Math 94 Professor: Padraic Bartlett

Lecture 8: Abstract Algebra

Week 8 *UCSB 2015*

This is the eighth week of the Mathematics Subject Test GRE prep course; here, we run a very rough-and-tumble review of **abstract algebra**! As always, this field is much bigger than one class; accordingly, we focus our attention on key definitions and results.

1 Groups: Definitions and Theorems

Definition. A **group** is a set G along with some operation $\cdot$ that takes in two elements and outputs another element of our group, such that we satisfy the following properties:

- **Identity**: there is a unique identity element $e \in G$ such that for any other $g \in G$, we have $e \cdot g = g \cdot e = g$.
- **Inverses**: for any $g \in G$, there is a unique g^{-1} such that $g \cdot g^{-1} = g^{-1} g = e$.
- **Associativity**: for any three $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definition. A **subgroup** H of a group $\langle G, \cdot \rangle$ is any subset H of G such that H is also a group with respect to the $\cdot$ operation.

Definition. A group $\langle G, \cdot \rangle$ is called **abelian**, or **commutative**, if it satisfies the following additional property:

- **Commutativity**: for any $a, b \in G$, $a \cdot b = b \cdot a$.

There are **many** different examples of groups:

Example.

1. The real numbers with respect to addition, which we denote as $\langle \mathbb{R}, + \rangle$, is a group: it has the identity 0, any element x has an inverse $-x$, and it satisfies associativity.
2. Conversely, the real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}, \cdot \rangle$, is **not** a group: the element $0 \in \mathbb{R}$ has no inverse, as there is nothing we can multiply 0 by to get to 1!
3. The nonzero real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}^{\times}, \cdot \rangle$, is a group! The identity in this group is 1, every element x has an inverse $1/x$ such that $x \cdot (1/x) = 1$, and this group satisfies associativity.
4. The integers with respect to addition, $\langle \mathbb{Z}, + \rangle$ form a group!
5. The integers with respect to multiplication, $\langle \mathbb{Z}, \cdot \rangle$ do not form a group: for example, there is no integer we can multiply 2 by to get to 1.

6. The natural numbers $\mathbb{N}$ are not a group with respect to either addition or multiplication. For example: in addition, there is no element $-1 \in \mathbb{N}$ that we can add to 1 to get to 0, and in multiplication there is no natural number we can multiply 2 by to get to 1.

7. $GL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices, is a group under the operation of matrix multiplication. Notice that this group is an example of a **non-abelian** group, as there are many matrices for which $AB \neq BA$: consider $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ versus $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

8. $SL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices with determinant 1, is also a group under the operation of matrix multiplication; this is because the property of being determinant 1 is preserved under taking inverses and multiplication for matrices.

9. The integers mod n, $\mathbb{Z}/n\mathbb{Z}$ is a group with respect to addition! As a reminder, the object $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$ is defined as follows:

   - Your set is the numbers $\{0, 1, 2, \ldots n-1\}$.
   - Your addition operation is the operation "addition mod n," defined as follows: we say that $a + b \equiv c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

     For example, suppose that $n = 3$. Then $1 + 1 \equiv 2 \mod 3$, and $2 + 2 \equiv 1 \mod 3$.
   - Similarly, our multiplication operation is the operation "multiplication mod n," written $a \cdot b \equiv c \mod n$, and holds whenever $a + b$ and c differ by a multiple of n.

     For example, if $n = 7$, then $2 \cdot 3 \equiv 6 \mod 7$, $4 \cdot 4 \equiv 2 \mod 7$, and $6 \cdot 4 \equiv 3 \mod 7$.

10. $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots p-1\}$ is a commutative group with respect to the operation of multiplication mod p, if and only if p is a prime.

    Seeing this is not too difficult, and is a useful thing to do to remind ourselves about how modular arithmetic works:

    - It is easy to see that $(\mathbb{Z}/p\mathbb{Z})^\times$ satisfies **associativity**, **identity** and **commutativity**, simply because these properties are "inherited" from the integers $\mathbb{Z}$: i.e. if $a \cdot b = b \cdot a$, then surely $a \cdot b \cong b \cdot a \mod p$, because equality implies equivalence mod p!
    - Therefore, the only property we need to check is inverses. We first deal with the case where p is not prime. Write $p = mn$ for two positive integers $m, n \neq 1$; notice that because both of these values must be smaller than p if their product is p, both m and n live in the set $\{1, \ldots p-1\}$.

Consider the element n. In particular, notice that for any k, we have

$$\begin{aligned} & kn \equiv x \mod p \\ \Rightarrow & kn - x \text{ is a multiple of } p \\ \Rightarrow & kn - x \text{ is a multiple of } mn \\ \Rightarrow & kn - x \text{ is a multiple of } n \\ \Rightarrow & x \text{ is a multiple of } n. \end{aligned}$$

(If none of the above deductions make sense, reason them out in your head!) Because of this, we can see that n has no inverse in $(\mathbb{Z}/p\mathbb{Z})^\times$, as kn is only congruent to multiples of n, and 1 is not a multiple of n.

- The converse — showing that if p is prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ has inverses — is a little trickier. We do this as follows: first, we prove the following claim.

  Claim. For any $a, b \in \{0, \ldots p-1\}$, if $a \cdot b \equiv 0 \mod p$, then at least one of a, b are equal to 0.

  Proof. Take any a, b in $\{0, \ldots p-1\}$. If one of a, b are equal to 0, then we know that $a \cdot b = 0$ in the normal "multiplying integers" world that we've lived in our whole lives. In particular, this means that $a \cdot b \equiv 0 \mod p$ as well.
  Now, suppose that neither a nor b are equal to 0. Take both a and b. Recall, from grade school, the concept of **factorization**:

  Observation. Take any nonzero natural number n. We can write n as a product of prime numbers $n_1 \cdot \ldots \cdot n_k$; we think of these prime numbers $n_1, \ldots n_k$ as the "factors" of n. Furthermore, these factors are **unique**, up to the order we write them in: i.e. there is only one way to write n as a product of prime numbers, up to the order in which we write those primes. (For example: while you could say that 60 can be factored as both $2 \cdot 2 \cdot 3 \cdot 5$ and as $3 \cdot 2 \cdot 5 \cdot 2$, those two factorizations are the same if we don't care about the order we write our numbers in.)
  In the special case where $n = 1$, we think of this as already factored into the "trivial" product of no prime numbers.

  Take a, and write it as a product of prime numbers $a_1 \cdot \ldots \cdot a_k$. Do the same for b, and write it as a product of primes $b_1 \cdot \ldots \cdot b_m$. Notice that because a and b are both numbers that are strictly between 0 and $n-1$, n cannot be one of these prime numbers (because positive multiples of n must be greater than n!)
  In particular, this tells us that the number $a \cdot b$ on one hand can be written as the product of primes $a_1 \cdot \ldots \cdot a_k \cdot b_1 \cdot \ldots \cdot b_m$, and on the other hand (because factorizations into primes are unique, up to ordering!) that there is no n in the prime factorization of $a \cdot b$.
  Conversely, for any natural number k, the number $k \cdot n$ **must** have a factor of n in its prime factorization. This is because if we factor k into prime numbers $k_1 \cdot \ldots \cdot k_j$, we have $k \cdot n = k_1 \cdot \ldots \cdot k_j \cdot n$, which is a factorization into prime numbers and therefore (up to the order we write our primes) is unique!

In particular, this tells us that for any k, the quantities $a \cdot b$ and $k \cdot p$ are distinct; one of them has a factor of p, and the other does not. Therefore, we have shown that if both a and b are nonzero, then $a \cdot b$ cannot be equal to a multiple of p — in other words, $a \cdot b$ is not congruent to 0 modulo p! Therefore, the only way to pick two $a, b \in \{0, \dots p-1\}$ such that $a \cdot b$ is congruent to 0 modulo p is if at least one of them is equal to 0, as claimed. □

- From here, the proof that our group has inverses is pretty straightforward. Take any $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, and suppose for contradiction that it did not have any inverses. Look at the multiplication table for x in $(\mathbb{Z}/p\mathbb{Z})^\times$:

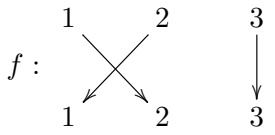
	1	2	3	...	$p-1$
x	?	?	?	...	?

If x doesn't have an inverse, then 1 does not show up in the above table! The above table has p slots, and if we're trying to fill it without using 1, we only have $p-1$ values to put in this table; therefore some value is repeated! In other words, there must be two distinct values $k < l$ with $xl \equiv xk \mod p$.

Consequently, we have $x(l-k) \equiv 0 \mod p$, which by our above observation means that one of $x, (l-k)$ are equal to 0. But x is nonzero, as it's actually in $(\mathbb{Z}/p\mathbb{Z})^\times$: therefore, $l-k$ is equal to 0, i.e. $l = k$. But we said that k, l are distinct; so we have a contradiction! Therefore, every element x has an inverse, as claimed.

11. The **symmetric group** S_n is the collection of all of the permutations on the set $\{1, \dots n\}$, where our group operation is composition. In case you haven't seen this before:

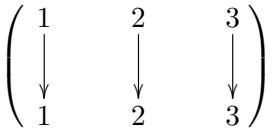
- A **permutation** of a set is just a bijective function on that set. For example, one bijection on the set $\{1, 2, 3\}$ could be the map f that sends 1 to 2, 2 to 1, and 3 to 3.
- One way that people often denote functions and bijections is via "arrow" notation: i.e. to describe the map f that we gave above, we could write

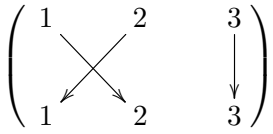


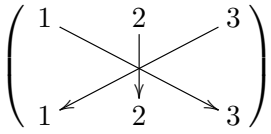
- This, however, is not the most space-friendly way to write out a permutation. A much more condensed way to write down a permutation is using something called **cycle notation**. In particular: suppose that we want to denote the permutation that sends $a_1 \to a_2$, $a_2 \to a_3$, $\dots a_{n-1} \to a_n$, $a_n \to a_1$, and does not change any of the other elements (i.e. keeps them all the same.) In this case, we would denote this permutation using cycle notation as the permutation

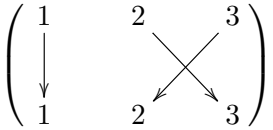
$$(a_1 a_2 a_3 \dots a_n).$$

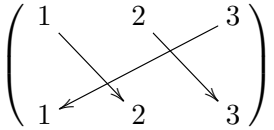
To illustrate this notation, we describe all of the six possible permutations on $\{1, 2, 3\}$ using both the arrow and the cycle notations:

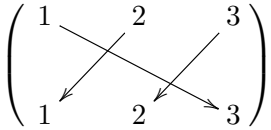
id : 

(12) : 

(13) : 

(23) : 

(123) : 

(132) : 

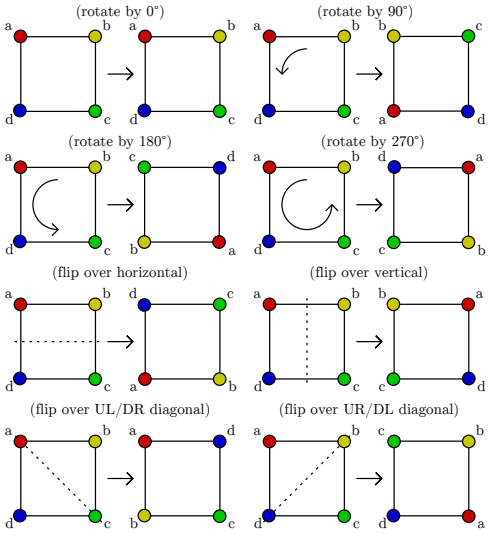
The symmetric group has several useful properties. Two notable ones are the following:

Claim. We can write any $\sigma \in S_n$ as a product of transpositions[1].

Claim. For any finite group G, there is some n such that G is a subgroup of S_n.

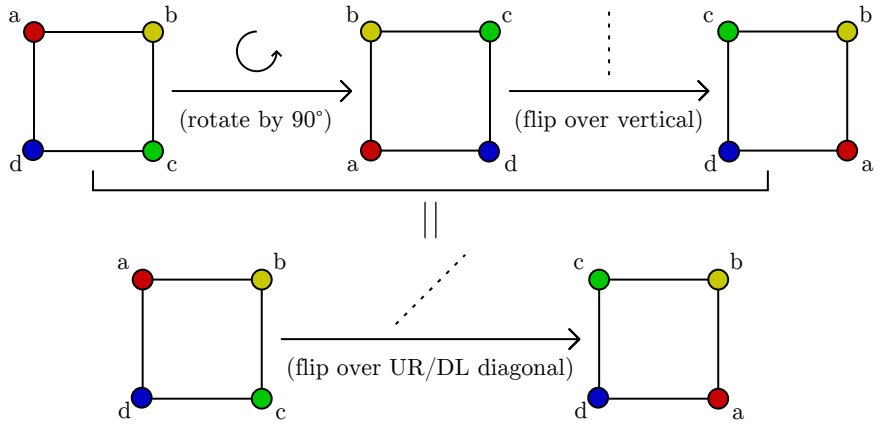
12. The **dihedral group of order** $2n$, denoted D_{2n}, is constructed as follows:

    Consider a regular n-gon. There are a number of geometric transformations, or **similarities**, that we can apply that send this n-gon to "itself" without stretching or tearing the shape: i.e. there are several rotations and reflections that when applied to a n-gon do not change the n-gon. For example, given a square, we can rotate the plane by $0°, 90°, 180°$, or $270°$, or flip over one of the horizontal, vertical, top-left/bottom-right, or the top-right/bottom-left axes:



[1] A permutation $\sigma \in S_n$ is called a **transposition** if we can write $\sigma = (ab)$, for two distinct values $a, b \in \{1, \ldots n\}$.

Given two such transformations f, g, we can compose them to get a new transformation $f \circ g$. Notice that because these two transformations each individually send the n-gon to itself, their composition also sends the n-gon to itself! Therefore composition is a well-defined operation that we can use to combine two transformations.



This is a group!

Now that we have some examples of groups down, we list some useful concepts and definitions for studying groups:

Definition. Take any two groups $\langle G, \cdot \rangle, \langle H, \star \rangle$, and any map $\varphi : G \to H$. We say that φ is a **group isomorphism** if it satisfies the following two properties:

1. **Preserves size**: φ is a bijection[2].
2. **Preserves structure**: φ, in a sense, sends $\cdot$ to $\star$. To describe this formally, we say the following:

$$\forall g_1, g_2 \in G, \quad \varphi(g_1 \cdot g_2) = \varphi(g_1) \star \varphi(g_2).$$

This property "preserves structure" in the following sense: suppose that we have two elements we want to multiply together in H. Because φ is a bijection, we can write these two elements as $\varphi(g_1), \varphi(g_2)$. Our property says that $\varphi(g_1 \cdot g_2) = \varphi(g_1) \star \varphi(g_2)$: in other words, if we want to multiply our two elements in H together, we can do so using either the G-operation $\cdot$ by calculating $\varphi(g_1 \cdot g_2)$, or by using the H-operation $\star$ by calculating $\varphi(g_1) \star \varphi(g_2)$.

Similarly, if we want to multiply any two elements g_1, g_2 in G together, we can see that $g_1 \cdot g_2 = \varphi^{-1}(\varphi(g_1 \cdot g_2)) = \varphi^{-1}(\varphi(g_1) \star \varphi(g_2))$. So, again, we can multiply elements using either G or H's operation! To choose which operation we use, we just need to apply φ or φ^{-1} as appropriate to get to the desired set, and perform our calculations there.

[2]Notice that this means that there is an inverse map $\varphi^{-1} : H \to G$, defined by $\varphi^{-1}(h) =$ the unique $g \in G$ such that $\varphi(g) = h$.

Definition. Take any two groups $\langle G, \cdot \rangle, \langle H, \star \rangle$, and any map $\varphi : G \to H$. We say that φ is a **group homomorphism** if it satisfies the "preserves structure" property above.

Theorem. If G, H are groups and $\varphi : G \to H$ is a homomorphism, then $ker(\varphi) = \{g \in G \mid \varphi(g) = id\}$ is a subgroup of G, and for any subgroup S of G, $\varphi(S) = \{\varphi(s) \mid s \in S\}$ is a subgroup of H.

Definition. A subgroup H of a group G is called **normal** if for any $g \in G$, the **left and right cosets**[3] gH, Hg are equal. We write $H \trianglelefteq G$ to denote this property.

Theorem. Suppose G is a group and H is a normal subgroup. Define the set G/H to be the collection of all of the distinct left cosets gH of H in G. This set forms something called the **quotient group** of G by H, if we define $g_1H \cdot g_2H = (g_1g_2)H$. This is a useful construction, and comes up all the time: for example, you can think of $\mathbb{Z}/n\mathbb{Z}$ as a quotient group, where G is $\mathbb{Z}$ and $H = n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$.

Definition. Take any group $\langle G, \cdot \rangle$ of order n: that is, any group G consisting of n distinct elements. We can create a **group table** corresponding to G as follows:

- Take any ordering $r_1, \ldots r_n$ of the n elements of G: we use these elements to label our rows.
- Take any other ordering $c_1, \ldots c_n$ of the n elements of G: we use these elements to label our columns. (This ordering is usually the same as that for the rows, but it does not have to be.)
- Using these two orderings, we create a $n \times n$ array, called the **group table** of G, as follows: in each cell (i, j), we put the entry $r_i \cdot c_j$.

Theorem. Two groups $\langle G, \cdot \rangle, \langle H, \star \rangle$ are isomorphic if and only if there is a bijection $\varphi : G \to H$ such that when we apply φ to a group table of G, we get a group table of H.

Theorem. (Cayley.) Let $\langle G, \cdot \rangle$ be a finite group, and $g \in G$ be any element of G. Define the **order** of g to be the smallest value of n such that $g^n = id$. Then the order of g always divides the total number of elements in G, $|G|$.

More generally, suppose that H is any subgroup of G. Then $|H|$ divides $|G|$.

This theorem has a useful special case when we consider the group $(\mathbb{Z}/p\mathbb{Z})^\times$:

Theorem. Fermat's Little Theorem. Let p be a prime number. Take any $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Then

$$a^{p-1} \equiv 1 \mod p.$$

[3] The **left coset** gH of a subgroup H by an element g is the set $\{g \cdot h \mid h \in H\}$. Basically, it's H if you "act" on each element by g. Right cosets are the same, but with Hg instead.

Theorem. Any finite abelian group G is isomorphic to a **direct sum**[4] of groups of the form $\mathbb{Z}/p_j^{k_j}\mathbb{Z}$. In other words, for any finite abelian group G, we can find primes $p_1, \dots p_l$ and natural numbers $k_1, \dots k_l$ such that

$$G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{k_l}}.$$

Groups are not the only algebraic objects people study:

2 Rings and Fields: Definitions and Theorems

Definition. A **ring** is a set R along with two operations $+, \cdot$ so that

- $\langle R, + \rangle$ is an abelian group.
- $\langle R, \cdot \rangle$ satisfies the associativity and identity properties.
- R satisfies the distributive property: i.e. for any $a, b, c \in R$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$.
- The identity for $+$ is not the identity for $\cdot$.

Some people will denote a ring with a multiplicative identity as a "ring with unity." I believe it is slightly more standard to assume that all rings have multiplicative identities, and in the odd instance that you need to refer to a ring without a multiplicative identity as a "rng."

Many of the examples we saw of groups are also rings:

Example.
1. The integers with respect to addition and multiplication form a ring, as do the rationals, reals, and complex number systems.
2. The **Gaussian integers** $\mathbb{Z}[i]$, consisting of the set of all complex numbers $\{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$ form a ring with respect to addition and multiplication.

$\mathbb{Z}/n\mathbb{Z}$ is a ring for any n.

Definition. A **integral domain** is any ring R where the following property holds:

- For any $a, b \in R$, if $ab = 0$, then at least one of a or b is 0.

Example.
1. The integers with respect to addition and multiplication form a integral domain, as do the rationals, reals, and complex number systems.

[4] A group G is called the direct sum of two groups H_1, H_2 if the following properties hold:

- Both H_1, H_2 are normal subgroups of G.
- $H_1 \cap H_2$ is the identity; i.e. these two subgroups only overlap at the identity element.
- Any element in G can be expressed as a finite combination of elements from H_1, H_2.

We think of $G = H_1 \oplus H_2$.

2. $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain for any compositite n: if we can write $n = ab$ for two $a, b < n$, then we have that $a \cdot b \equiv 0 \mod n$, while neither a, b are multiples of n (and thus not equivalent to 0).

Definition. A **field** is any ring R where $\langle R^\times, \cdot \rangle$ is a group. (By $R^\times$, we mean the set of all elements in R other than the additive identity.)

Example. 1. The integers with respect to addition and multiplication are not a field.

2. The rationals, reals, and complex number systems are fields with respect to addition and multiplication!

3. $\mathbb{Z}/p\mathbb{Z}$ is a field with respect to addition and multiplication.

There are many many theorems about rings and fields; however, the GRE will not require you to know almost all of them. Instead, they mostly want you to be familiar with what they are, and how they are defined!

To illustrate how the GRE tests you on these concepts, we run a few practice problems here:

3 Sample GRE problems

Problem. Consider the set G made out of the four complex numbers $\{1, -1, i, -i\}$. This is a group under the operation of complex multiplication. Which of the following three statements are true?

1. The map $z \mapsto \overline{z}$ is a homomorphism.

2. The map $z \mapsto z^2$ is a homomorphism.

3. Every homomorphism $G \to G$ is of the form $z \mapsto z^k$, for some $k \in \mathbb{N}$.

(a) 1 only.	(b) 1 and 2 only.	(c) 2 and 3 only.	(d) 1 and 2 only.	(e) 1, 2 and 3.

Answer. We can answer this problem quickly by classifying all possible homomorphisms $\varphi : G \to G$. We can first notice that we must send 1 to 1 if we are a homomorphism. To see this, notice that $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$, and therefore by canceling a $\varphi(1)$ on both sides we have $1 = \varphi(1)$.

Now, consider where to send i. If we have $\varphi(i) = i$, then we must have $\varphi(-1) = \varphi(i^2) = \varphi(i)\varphi(i) = i \cdot i = -1$, and $\varphi(-i) = \varphi(i^3) = \varphi(i)\varphi(i)\varphi(i) = i^3 = -i$. So we're the identity, and also we are the map $z \mapsto z^3$.

If we have $\varphi(i) = 1$, then we must have $\varphi(-1) = \varphi(i^2) = \varphi(i)\varphi(i) = 1 \cdot 1 = 1$, and $\varphi(-i) = \varphi(i^3) = \varphi(i)\varphi(i)\varphi(i) = 1^3 = 1$. So we're the map that sends everything to 1; alternately, we're the map $z \mapsto z^4$.

Similarly, if we have $\varphi(i) = -1$, then we must have $\varphi(-1) = \varphi(i^2) = \varphi(i)\varphi(i) = -1 \cdot -1 = 1$, and $\varphi(-i) = \varphi(i^3) = \varphi(i)\varphi(i)\varphi(i) = (-1)^3 = -1$. So we're the map $z \mapsto z^2$.

The last possibility is if we have $\varphi(i) = -i$, then we must have $\varphi(-1) = \varphi(i^2) = \varphi(i)\varphi(i) = -i \cdot -i = -1$, and $\varphi(-i) = \varphi(i^3) = \varphi(i)\varphi(i)\varphi(i) = (-i)^3 = i$. So we're the map $z \mapsto \overline{z}$, or alternately the map $z \mapsto z^3$.

As a result, all of the claims 1,2,3 are all true; so our answer is e.

Problem. Let R be a ring. Define a **right ideal** of R as any subset U of R such that

- U is an additive subgroup of R.
- For any $r \in R, u \in U$, we have $ur \in U$.

Suppose that R only has two distinct right ideals. Which of the following properties must hold for R?

1. R contains infinitely many elements.
2. R is commutative.
3. R is a division ring; that is, every nonzero element in R has a multiplicative inverse.

(a) 1 only.	(b) 2 only.	(c) 3 only.	(d) 2 and 3 only.	(e) 1, 2 and 3.

Answer. We first notice that any ring always has two ideals, namely $\{0\}$ and R.

The first property is eliminated by noticing that $R = \mathbb{Z}/2\mathbb{Z}$ is a ring. Its only additive subgroups are $\{0\}$ and R, so in particular those are its only two ideals, and this group is clearly finite.

The second property is eliminated by recalling the quaternions $\mathbb{H}$, which are a noncommutative ring!

Finally, we can verify that the third property must hold. To see this, take any a, and consider the set $aR = \{ar \mid r \in R\}$. This is an additive subgroup, and also a right ideal! Therefore it is either the all-zero subgroup (only if $a = 0$, as otherwise $a \cdot 1 = a \neq 0$) or all of R. But this means that there is some $ar \in aR, s \in R$ such that $ars = 1$; i.e. $rs = a^{-1}$. So a has an inverse!

This leaves 3 as the only possibility.