# Final Review

Joseph C. McGuire
Dr. J. Morris
MATH 320

December 10, 2018

## 1 Let $G$ be a group, and let $x \in G$ be an element of order 40. List all elements in $< x >$ that have

### 1.1 Order 5

Using Theorem 4.2, we have $< x^k >=< x^{gcd(40,k)} >$ and $|x^k| = \frac{40}{gcd(40,k)}$. In this case, we want $\frac{40}{gcd(40,k)} = 5$. Hence $gcd(40, k) = 8$. The only $k$'s that satisfy this are: $k = 8, 16, 24$, and 32. Hence

$$|x^8| = |x^{16}| = |x^{24}| = |x^{32}| = 5,$$

by Theorem 4.2.

### 1.2 Order 10

Again using Theorem 4.2. We want to solve for all the $k$ in the equation:

$$|x^k| = \frac{40}{gcd(40, k)} = 10.$$

The only such $k$ that satisfy this are $k = 4, 12, 28$, and 36. Hence we have

$$|x^4| = |x^{12}| = |x^{28}| = |x^{36}| = 10,$$

by Theorem 4.2.

### 1.3 Order 20

Again using Theorem 4.2. We want for all the $k$ in the equation:

$$|x^k| = \frac{40}{gcd(40, k)} = 20.$$

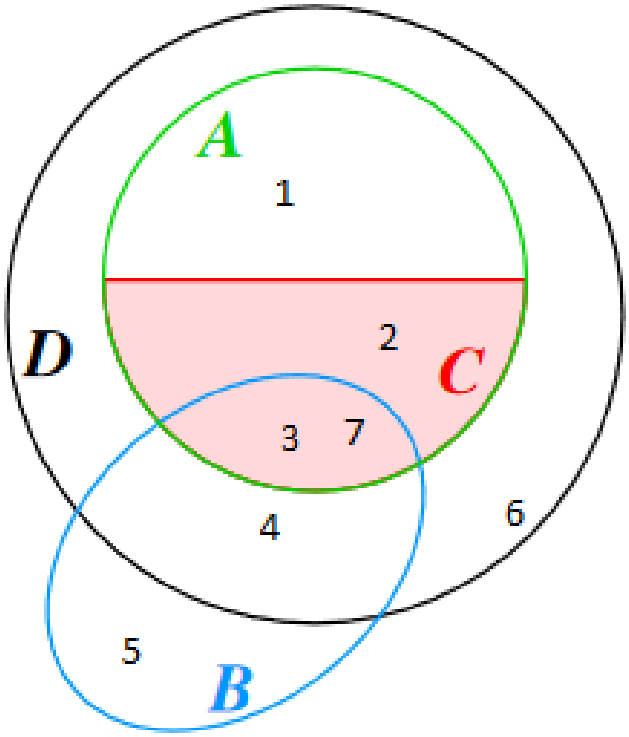
The only such $k$ that satisfy this are $k = 2, 6, 14, 18, 22, 26, 34$, and 38.

$$|x^2| = |x^6| = |x^{14}| = |x^{18}| = |x^{22}| = |x^{26}| = |x^{34}| = |x^{38}| = 20$$

## 2 Show that no two of the following five groups are isomorphic: $D_{30}, A_5, D_5 \oplus S_3, \mathbb{Z}_{60}, \mathbb{Z}_{30} \oplus \mathbb{Z}_2$

*Proof.* $(D_{30} \not\approx A_5)$
The element $R_0 \in D_{30}$ has $|R_0| = 30$, but all the elements of $A_5$ have even length, hence if $x \in A_5$, $|x| = 1, 2$, or 4.
$(D_{30} \not\approx D_5 \oplus S_3)$
Consider the element $|R_0| = 30$, but for all $x \in S_3$, we have either the length of $x$ in disjoint form is either 1 or 2 or 3. Additionally $D_5$ has elements only of order 1 and 5. Thus the elements of $D_5 \oplus S_3$ can either have order that is an LCM of a combination of these two numbers. Hence the elements of $D_5 \oplus S_3$ either has order of $1, 2, 3, 5, 10$, or 15. Thus there can't be any order-preserving bijection between the two sets. Hence there is no isomorphism between the two sets.
$(D_{30} \not\approx \mathbb{Z}_{60})$
Note that by previous exercises we have $\mathbb{Z}_{60}$ is Abelian, but $D_{30}$ is not Abelian. Thus they are non-isomorphic groups.
$(D_{30} \not\approx \mathbb{Z}_{30} \oplus \mathbb{Z}_2)$
Note that by previous example we have $D_{30}$ is non-Abelian, but $\mathbb{Z}_{30} \oplus \mathbb{Z}_2$ is Abelian.
$(A_5 \not\approx D_5 \oplus S_3)$
Note that for all elements of $x \in A_5$, we have either $|x| = 1, 2$, or 4. But for $D_5 \oplus S_3$, we have the elements of $D_5$ have order of 1 or 5, and $S_3$ has elements of order $1, 2$, or 3. By Theorem 8.1, we have $D_5 \oplus S_3$ has no element of order 4. Hence the two groups can't be isomorphic, since there can't exist an order-preserving bijection between the two groups.
$(A_5 \not\approx \mathbb{Z}_{60})$
Note that while here $|1| = 60$ in $\mathbb{Z}_{60}$, by our previous argument $A_5$ has no such element. Thus there exists no order-preserving bijection between the two groups. Hence they are not isomorphic.
$(A_5 \not\approx \mathbb{Z}_{30} \oplus \mathbb{Z}_2)$
Note that the element of $\mathbb{Z}_{30} \oplus \mathbb{Z}_2$, $|(1, 1)| = 15$, by Theorem 8.1. But again, $A_5$ has no such element with order 15. Hence there can't be any order-preserving bijection between the two sets, thus they aren't isomorphic.
$(D_5 \oplus S_3 \not\approx \mathbb{Z}_{60})$
Note that $|1| = 60$ in $\mathbb{Z}_{60}$, while $D_5 \oplus S_3$ has no such element. Hence there can exist no order-preserving bijection between the two groups. Thus they are not isomorphic.
$(D_5 \oplus S_3 \not\approx \mathbb{Z}_{30} \oplus \mathbb{Z}_2)$
Note that $D_5 \oplus S_3$ has no element of order 30. While the element $(30, 1)$ has order 30, by Theorem 8.2. Thus there exists no order-preserving bijection between the two groups.
$(\mathbb{Z}_{60} \not\approx \mathbb{Z}_{30} \oplus \mathbb{Z}_2)$
By Corollary 2 to Theorem 8.2, we have these two groups aren't isomorphic, since we have $gcd(30, 2) \neq 1$. □

**3 Let A denote the set of all integral domains, B the set of all finite rings, C the set of all fields, and D the set of all commutative rings. Draw a Venn diagram that illustrates the relationship between these four sets. Then, for each of the regions that your Venn diagram divides the plane into, find a specific example of a ring that fits all of the properties of that portion of your diagram**




**3.1 An integral domain, commutative rings, but not a field nor a finite ring.**

$\mathbb{Z}$

**3.2 An integral domain, field, and a commutative ring, but not a finite ring.**

$\mathbb{R}$

**3.3 An integral domain, field, commutative ring, and a finite ring.**

$\mathbb{Z}_p$ for any prime $p$

### 3.4 A finite commutative ring, but not a field nor an integral domain.

$\mathbb{Z}_n$ for any non-prime positive integer.

### 3.5 A finite ring, but not commutative, nor a field, nor a integral domain.

$M_n(R)$ for any finite ring $R$ and any positive integer $n$.

### 3.6 A commutative ring, but not a finite ring, nor a field, nor an integral domain.

$\mathbb{Z}_n \oplus \mathbb{Z}$, this is a commutative ring infinite, but not an integral domain if $n$ is not a prime.

### 3.7 An integral domain and a finite ring, commutative, but not a field

## 4 Recall that $\mathbb{Z}[x]$ denotes the ring of all polynomials that have coefficients in $\mathbb{Z}$. For each of the following subsets of $A$ of $\mathbb{Z}[x]$, decide (i.) whether $A$ is a subring of $\mathbb{Z}[x]$, and (ii.) whether $A$ is an ideal in $\mathbb{Z}[x]$. Justify your answer in each case.

### 4.1 $A = \{$even integers$\}$ (i.e, the set of all constant polynomials with even integer coefficients).

#### 4.1.1

*Proof.* Let $A = \{2k : k \in \mathbb{Z}\}$, then $A \subseteq \mathbb{Z}[x]$. Note that $2 \cdot 1 = 2 \in A$, hence $A \neq \emptyset$. Let $a, b \in A$. Then we have $a = 2k$ and $b = 2m$, for some $m, k \in \mathbb{Z}$. Hence $a - b = 2k - 2m = 2(k - m)$ and $a - b \in A$. Thus by the Sub-Ring Test, we have $A$ is a subring of $\mathbb{Z}[x]$. □

#### 4.1.2

By part (i.) we already have condition (i) of Theorem 14.1. But condition (ii) of Theorem 14.1 doesn't hold: Consider $4 \in A$ and $7x + 7 \in \mathbb{Z}[x]$. Then $4(7x + 7) \notin A$, thus by the Ideal Test $A$ isn't an ideal.

### 4.2 $A = \{$non-negative integers$\}$

#### 4.2.1

It is not a subring, since we have $2 \in A$ and $3 \in A$, but $2 - 3 = -1 \notin A$. Thus, by the sub-ring Test, we have $A$ is not a subring of $\mathbb{Z}_[x]$.

#### 4.2.2

Since, by definition, an ideal is a subring of $\mathbb{Z}[x]$, we have $\mathbb{Z}[x]$ is not an ideal.

### 4.3 $A = \{p(x) \in \mathbb{Z}[x] : p(0) = 0\}$

#### 4.3.1

*Proof.* Note that $A$ is all of the polynomials no constant part; that is
$A = \{a_1x + a_2x^2 + a_3x^3 + ... : a_i \in \mathbb{Z} \text{ for all } i \in \mathbb{N}\}$. Let $p, q \in A$. Then for some sequences $a_i \in \mathbb{Z}$ for all $i \in \mathbb{N}$ and $b_i \in \mathbb{Z}$ for all $i \in \mathbb{N}$, we have $p = a_1x + a_2x^2 + ...$ and $q = b_1x + b_2x^2 + ....$ Thus $p - q = (a_1 - b_1)x + (a_2 - b_2)x^2 + ....$ Then we have that $(p - q)(0) = 0$. Hence $p - q \in A$. Thus by the sub-ring test, we have $A$ is a sub-ring of $\mathbb{Z}[x]$. □

#### 4.3.2

*Proof.* By part (1.) we have the first condition holds. Then we will show the (2) condition holds: Let $a \in A$ and $r \in \mathbb{Z}[x]$. Then we have $a = a_1x + a_2x^2 + ...$ and $r = b_0 + b_1x + b_2x^2 + ....$ Next consider the following:

$$ar = (a_1x + a_2x^2 + ...)(b_0 + b_1x + b_2x^2 + ...),$$

since $a(0) = 0$, we have $(a \cdot r)(0) = 0$. Thus $ar \in A$, similarly since we are in an Abelian ring we have $ra \in A$. Thus by the Ideal Test, we have $A$ is an ideal of $\mathbb{Z}[x]$. □

## 5 Consider the ring $\mathbb{Z}_2[x]$ and the principal ideals $A = < x^2 + 1 >$ and $B = < x^2 + x + 1 >$.

### 5.1 Make an addition and multiplication table for the factor ring $\mathbb{Z}_2[x]/A$. Is $\mathbb{Z}_2[x]/A$ an integral domain? Justify your answer. (Hint: In $\mathbb{Z}_2[x]/A$, there are four elements: $A$, $1 + A$, $x + A$, and $1 + x + A$.)

| Addition $\mathbb{Z}_2[x]/A$ | $A$ | $1 + A$ | $x + A$ | $1 + x + A$ |
|---|---|---|---|---|
| $A$ | $A$ | $1 + A$ | $x + A$ | $1 + x + A$ |
| $1 + A$ | $1 + A$ | $A$ | $1 + x + A$ | $x + A$ |
| $x + A$ | $x + A$ | $1 + x + A$ | $A$ | $1 + A$ |
| $1 + x + A$ | $1 + x + A$ | $x + A$ | $1 + A$ | $A$ |

| Multiplication $\mathbb{Z}_2[x]/A$ | $A$ | $1 + A$ | $x + A$ | $1 + x + A$ |
|---|---|---|---|---|
| $A$ | $A$ | $A$ | $A$ | $A$ |
| $1 + A$ | $A$ | $1 + A$ | $x + A$ | $1 + x + A$ |
| $x + A$ | $A$ | $x + A$ | $1 + A$ | $1 + x + A$ |
| $1 + x + A$ | $A$ | $1 + x + A$ | $1 + x + A$ | $A$ |

We see from the multiplication table that $A$ is not an integral domain since $(1 + x + A)^2 = 0 + A$, where $0 + A$ is the equivalent of the zero element of this factor ring.

**5.2 Make an addition and multiplication table for the factor ring $\mathbb{Z}_2[x]/B$. Is $\mathbb{Z}_2[x]/B$ an integral domain? Justify your answer. (Hint: In $\mathbb{Z}_2[x]/B$, there are four elements: $B$, $1+B$, $x+B$, and $1+x+B$.)**

| Addition $\mathbb{Z}_2[x]/A$ | $B$ | $1+B$ | $x+B$ | $1+x+B$ |
|---|---|---|---|---|
| $B$ | $B$ | $B$ | $B$ | $B$ |
| $1+B$ | $1+B$ | $B$ | $1+x+B$ | $x+B$ |
| $x+B$ | $x+B$ | $1+x+B$ | $B$ | $1+B$ |
| $1+x+B$ | $1+x+B$ | $x+B$ | $1+B$ | $B$ |

| Multiplication $\mathbb{Z}_2[x]/B$ | $B$ | $1+B$ | $x+B$ | $1+x+B$ |
|---|---|---|---|---|
| $B$ | $B$ | $B$ | $B$ | $B$ |
| $1+B$ | $B$ | $1+B$ | $x+B$ | $1+x+B$ |
| $x+B$ | $B$ | $x+B$ | $1+x+B$ | $1+B$ |
| $1+x+B$ | $B$ | $1+x+B$ | $1+B$ | $x+B$ |

We have by the above Cayley table that every non-zero element of the factor ring has a multiplicative inverse and no non-zero zero divisors, thus $\mathbb{Z}_2[x]/B$ is both an integral domain and a field.

**5.3 Which, if either, of the ideals $A$ or $B$ are maximal in $\mathbb{Z}_2[x]$? Justify your answer.**

We have by Theorem 14.4, that $B$ is a maximal ideal, while $A$ is not.

# 6 For each of the following, use Burnside's Theorem to count the number of different ways to color the vertices of a regular octagon given the specified colors and allowed motions of the octagon.

**6.1 There are 4 colors available, and the octagon can be rotated but not flipped.**

First note that here we have $S = 4^8$ and $G = D_8 \setminus \{\text{All the flips}\}$.

| Types of Elements of $G$ | $\#elements$ | $\lvert fix(\phi)\rvert$ |
|---|---|---|
| $(1)$ | 1 | $4^8$ |
| $(a\ b\ c\ d\ e\ f\ g\ h)$ | 4 | $4^1$ |
| $(a\ b\ c\ d)(e\ f\ g\ h)$ | 2 | $4^2$ |
| $(a\ b)(c\ d)(d\ e)(g\ h)$ | 1 | $4^4$ |

Hence by Burnside's Theorem, we have the number of orbits is:

$$\frac{1}{|G|}\sum_{\phi\in G}|fix(\phi)| = \frac{1}{8}(1\cdot 4^8 + 4^4\cdot 4^1 + 2\cdot 4^2 + 1\cdot 4^4) = 8230.$$

How we did this was: first, take a simple labeling and use that to come up with a cycle notation for the symmetries. Secondly, count the number of rotations that have the same general form. Lastly, take the number of colors $k$, and the number of disjoint cycles $n$ and you have the $|fix(\phi)| = k^n$.

### 6.2 There are 4 colors available, and the octagon can be rotated or flipped.

| Types of Elements of $G$ | $\#elements$ | $\lvert fix(\phi)\rvert$ |
|---|---|---|
| $(1)$ | 1 | $4^8$ |
| $(a\ b\ c\ d\ e\ f\ g\ h)$ | 4 | $4^1$ |
| $(a\ b\ c\ d)(e\ f\ g\ h)$ | 2 | $4^2$ |
| $(a\ b)(c\ d)(d\ e)(g\ h)$ | 5 | $4^4$ |
| $(a)(b)(c\ d)(e\ f)(g\ h)$ | 4 | $4^5$ |

Hence by Burnside's Theorem we have the total number of orbits, hence the total number of different ways of coloring the vertices of a regular octagon:

$$\frac{1}{|G|}\sum_{\phi\in G}|fix(\phi)| = \frac{1}{16}(1\cdot 4^8 + 4\cdot 4^1 + 2\cdot 4^2 + 5\cdot 4^4 + 4\cdot 4^4) = 4435$$

### 6.3 There are n colors available, and the octagon can be rotated or flipped.

| Types of Elements of $G$ | $\#elements$ | $\lvert fix(\phi)\rvert$ |
|---|---|---|
| $(1)$ | 1 | $n^8$ |
| $(a\ b\ c\ d\ e\ f\ g\ h)$ | 4 | $n^1$ |
| $(a\ b\ c\ d)(e\ f\ g\ h)$ | 2 | $n^2$ |
| $(a\ b)(c\ d)(d\ e)(g\ h)$ | 5 | $n^4$ |
| $(a)(b)(c\ d)(e\ f)(g\ h)$ | 4 | $n^5$ |

By Burnside's Theorem we get the following formula:

$$\frac{1}{|G|}\sum_{\phi\in G}|fix(\phi)| = \frac{n^8 + 4n^5 + 5n^4 + 2n^2 + 4n}{16} \text{ ways.}$$

## 7 Complete the outline below to finish the proof of the following theorem:

**Theorem**. Every finite field has "prime power order"; that is, every finite field has order $p^n$, where $p$ is a prime and $n$ is a positive integer.

**Proof**. Let $F$ be a finite field, with $|F| = k$ and $char(F) = m$. Let $p$ and $q$ be any primes that divide $k$. Since $F$ is an Abelian group under the addition operation, we know from Theorem 9.5 that we can choose $a, b \in F$ such that the additive order of $a$ is $p$ and the additive order of $b$ is $q$.

### 7.1 Explain why $k \geq 2$.

By the definition of a field, it must have a unity element and an additive identity; i.e. $0, 1 \in F$. Thus $|F| \geq 2$.

### 7.2 Prove that $m$ is prime.

By Theorem 13.4, we know that the characteristic of any integral domain is 0 or prime; that is, it's either infinite or has prime characteristic. Since we know every field is an integral domain, and since $F$ is a finite field, we have that $F$ has a prime characteristic. Thus $m$ is prime.

### 7.3 Prove that $p = q$, and explain how this fact completes the proof of the theorem.

*Proof.* By our previous result, we have that $m$ is prime. Since $char(F) = m$, we have for all $x \in F$ $xm = 0$, where 0 is the additive identity of $F$. Also we have $|a| = p$ and $|b| = q$. Hence $ap = 0$ and $bq = 0$. Thus, by Corollary 2 to Theorem 4.1, that $p|m$ and $q|m$. But since we assumed $p$ and $q$ are prime, we have $p = m$ and $q = m$. Thus $p = q$. □

We have shown that $k$ is made up of only one distinct prime, since there aren't any more than 1 prime that divides the order of a finite field. Hence $|F| = p^n$, where $p$ is prime and $n$ is a positive integer.

## 8 Prove that a commutative ring $R$ with unity is a field if and only it, for every ideal $I$ in $R$, we have either $I = \{0\}$ or $I = R$.

*Proof.* ($\longrightarrow$) Assume that $R$ is a field. Let $I$ be any ideal in $R$. If $I = \{0\}$, we are done, so we will assume that $I \neq \{0\}$. [To show: $I = R$]
Then there exists a nonzero $x \in I$. Since $R$ is a field, $x$ has a multiplicative inverse $x^{-1} \in R$. Since $I$ is an ideal, we have

$$1 = x^{-1}x \in I.$$

Now that any $r \in R$. Since $1 \in I$, we have

$$r = 1 \cdot r \in I,$$

by the absorption property again. Thus $R \subseteq I$. Since $I \subseteq R$ is assumed, we have $R = I$.
($\longleftarrow$) Assume $R$ is not a field. [To show: there exists an ideal of $R$ that's not zero and not the entire ring.] Then we can choose a nonzero element $y \in R$ such that $y$ is not a unit. Now consider the principal ideal $I = < y > = \{ay : a \in R\}$. Since $y \in I$, $I \neq \{0\}$. On the other hand, since $y$ is not a unit, $ay \neq 1$ for all $a \in R$. It follows that $q \notin I$, so $I \neq R$. □

## 9 Up to isomorphism, how many distinct Abelian groups are there of the indicated order? Write down one group from each isomorphism class.

### 9.1 order 32

### 9.2 order 400

### 9.3 order 573 (Note: $573 = 3 \cdot 191$ is prime.)

## 10 Let $H_1$ and $H_2$ be subgroups of a group $G$. Prove that $H_1 \cap H_2$ is a subgroup of $G$.

*Proof.* Let $G$ be a group and $H_1$ and $H_2$ be subgroups of $G$. Note then that $e \in H_1$ and $e \in H_2$, where $e$ is the identity element of $G$. Hence $e \in H_1 \cap H_2$, thus $H_1 \cap H_2 \neq \emptyset$. Next we will show that $H_1 \cap H_2$ is a subgroup using Theorem 3.2 (Two-Step Subgroup Test).
($a^{-1} \in H_1 \cap H_2$)

Let $a \in H_1 \cap H_2$, then $a \in H_1$ and $a \in H_2$. Thus, since $H_1$ and $H_2$ are subgroups of $G$ we have $a^{-1} \in H_1$ and $a^{-1} \in H_2$, thus $a^{-1} \in H_1 \cap H_2$.
($ab \in H_1 \cap H_2$)

Let $a, b \in H_1 \cap H_2$. Then we have $a \in H_1$, $a \in H_2$, $b \in H_1$, and $b \in H_2$. Furthermore, since $H_1$ and $H_2$, we have $ab \in H_1$ and $ab \in H_2$. Hence $ab \in H_1 \cap H_2$.

Thus, by Theorem 3.2 (Two-Step Subgroup Test), we have $H_1 \cap H_2$ is a subgroup of $G$. □