg\exists R_x^{-1} \in H_3$ because $R_{180} \notin D_n$ when n is odd. Thus for any $R_y \in D_n$, $R_y \neq R_y^{-1}$.

  Therefore H_3 is not a subgroup of D_n

- $\underline{H_4 = \left\{e, F^l, R_x, R_y\right\}}$

  Consider the subset H_4 of D_n where $H_4 = \left\{e, F^l, R_x, R_y\right\}$. To show that this subset is not closed it suffices to show that $\{R_x, R_y\}$ is not closed.

  Clearly this subset is not closed because every subgroup(or equivalently closed subset for our purposes) of $\left\langle R_{\frac{360}{n}} \right\rangle$ must divide n(see the argument for H_1).

  Thus the subset $\{R_x, R_y\}$ is not a closed subset of $\left\langle R_{\frac{360}{n}} \right\rangle$ because $2 \nmid n$ when n is odd. So we can conclude that H_4 is not a closed subset of D_n because there are only the 2 rotations in H_4.

  Therefore H_4 is not a subgroup of D_n

Then since every identity containing subset of D_n with order 4 fails the subgroup criteria, we conclude that D_n contains no subgroup of order 4. ■

Evan Oman
Graduate Student
MATH 5371
Joe Gallian
October 23, 2013

Homework 4

Gallian 5.10: What is the maximum order of any element of A_{10}?

Since we are working with A_{10} we only have to worry about even permutations. So the only cycle length that we need to consider are 1, 2, and odd numbers less than 10.
So we can consider the following cases which would make up any element of A_{10} since they are the additive factors of 10:

- $(\underline{9}, \underline{1}) \Rightarrow \text{lcm}(9,1) = 9$
- $(\underline{7}, \underline{3}) \Rightarrow \text{lcm}(7,3) = 21$
- $(\underline{9}, \underline{1}) \Rightarrow \text{lcm}(5,5) = 5$
- Else $\Rightarrow \text{lcm}(n_1, n_2, \ldots, n_m) \leq 12$ when $n_i \leq 4$

So we can see that the largest order in the above list of possibilities is 21. ■

Gallian 5.26: Let α and β belong to S_n. Prove that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation.

Let $\alpha, \beta \in S_n$. Then we know by Theorem 5.4 that α, β can be rewritten as some composition of two cycles in the form:

$$\alpha = \gamma_1\gamma_2\gamma_3\cdots\gamma_n$$
$$\beta = \delta_1\delta_2\delta_3\cdots\delta_m$$

where γ_i, δ_i are 2-cycles and $n, m \in \mathbb{Z}^+$.
Then since every 2-cycle is its own inverse we can say that:

$$\alpha^{-1} = \gamma_n\gamma_{n-1}\gamma_{n-2}\cdots\gamma_1$$
$$\beta^{-1} = \delta_m\delta_{m-1}\delta_{m-2}\cdots\delta_1$$

Thus we have:

$$\alpha^{-1}\beta^{-1}\alpha\beta = \underbrace{(\gamma_n\gamma_{n-1}\cdots\gamma_1)}_{n\text{ 2-cycles}}\underbrace{(\delta_m\delta_{m-1}\cdots\delta_1)}_{m\text{ 2-cycles}}\underbrace{(\gamma_1\gamma_2\cdots\gamma_n)}_{n\text{ 2-cycles}}\underbrace{(\delta_1\delta_2\cdots\delta_m)}_{m\text{ 2-cycles}}$$

So we have a total of

$$n + m + n + m = 2\,(n + m)$$

2-cycles and since n, m are positive integers we know that we have an even number of 2-cycles. Therefore $\alpha^{-1}\beta^{-1}\alpha\beta$ can be rep[resented by an even number of 2-cycles which, by Theorem 5.5, guarantees that every other representation will also be even.
So $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation. ■

Gallian 5.28: How many elements of order 5 are in S_7?

In order for an element of S_n to have an order of 5 the lcm of the lengths of all the n-cycles of that element must be 5.
So from the ordering given in the chapter we need only consider elements of the form $(\underline{5})\,(\underline{1})\,(\underline{1})$.
So an arbitrary element of this form would look like:

$$(\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5)\,(\alpha_6)\,(\alpha_7)$$

In order to find the total number of possible elements of this form we need only consider the 5-cycle(since the 2 1-cycles would just be what is left over from the 5-cycle). Clearly there are $7\cdot6\cdot5\cdot4\cdot3$ possible orderings of $(\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5)$. However simply counting by this method counts the same permutation 5 times since:

$$(\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5) = (\alpha_2\alpha_3\alpha_4\alpha_5\alpha_1) = (\alpha_3\alpha_4\alpha_5\alpha_1\alpha_2) = (\alpha_4\alpha_5\alpha_1\alpha_2\alpha_3) = (\alpha_5\alpha_1\alpha_2\alpha_3\alpha_4)$$

Thus we have $\dfrac{7\cdot6\cdot5\cdot4\cdot3}{5} = 504$ elements of order 5. ■

Gallian 5.30: Prove that (1 2 3 4) is not the product of 3-cycles.

Consider $\alpha = (1\ 2\ 3\ 4) \in S_n$. First we know that α can be rewritten as

$$\alpha = (1\ 4)\,(1\ 3)\,(1\ 2)$$

so we can say that α is an odd permutation.
Now assume by contradiction that α can be written as the product of some sequence of 3-cycles $\beta_i \in S_n$ so that

$$\alpha = \beta_1\beta_2\beta_3\cdots\beta_m$$

where each $\beta_i = (\gamma_i\ \delta_i\ \epsilon_i)$.
However since each β_i is a 3-cycle it can be rewritten as

$$\beta_i = (\gamma_i\ \delta_i\ \epsilon_i) = (\gamma_i\ \epsilon_i)\,(\gamma_i\ \delta_i)$$

indicating that α can be written as:

$$\begin{aligned}\alpha = \beta_1\beta_2\beta_3\cdots\beta_m &= [(\gamma_1\ \delta_1\ \epsilon_1)]\,[(\gamma_2\ \delta_2\ \epsilon_2)]\,[(\gamma_3\ \delta_3\ \epsilon_3)]\cdots[(\gamma_m\ \delta_m\ \epsilon_m)] \\ &= [(\gamma_1\ \epsilon_1)\,(\gamma_1\ \delta_1)]\,[(\gamma_2\ \epsilon_2)\,(\gamma_2\ \delta_2)]\,[(\gamma_3\ \epsilon_3)\,(\gamma_3\ \delta_3)]\cdots[(\gamma_m\ \epsilon_m)\,(\gamma_m\ \delta_m)]\end{aligned}$$

giving us a total of $2 \cdot m$ 2-cycles, which is clearly even.
However by Theorem 5.5 we know that every representation of α must contain an odd number of 2-cycles so we arrive at a contradiction of α being odd.
Therefore (1 2 3 4) is not the product of 3-cycles. ∎

Gallian 5.38: Let $H = \{\beta \in S_5 | \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5. How many elements are in H? Is your argument valid when S_5 is replaced by S_n when $n \geq 3$? How many elements are in H when S_5 is replaced by A_n for $n \geq 4$?

H is a Subgroup of S_5

Let $H = \{\beta \in S_5 | \beta(1) = 1 \text{ and } \beta(3) = 3\}$.
Then we know that the identity element is in H because the identity "fixes" every value, including 1 and 3. So H is non-empty.
So $\alpha \in H \;\Rightarrow\; \alpha^{-1} \in H$.
Now assume that $\alpha, \beta \in H$.
Then we can easily see that α^{-1} is in H because $\alpha^{-1}(\alpha(1)) = 1 \Rightarrow \alpha^{-1}(1) = 1$ since the identity element fixes every value.
Now consider the composition $\alpha \circ \beta$:

$$\alpha \circ \beta(1) = \beta(\alpha(1)) = \beta(1) = 1$$
$$\alpha \circ \beta(3) = \beta(\alpha(3)) = \beta(3) = 3$$

Thus $\alpha \circ \beta$ fixes both 1 and 3 so $\alpha \circ \beta \in H$.
So $\alpha, \beta \in H \;\Rightarrow\; \alpha\beta \in H$.
Therefore H passes the two-step subgroup test and consequently $H \leq S_5$.

Cardinality of H

Any $\alpha \in H \leq S_5$ would have the form:

$$\alpha = (1)\,(2)\,(3)\,(4)\,(5) \tag{1}$$
$$\text{OR }\; (a_1 a_2)\,(a_3)\,(1)\,(3) \tag{2}$$
$$\text{OR }\; (a_1 a_2 a_3)\,(1)\,(3) \tag{3}$$

So we can now look at how many elements would satisfy each case:

1. **1 Element:** Only one element can take this form, the identity.
2. **3 Elements:** In a similar manner to #28 we can see that there would be $\dfrac{3 \cdot 2}{2} = 3$ elements of this form.
3. **2 Elements:** Similarly there would be $\dfrac{3 \cdot 2 \cdot 1}{3} = 2$ elements of this form.

So $|H| = 1 + 3 + 2 = 6$.

Would this argument apply to S_n?
Clearly the cardinality argument would not apply to S_n because instead of only those cases listed above there would be considerable more because we are only fixing 2 elements.
However we can think of $|H|$ when $H \leq S_n$ as a system where we have 2 fixed values leaving open possibilities for the remaining $n-2$ values. So we would be working with the permutations of $n-2$ symbols, which we know from the chapter to be $(n-2)!$.
Therefore if $H \leq S_n$, then $|H| = (n-2)!$
The proof that $H \leq S_5$ would however also prove that $H \leq S_n$ because the fact that $1, 3 \in S_5$ has no bearing on the validity of the proof.

What is $|H|$ when S_5 is replaced by A_n for $n \geq 4$? From the previous sub-question we know that when $H \leq S_n$, $|H| = (n-2)!$. Then from the chapter we also know that half of the $(n-2)!$ permutations would be even and the other half would be odd.
Therefore would only consider half of the $(n-2)!$ permutations giving $|H| = \dfrac{(n-2)!}{2}$ when $H \leq A_n$ for $n \geq 4$.
Note that when $n < 4$ we would only consider $n = 3$(since A_2 could not possibly fix 3). So we would have $\dfrac{3-2)!}{2} = 1.5 \notin \mathbb{Z}^+$.
When $n = 3$ we would have $|H| = 1$ because it would contain only the identity element.

■

Gallian 5.54: Let n be an even positive integer. Prove that A_n has an element of order greater than n if and only if $n \geq 8$.

$(\Rightarrow)$
Assume A_n has an element of order greater than n where n is even and assume by contradiction that $n < 8$.
Then we would simply have the following cases:

- $n = 6$

  When $n = 6$ every element would take the form

  - $(\underline{5})\,(\underline{1})$ where lcm(1,5) $= |\,(\underline{5})\,(\underline{1})\,| = 5 < 6$
  - $(\underline{3})\,(\underline{3})$ where lcm(3,3) $= |\,(\underline{3})\,(\underline{3})\,| = 3 < 6$
  - $(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})$ where lcm(1,1,1,1,1,1) $=|\,(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})\,| = 1 < 6$

  Then there are no elements with order greater than 6 so we arrive at a contradiction.

- $n = 4$

  When $n = 4$ every element would take the form

  - ○ $(\underline{3})\,(\underline{1})$ where lcm(1,3) $= |\,(\underline{3})\,(\underline{1})\,| = 3 < 4$
  - ○ $(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})$ where lcm(1,1,1,1) $=|\,(\underline{1})\,(\underline{1})\,(\underline{1})\,(\underline{1})\,| = 1 < 4$

  Then there are no elements with order greater than 4 so we arrive at a contradiction.

- $\underline{n = 2}$

  When $n = 2$ we would only have the identity element:

  - ○ $(\underline{1})\,(\underline{1})$ where lcm(1,1) $=|\,(\underline{1})\,(\underline{1})\,| = 1 < 2$

  Then there are no elements with order greater than 2 so we arrive at a contradiction.

Thus we arrive at a contradiction in every case so we can see that if A_n has and element of order greater than n, then $n \geq 8$.
$(\Leftarrow)$
Consider A_n where n is an even integer such that $n \geq 8$. Then we can consider the following 2 cases:

1. $\underline{\frac{n}{2} \text{ is Even}}$

   Assume $\frac{n}{2}$ is even. Then we know that $\frac{n}{2} \pm 1$ will be odd so $\left(\underline{\frac{n}{2}+1}\right)\left(\underline{\frac{n}{2}-1}\right) \in A_n$.

   Then since $d\left(\frac{n}{2}+1, \frac{n}{2}-1\right) = 2$, we know that $\gcd\left(\frac{n}{2}+1, \frac{n}{2}-1\right) \leq 2$. However since both are odd, we say that the gcd is 1.

   Then since $\frac{n}{2}+1$, $\frac{n}{2}-1$ are relatively prime, we know that

   $$\operatorname{lcm}\left(\frac{n}{2}+1, \frac{n}{2}-1\right) = \frac{(\frac{n}{2}+1)(\frac{n}{2}-1)}{1} = \frac{n^2}{4} - 1$$

   which is clearly greater than n for $n \geq 8$.

2. $\underline{\frac{n}{2} \text{ is Odd}}$

   Assume $\frac{n}{2}$ is odd. Then we know that $\frac{n}{2}, \frac{n}{2}-2$ will be odd so $\left(\underline{\frac{n}{2}}\right)\left(\underline{\frac{n}{2}-2}\right) \in A_n$.

   Then since $d\left(\frac{n}{2}, \frac{n}{2}-2\right) = 2$, we know that $\gcd\left(\frac{n}{2}, \frac{n}{2}-2\right) \leq 2$. However since both are odd, we say that the gcd is 1.

   Then since $\frac{n}{2}$, $\frac{n}{2}-2$ are relatively prime, we know that

   $$\operatorname{lcm}\left(\frac{n}{2}, \frac{n}{2}-2\right) = \frac{(\frac{n}{2})(\frac{n}{2}-2)}{1} = n\left(\frac{n}{4}-1\right)$$

   which is clearly greater than n for $n \geq 8$.

Therefore in every case we have found an element with an adequate order so we conclude that given A_n where $n \geq 8$, $\exists$ an element whose order is greater than n. ■

Evan Oman
Graduate Student
MATH 5371
Joe Gallian
November 1, 2013

Homework 5

Gallian 6.6: Prove that isomorphism is an equivalence relation. That is, for any groups G, H, and K, $G \cong G$, $G \cong H$ implies $H \cong G$, and $G \cong H$ and $H \cong K$ implies $G \cong K$.

Let G, H, K be groups.
$\underline{G \cong G}$
Consider $\varphi : G \to G$ defined by $\forall g \in G$, $\varphi(g) = g$.
Then clearly the map is one to one and onto so we say it is bijective.
Also $\varphi(g_1 g_2) = g_1 g_2 = \varphi(g_1)\varphi(g_2)$ so the map φ is structure preserving.
Therefore φ is an isomorphism so $G \cong G$.
$\underline{G \cong H \Rightarrow H \cong G}$
Assume $\varphi : G \to H$.
Then clearly the function φ^{-1} is also bijective since φ is bijective.
Then we can see that φ^{-1} is structure preserving since, letting $a, b \in G$:

$$\varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(ab) = ab = \varphi^{-1}(\varphi(a))\varphi^{-1}(\varphi(b))$$

So φ^{-1} is structure preserving.
Therefore φ^{-1} is a structure preserving bijection making it an isomorphism. So $G \cong H \Rightarrow H \cong G$.
$\underline{G \cong H \text{ and } H \cong K \text{ implies } G \cong K.}$
Assume $\varphi : G \to H$ and $\psi : H \to K$ such that φ and ψ are isomorphisms.
Then to see that $\exists$ a homomorphism $\sigma : G \to K$ defined as $\sigma = \psi \circ \varphi$. Then letting $a, b \in G$ we have:

$$\begin{aligned}
\sigma(a)\sigma(b) &= \psi(\varphi(a))\psi(\varphi(b)) && \text{(since } \sigma = \psi \circ \varphi) \\
&= \psi(\varphi(a)\varphi(b)) && \text{(since } \psi \text{ is structure preserving)} \\
&= \psi(\varphi(ab)) && \text{(since } \varphi \text{ is structure preserving)} \\
&= \sigma(ab)
\end{aligned}$$

Thus $\sigma(a)\sigma(b) = \sigma(ab)$ so σ is structure preserving.
Then we know that σ is bijective because the composition of bijective maps is also bijective.
Therefore $G \cong H$ and $H \cong K$ implies that there exists some map $\sigma : G \to K$ that is a structure preserving bijection so it is an isomorphism.
Therefore $G \cong H$ and $H \cong K$ implies $G \cong K$.

Thus isomorphism is reflexive, symmetric, and transitive so we conclude that it forms an equivalence relation on groups.

■

Gallian 6.10: Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.

($\Rightarrow$)
Assume that $\alpha : G \to G$ defined by $\alpha(g) = g^{-1}$ is an automorphism.
Then since α is an isomorphism we know that given any $g_1, g_2 \in G$,

$$\alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2)$$

then based on the definition of α, we see that

$$\alpha(g_1 g_2) = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$$

and

$$\alpha(g_1)\alpha(g_2) = g_1^{-1} g_2^{-1}$$

giving us:

$$g_1^{-1} g_2^{-1} = g_2^{-1} g_1^{-1}$$

This in turn implies that

$$g_1 g_2 = g_2 g_1$$

Therefore we conclude that if α is an automorphism, G must be Abelian.
($\Leftarrow$)
Assume that G is Abelian and consider the function α defined by $\alpha(g) = g^{-1}$.
Then we can see that the function is clearly a bijection since it maps every element to its own inverse, which we know to be unique.
Then to see that α is structure preserving let $g_1, g_2 \in G$:

$$\begin{aligned}\alpha(g_1 g_2) &= (g_1 g_2)^{-1} \\ &= g_2^{-1} g_1^{-1} \\ &= g_1^{-1} g_2^{-1} \text{ (since } G \text{ is abelian)} \\ &= \alpha(g_1)\alpha(g_2)\end{aligned}$$

So $\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2)$.
Therefore α is a structure preserving bijection so we conclude that if G is Abelian then α is an automorphism. ■

Gallian 6.18: Let H be the subgroup of all rotations in D_n and let ϕ be an automorphism of D_n Prove that $\phi(H) = H$

Let $\phi : D_n \to D_n$. Then consider the subgroup H of D_n consisting of all rotations in D_n.
Then we know that the subgroup H is cyclic with order n since the set of all rotations is cyclic.
Thus the only elements in D_n that are cyclic with an overall order of n in D_n are the elements of the set of all rotations.

Additionally, we know that automorphism must map subgroups to subgroups. Then the only possible place that ϕ could send H is H because D_n has only one subgroup of order n(which is significant because $|H| = n$).
Therefore the only way we can preserve the structure of the group with an isomorphism is by mapping the elements within the cyclic group to other elements within the cyclic group. So $\phi(H) = H$. ■

Gallian 6.34: Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

To see whether or not $U(24)$ and $U(20)$ are isomorphic, consider the following tables:

n	Elements of order n	Total # of elements with order n
1	$\{1\}$	1
2	$\{3, 5, 7, 11, 13, 17, 23\}$	7

Table 1: Orders of elements of $U(24)$

n	Elements of order n	Total # of elements with order n
1	$\{1\}$	1
2	$\{9, 11, 19\}$	3
3	$\emptyset$	0
4	$\{3, 7, 13, 17\}$	4

Table 2: Orders of elements of $U(20)$

So we can see that the orders of the elements of the 2 groups are not compatible so there can not exist an isomorphism between $U(20)$ and $U(24)$.
Thus $U(24)$ and $U(20)$ are not isomorphic. ■

Gallian 6.42: Suppose that G is a finite Abelian group and G has no element of order 2. Show that the mapping $g \to g^2$ is an automorphism of G. Show, by example, that there is an infinite Abelian group for which the mapping $g \to g^2$ is one to one and operation preserving but not an automorphism.

Automorphism
Let $G = \{e, g_1, g_2, g_3, \ldots, g_n\}$ such that $\forall g_i \in G$, $g_i^2 \neq e$. To see that $\varphi : G \to G$ is an automorphism we must show the following:

1. Injective

   To see that φ is injective, consider $g_1, g_2 \in G$ and assume that $\varphi(g_1) = \varphi(g_2)$.

Then

$$\begin{aligned}\varphi(g_1) = \varphi(g_2) &\Rightarrow g_1^2 = g_2^2 \\ &\Rightarrow g_1^2 {g_2}^{-2} = e \\ &\Rightarrow g_1 g_1 {g_2}^{-1} {g_2}^{-1} = e \\ &\Rightarrow g_1 {g_2}^{-1} g_1 {g_2}^{-1} = e \\ &\Rightarrow (g_1 {g_2}^{-1})^2 = e\end{aligned}$$

However G has no elements of order 2 so the only way this could happen is if $g_1 {g_2}^{-1} = e$. Thus we would have

$$g_1 {g_2}^{-1} = e \Rightarrow g_1 = g_2$$

So $\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$ and consequently φ is injective.

2. Surjective

   To see that φ is surjective, we must show that every element of G is the sqaure of another element.

   Consider $g_i \in G$. Then we know from the above injective proof that g_i^2 is a distinct, non-identity element of G. However by closure we know that g_i^2 is in G so we can say that $\forall g_i \in G$, $g_i^2 \neq g_j^2$ and $g_i^2 = g_k$ for some $g_k \in G$.

   Therefore every element in G can be uniquely written as the square of some other element so φ is surjective.

3. Structure Preserving

   To see that φ is structure/operation preserving consider $g_1, g_2 \in G$:

$$\begin{aligned}\varphi(g_1)\varphi(g_2) &= g_1^2 g_2^2 \\ &= g_1 g_2 g_1 g_2 \\ &= (g_1 g_2)^2 \\ &= \varphi(g_1 g_2)\end{aligned}$$

   Therefore $\varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2)$ and we conclude that the map is structure preserving.

Thus φ is a structure preserving bijection from G to G so we can conclude that φ is an automorphism of G.

Example

For an example of a group meeting the requirements, consider the integers under addition, $(\mathbb{Z}, +)$.

Then we can see that $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is clearly injective since if $n \in (\mathbb{Z}, +)$, $\varphi(n) = 2$. Thus there are no other elements in $\mathbb{Z}$ that could possible map to $2n$ so φ is injective.

The map φ is also structure preserving since:

$$\begin{aligned}\varphi(n_1) + \varphi(n_2) &= 2 \cdot n_1 + 2 \cdot n_2 \\ &= 2(n_1 + n_2) \\ &= \varphi(n_1 + n_2)\end{aligned}$$

Then finally the map can not possibly be surjective since any odd number would not be mapped to because $\frac{n}{2} \notin \mathbb{Z}$ if n is odd.
Therefore $(\mathbb{Z}, +)$ is an infinite abelian group that is injective and operation preserving but not surjective. ■

Gallian 6.58: Show that every automorphism ϕ of the rational numbers $\mathbb{Q}$ under addition to itself has the form $\phi(x) = x\phi(1)$.

Let $\phi : \mathbb{Q} \to \mathbb{Q}$ be an arbitrary automorphism of $\mathbb{Q}$.
Then consider some $x \in \mathbb{Q}$. Then we know that x can be written as $x = \dfrac{p}{q}$ where $p, q \in \mathbb{Z}$ and $q \neq 0$.
Then since $\langle 1 \rangle = \mathbb{Z}$, we know that if $p > 0$

$$p = \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}}$$

and if $p < 0$

$$p = \underbrace{-1 - 1 - \cdots - 1}_{p \text{ times}}$$

The same argument applies to q. Then using the fact that $q \cdot x = p$, we can see that

$$\begin{aligned} \phi(q \cdot x) &= \phi\left(p\right) \\ &= \underbrace{\pm\phi\left(1\right) \pm \phi\left(1\right) \pm \phi\left(1\right) \pm \cdots \pm \phi\left(1\right)}_{p \text{ times}} \\ &= p \cdot \phi(1) \end{aligned}$$

Note that we can say that $\phi(\pm 1) = \pm\phi(1)$ because first $\phi(1) = 1 \cdot \phi(1)$. Then since ϕ is an automorphism, for any $x \in \mathbb{Q}$, $\phi(x^{-1}) = \phi(x)^{-1}$. Then since we are in $\mathbb{Q}$ under addition it follows that $\phi(x^{-1}) = \phi(-x) = -\phi(x) = \phi(x)^{-1}$. Thus $\phi(-1) = -\phi(1)$.
Then usthe equality $\phi(q \cdot x) = p \cdot \phi(1)$. Then we can see

$$\begin{aligned} p \cdot \phi(1) &= \phi(q \cdot x) \\ &= \underbrace{\pm\phi\left(x\right) \pm \phi\left(x\right) \pm \phi\left(x\right) \pm \cdots \pm \phi\left(x\right)}_{q \text{ times}} \\ &= q \cdot \phi(x) \end{aligned}$$

Thus we conclude that

$$q \cdot \phi(x) = p \cdot \phi(1) \Rightarrow \phi(x) = \frac{p}{q}\phi(1) \Rightarrow \phi(x) = x \cdot \phi(1)$$

Then we can see that this is true for any $x \in \mathbb{Q}$ except 0. However we do know that $\phi(0) = 0$ since ϕ is a homomorphism which must map the identity to the identity which is 0 in $\mathbb{Q}$ under addition. Then clearly:

$$\phi(0) = 0 = 0 \cdot \phi(0)$$

Therefore since ϕ was arbitrary we can see that for any automorphism of $\mathbb{Q}$, $\phi(x) = x \cdot \phi(x)$. ■

Evan Oman
Graduate Student
MATH 5371
Joe Gallian
November 18, 2013

Homework 6

Gallian 7.16: Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

Assume $K \leq H \leq G$ and $|K| = 42$, $|G| = 420$.
Then we know by LaGrange's Theorem that $(|K|)|(|H|)$ and $(|H|)|(|G|)$. So we know that $42|(|H|)$, $(|H|)|420$, and, since K is a proper subgroup of H and H is a proper subgroup of G, $|H| \neq 42$ and $|H| \neq 420$.
Thus $|H|$ must be a multiple of 42 less than 420 that is also a divisor of 420. Since $42 \cdot 10 = 420$, we know that the divisors of 10, when multiplied by 42, are possible orders of H.
Therefore the possible orders of G are 84 and 210. ■

Gallian 7.26: Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

Let G be a group where $|G| > 1$ and suppose that G has no proper, non-trivial subgroups.
Then by closure we know that no element has order less than $|G|$ because otherwise we would get a subgroup generated by that element. Therefore we can see that G is a cyclic group where every $g \in G$ is a genterator.
Then by Lemma 0.1 we can see that G must be finite so $|G| = n$ for some $n \in \mathbb{N}\backslash\{0, 1\}$.
Then by the Fundamental Theorem of Finite Cyclic Groups we know that for each divisor k of n, $\left\langle g^{\frac{n}{k}} \right\rangle$ must be a subgroup of G.
However since G has no proper, nontrivial subgroups we know that $\neg\exists k$ where $k \in \mathbb{N}$ and $k > 1$ such that $k|n$. This is precisely the definition of a prime number.
Therefore we can conclude that n is a prime number and ultimately that if G is a group with no proper, nontrivial subgroups then G must be cyclic with prime order.

Lemma 0.1 (A cyclic group G with no nontrivial, proper subgroups must be finite)
Let G be a cyclic group and assume that G has no nontrivial, proper subgroups and assume by contradiction that G is infinite.
Then $\exists g \in G$ such that $\langle g \rangle = G$. Now consider the set $\left\langle g^2 \right\rangle \in G$.
Then the set $\left\langle g^2 \right\rangle$ forms a subgroup of G because $e \in \left\langle g^2 \right\rangle$, for any $a, b \in \left\langle g^2 \right\rangle$ we can see that $a = g^{2n}$, $b = g^{2m}$ so

$$ab^{-1} = g^{2n}g^{-2m} = g^{2n-2m} = g^{2(n-m)} = g^{2l} \subset \left\langle g^2 \right\rangle$$

for some $l \in \mathbb{Z}$.
Thus $\left\langle g^2 \right\rangle$ forms a proper subgroup of G and arrive at a contradiction. Therefore if G is cyclic and has no proper, nontrivial subgroups then G must be finite.

■

Gallian 7.28: Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all $g \in G$. Generalize to any group of order p^2 where p is prime. Does your proof work for this generalization?

Let G be a group such that $|G| = 25$ and assume that $\forall g \in G$, $|g| \neq 5$.
Then by the Corollary 2 of LaGrange's Theorem, we know that $|g| \mid |G|$. However since the only divisors of 25 are 1, 5, and 25, the only possible order for some element $g \in G$ is 1 or 25.
However since the identity is unique we know that for any element $g \in G$ where $g \neq e$, $|g| = 25$.
Then since the order of every element is 25, by closure we know that every element is a generator of G which clearly implies that $\langle g \rangle = G$ so G is cyclic.
Therefore if the order of G is 25 and no element has order 5, we know that G is cyclic.

The argument above could easily be expanded to work for the general case:
Let G be a group such that $|G| = p^2$ where p is prime and assume that $\forall g \in G$, $|G| \neq p$.
Then by the Corollary 2 of LaGrange's Theorem, we know that $|g| \mid |G|$. However since the only divisors of p^2 are 1, p, and p^2(since p is prime), the only possible orders for some element $g \in G$ is 1 or p^2.
However since the identity is unique we know that for any element $g \in G$ where $g \neq e$, $|g| = p^2$.
Then since the order of every element is p^2, by closure we know that every element is a generator of G which clearly implies that $| \langle g \rangle = G$ so G is cyclic.
Therefore if the order of G is p^2 and no element has order p, we know that G is cyclic. ■

Gallian 7.40 Prove that a group of order 63 must have an element of order 3.

Let G be a group such that $|G| = 63$ and assume by contradiction that $\neg\exists g \in G$ such that $|g| = 3$.
Then since the order of G is 63, we know that the possible order of any element of G is $1, \cancel{3}, 7, 21, 63$ where we can automatically eliminate 3 since we assumed there are no elements of order 3.
Then for some $g \in G$ we have the following situations:

- If $|g| = 63$, then $|g^{21}| = 3$, a contradiction. Thus 63 is not a possible order.
- If $|g| = 21$, then $|g^7| = 3$, a contradiction. Thus 21 is not a possible order.
- If $|g| = 9$, then $|g^3| = 9$, a contradiction. Thus 9 is not a possible order.

Thus we are only left with the possible orders of 1 and 7. However identities are unique so there is only one element of order 1. Thus there would have to be 62 elements of order 7.
However by Corollary 1 to Theorem 4.4 we know that in any finite group the number of elements of order d is an integer multiple of $\phi(d)$. But $\phi(7) = 6$ and since $6 \nmid 62$, we arrive at a contradiction since 62 is not a multiple of 6.
Therefore in any group of order 63, there must exists some element of order 3. ■

Gallian 7.44: Prove that every subgroup of D_n of odd order is cyclic.

Consider some $H \leq G$. Then we know that there are two possible cases for H:

- <u>H has reflections</u>

  If H has reflections, we know that H must have an equal number of rotations and reflections(by property of dihedral groups).

  Thus if H has m rotations and m reflections(where R_0 is assumed to be a rotation) then $|H| = 2m$ which is even. Therefore no subgroup with a reflection can have odd order.

- H has no reflections

  If H has no reflections when we know that H must consist entirely of rotations. Thus we know that H is a subgroup of rotations and since the set of all rotations is cyclic, H must be cyclic.

Therefore the only candidate for a subgroup of D_n with odd order is a cyclic subgroup of set of the rotations so every subgroup of D_n with odd order is cyclic. ■

Gallian Grad Problem: Suppose that G is a group of order p^3, where p is prime, and G has exactly one subgroup for each divisor of p^3. Show that G is cyclic.

Let G be a finite group of order p^3 where p is prime and assume that G has exactly one subgroup for each divisor of p^3.
Then $H_1, H_2 \leq G$ where $|H_1| = p$ and $|H_2| = p^2$ are the only proper subgroups of G.
Then since p is prime, we know that H_1 is cyclic since every group of prime order is cyclic. Then we can see that every element of order p is in H_1, otherwise the other element of order p would generate another subgroup of order p, which is not allowed.
Thus we have found exactly $p - 1$ elements of order p in G and these are the only elements of order p.
Now consider $H_2 \leq G$ where $|H_2| = p^2$. Then by problem 7.28 we know that either **a)** $g^p = e \ \forall g \in H_2$ or **b)** H_2 is cyclic.
However, **a)** implies that there are $p^2 - 1$(the number of nonidentity elements in H_2) elements of order p which we know to be false. Thus **b)** must be the case that H_2 is cyclic.
Then by the Fundamental Theorem of Finite Cyclic Groups we know that H_2 has one subgroup of order p(its only nontrivial divisor since p is prime) and since G has only one subgroup of order p, we know that $H_1 \leq H_2$.
Then examining the number of elements of each order in H_2, we know that H_2 has 1 element of order 1, $p - 1$ elements of order p which tells us that there are $p^2 - (p - 1) - 1 = p^2 - p$ elements of order p^2.
Then we can see that in the entire group, there are $(1) + (p - 1) + (p^2 - p)$ elements of order (1), (p), and (p^2) respectively. Thus we have a total of p^2 elements of order less than p^3 which implies that there must be some elements of order p^3(since it is the only remaining possible order for any element).
Therefore $\exists$ an element of order p^3 in G so we can conclude that G is cyclic. ■

Evan Oman
Graduate Student
MATH 5371
Joe Gallian
November 26, 2013

Homework 7

Gallian 8.26: The group $S_3 \oplus \mathbb{Z}_2$ is isomorphic to one of the following groups: $\mathbb{Z}_{12}, \mathbb{Z}_6 \oplus \mathbb{Z}_2, A_4, D_6$. Determine which one by elimination.

First we know by property of external direct products that $|S_3 \oplus \mathbb{Z}_2| = 6 \cdot 2 = 12|$ so based off of cardinality all four options are viable.
However we know that the group $S_3 \oplus \mathbb{Z}_2$ is not cyclic(since S_3 is not cyclic and every subgroup of a cyclic group should be cyclic) so we can rule out $\mathbb{Z}_{12}$, which is clearly cyclic.
Then we know that since S_3 is not abelian, $S_3 \oplus Z_2$ can not be abelian(since every every subgroup must be abelian) so we can rule out $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ which is abelian(since abelian groups can not be isomorphic to non-abelian groups).
Then finally $[(1\ 2\ 3), 1] \in S_3 \oplus \mathbb{Z}_2$ has order 6 while the maximal order of any element in A_4 is 3. Therefore the only remaining option is D_6 so we conclude that $S_3 \oplus \mathbb{Z}_2$ is isomorphic to D_6. ■

Gallian 8.36: Find a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ that has order 9.

Since $\mathbb{Z}_{12}, \mathbb{Z}_{15}$ have subgroups of order 3 and the trivial subgroup is a subgroup of every group, we can say that $H = \langle(1, 0, 5)\rangle$, which is isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_1 \oplus \mathbb{Z}_3$, is a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ with order $3 \cdot 3 = 9$. ■

Gallian 8.42: Determine the number of cyclic subgroups of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$. Provide a generator for each of the subgroups of order 15.

In order to be a subgroup of order 15, we begin by looking for elements of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$. The table below enumerates possible elements of the form (a, b) which have order 15 in the external direct product group:

Order of $a \in \mathbb{Z}_{90}$	Order of $b \in \mathbb{Z}_{36}$	Number of Possibilities
15	1	$\phi(15) \cdot \phi(1) = 8 \cdot 1 = 8$
15	3	$\phi(15) \cdot \phi(3) = 8 \cdot 2 = 16$
5	3	$\phi(5) \cdot \phi(3) = 4 \cdot 2 = 8$

Table 1: Possible elements of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$

where each pair of values has a lcm of 15 and each order is possible by property of cyclic groups.
Then since $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$ is not cyclic, we need to determine which elements of these forms generate distinct subgroups in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$. The number of elements of order 15(enumerated by type above) is 32 and since $\phi(15) = 8$, we know that there should be $32/8 = 4$ subgroups of this form.
Then clearly $\langle(a, b)\rangle = \langle(6, 0)\rangle$ forms a subgroup of order 15 of the first form listed above. But since 15 and 1 are relatively prime we know that this is the only distinct subgroup of this form.

Additionally $\langle(a,b)\rangle = \langle(6,12)\rangle$ forms a subgroup of order 15 of the second form listed above. However, since 15 and 3 are not relatively prime we know that this is not the only subgroup of this form. We can see that the subgroup $\langle(6,24)\rangle$ is also of the second form in the table but is distinct from $\langle(6,12)\rangle$ since the a value will be different even if the b value is the same multiple times.
Finally $\langle(a,b)\rangle = \langle(18,12)\rangle$ forms a subgroup of order 15 of the last form listed above. However, since 5 and 3 are relatively prime, we know that this is the only distinct subgroup of this form.
Thus we have found the four subgroups of order 15 in $\mathbb{Z}_{90} \oplus \mathbb{Z}_{36}$:

1. $\langle(6,0)\rangle$
2. $\langle(6,12)\rangle$
3. $\langle(6,24)\rangle$
4. $\langle(18,12)\rangle$

■

Gallian 8.56: Suppose that ϕ is an isomorphism from $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ to $\mathbb{Z}_{15}$ and $\phi(2,3) = 2$. Find the element in $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ that maps to 1.

Let $\phi : \mathbb{Z}_3 \oplus \mathbb{Z}_5 \to \mathbb{Z}_{15}$ and assume $\phi(2,3) = 2$. Now let $\phi(a,b) = 1$.
Then since 1 is a generator of $\mathbb{Z}_{15}$, we know that (a,b) must generate $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ since isomorphisms map generators to generators.
Then we also know that, by property of isomorphisms, that the following must be true:

$$\phi(2,3) = 2 = (1)^2 = (\phi(a,b))^2 = \phi(a^2,b^2)$$

and since ϕ is bijective we get the following:

$$a^2 = 1 \text{ and } b^2 = 3$$

where a is mod 3 and b is mod 5.
Therefore a must be 1 and b must be 4(since $4^2 = 8 \equiv_5 3$) which both generate their respective groups. Thus we conclude that $\phi(1,4) = 1$. ■

Gallian 8.66: Express $U(165)$ as an external direct product of cyclic groups of the form $\mathbb{Z}_n$.

By Corollary to Theorem 8.3 we have

$$U(165) \cong U(3) \oplus U(5) \oplus U(11)$$

Additionally we have from the chapter that $U(p^n) \cong Z_{p^n - p^{n-1}}$ if p is a prime number. Therefore we can conclude that

$$U(165) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}$$

which is an expression of $U(165)$ in terms of the product of cyclic groups as desired. ■

Gallian 8.78: Find a subgroup of order 6 in $U(700)$.

In order to simplify this problem we will consider this group in terms of the product of finite cyclic groups. By Corollary to Theorem 8.3 we have

$$U(700) \cong U(2^2) \oplus U(5^2) \oplus U(7)$$

and then by a property from the chapter we can further simplify:

$$U(700) \cong U(2^2) \oplus U(5^2) \oplus U(7) \cong \mathbb{Z}_{4^2-2} \oplus \mathbb{Z}_{5^2-5} \oplus \mathbb{Z}7 - 7^0 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_6$$

Thus it is clear that $\langle(0,0,1)\rangle \leq \mathbb{Z}_2 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_6$ is a subgroup of order 6. The equivalent in $U(2^2) \oplus U(5^2) \oplus U(7)$ would be $\langle(1,1,6)\rangle$ which we are guaranteed to also have order 6.
Finally to translate this element back into an element in $U(700)$ we will use the translation defined in the text:

$$U_{100}(7) = \{1, 101, 201, 401, 501, 601\}$$

where we omit the term 301 since it is divisible by 7.
Thus we have found a subgroup of order 6 in $U(700)$, namely $U_{100}(7)$ stated explicitly above. ■

Evan Oman
Graduate Student
MATH 5371
Joe Gallian
November 26, 2013

Homework 7

Gallian 9.24: The group $(\mathbb{Z}_4 \oplus \mathbb{Z}_{12})/\left\langle(2,2)\right\rangle$ is isomorphic to one of $\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Determine which one by elimination.

First we know that $|Z_4 \oplus \mathbb{Z}_{12}/\left\langle(2,2)\right\rangle| = \frac{|\mathbb{Z}_4 \oplus \mathbb{Z}_{12}|}{|\langle(2,2)\rangle|} = \frac{48}{6} = 8$ so by order alone all three groups are a possibility.
First consider the group $\left\langle(2,2)\right\rangle$:

$$\{(2,2),(0,4),(2,6),(0,8),(2,10),(0,0)\}$$

Then we know that $\mathbb{Z}_8$ only has one element of order 2, the element 4. However the group $(\mathbb{Z}_4 \oplus \mathbb{Z}_{12})/\left\langle(2,2)\right\rangle$ has more at least elements 2 elements of order, namely $(1,1)\left\langle(2,2)\right\rangle$ since $(1,1)^2 \cdot (0,0)$ is $(2,2)$ which is in the original set(meaning that the cosets are the same) indicating that we are at the identity so the element has order 2, and the other element would be $(1,3)\left\langle(2,2)\right\rangle$ since $(1,3)^2 \cdot (0,0) = (2,6)$ which is also in the original coset so it has order 2.
Next we know that the element $(2,3)\left\langle(2,2)\right\rangle$ has order 4 because

- $(2,3)(0,0) = (2,3) \notin \left\langle(2,2)\right\rangle$
- $(2,3)^2(0,0) = (0,6) \notin \left\langle(2,2)\right\rangle$
- $(2,3)^3(0,0) = (2,9) \notin \left\langle(2,2)\right\rangle$
- $(2,3)^4(0,0) = (0,6) \in \left\langle(2,2)\right\rangle$

Thus after 4 iterations we arrive at the identity element so $(2,3)\left\langle(2,2)\right\rangle$ has order 4, but $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has no elements of order 4 so $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not a possibility.
Therefore we can conclude that $(\mathbb{Z}_4 \oplus \mathbb{Z}_{12})/\left\langle(2,2)\right\rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$. ■

Gallian 9.36: Determine all subgroups of $\mathbb{R}^*$ (nonzero reals under multiplication) of index 2.

The index of a subgroup is the number of distinct left cosets in $\mathbb{R}^*$. The only subgroup with two distinct left cosets is the positive reals $\mathbb{R}^+$ where the cosets are $1 \cdot \mathbb{R}$ and $-1 \cdot \mathbb{R}^+$. ■

Gallian 9.38: Let H be a normal subgroup of G and let a belong to G. If the element aH has order 3 in the group G/H and $|H| = 10$, what are the possibilities for the order of a?

Since $(aH)^3 = H$ we know that $a^3 \in H$ by property of cosets. Then since the order of an element divides the order of the group so the possible orders of a^3 are 1, 2, 5, 10.
Thus the possibilities for the order of a are 3, 6, 15, or 30. ■

Gallian 9.42: An element is called a square if it can be expressed in the form b^2 for some b. Suppose that G is an Abelian group and H is a subgroup of G. If every element of H is a square and every element of G/H is a square, prove that every element of G is a square. Does your proof remain valid when "square" is replaced by "n^{th} power," where n is any integer?

Part 1
Let G be a group and assume that every element in H is a square and assume that every element in G/H is a square.
Then since every element in the factor group is a square, for some element $g \in G$, we know that $gH = (bH)^2 = b^2H$.
Thus we can see that since $gH = b^2H$, by property of factor groups $g \in b^2H$.
Then we know that some arbitrary element of b^2H would take the form $b^2c = b^2d^2$ since every element of H is a square.
Then since G is abelian and $b, d \in G$, we know that we can write

$$b^2d^2 = bbdd = bdbd = (bd)^2$$

Thus any of element b^2H is a square and since $g \in G$ and $g \in b^2H$ we can conclude that every element of G can be written as a square.
Part 2
Yes, let G be a group and assume that every element in H is a n^{th} power and assume that every element in G/H is a n^{th} power.
Then since every element in the factor group is a n^{th} power, for some element $g \in G$, we know that $gH = (bH)^n = b^nH$.
Thus we can see that since $gH = b^nH$, by property of factor groups $g \in b^nH$.
Then we know that some arbitrary element of b^nH would take the form $b^nc = b^nd^n$ since every element of H is a n^{th} power.
Then since G is abelian and $b, d \in G$, we know that we can write

$$b^nd^n = \underbrace{b \dots b}_{n \text{ times}}\underbrace{d \dots d}_{n \text{ times}} = \underbrace{bd \dots bd}_{n \text{ times}} = (bd)^n$$

Thus any element of b^nH is a square and since $g \in G$ and $g \in b^nH$ we can conclude that every element of G can be written as a n^{th} power. ■

Gallian 8.66: Let $|G| = p^nm$, where p is prime and $\gcd(p, m) = 1$. Suppose that H is a normal subgroup of G with order p^n. If K is a subgroup of G of order p^k, show that $K \subseteq H$.

Let G, H, K be defined as above and consider the element $x \in K$. Then by Lagrange we know that $|x| \big| p^k$ which in turn implies that $|x| \big| p^n$.
Then we know that $\gcd(|x|, m) = 1$(since $|x|$ is a divisor of a prime power). Then we know that $|G\ H| = \frac{|G|}{|H|} = \frac{p^nm}{p^n} = m$ so we can say that

$$\gcd(|x|, |G\ H|) = 1 \Rightarrow \gcd(|xH|, |G/H|) = 1$$

where the implication is from the fact that $|xH| \big| |x|$, a result from problem number 37(a proof of which could be shown on requested).
However since $xH \in G\ H$, we know again by Lagrange that $|xH| \big| |G\ H|$ which in turn implies $|xH| = 1$ which finally implies that $x \in H$.
Therefore since $x \in K$ was arbitrary we can conclude that $K \subseteq H$. ■