Math 250, Fall 2019

Groups, Rings and Fields, Fall 2019

Richard E. Borcherds, 219 Dwinelle, 9:30-11AM

Contents

1 Groups

There are two definitions to define a group.

Definition 1.1 (Concrete definition)
A group is a symmetries of something 1:1 map preserving "structure".

Example 1.2
Consider the rotation of a rectangle, we have a group of order 4.

Example 1.3
Consider the rotation of a icosahedron, we are able to obtain a group of order 60.

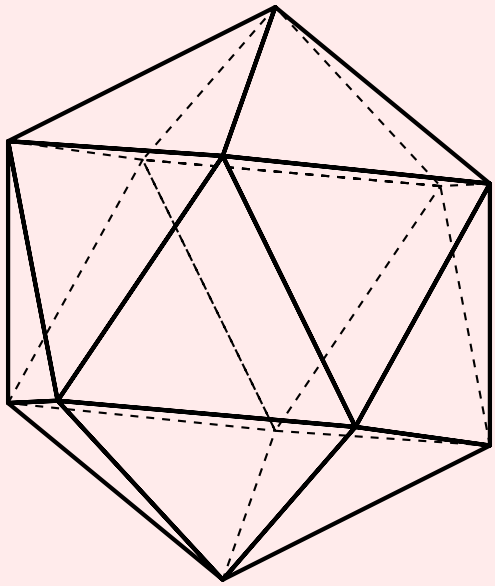


Image of a Icosahedron

Example 1.4
Let V be a n-dimensional over $\mathbb{R}$. The general linear group $GL_n(\mathbb{R})$, all matrices with $\det \neq 0$ from a group.

Definition 1.5 (Abstract Definition, Cayley)

A group is a set G with a binary operation $a+b$ or $a \times b$ or $a \circ b$ or ab (notation sucks) such that

1. Identity element 0, 1, or e, i,e $a1 = 1a = a$.
2. Each element has inverse a^{-1}, i,e $aa^{-1} = a^{-1}a = 1$.
3. Associative $(ab)c = a(bc)$ for all $a, b, c \in G$

Definition 1.6

A group G acts on S means given operation

$$G \times S \to S$$

such that $1s = s$ and $a(bs) = ab(s)$.

Example 1.7

Let G be the icosahedron group and let S be the icosahedron.

Question 1.8

How does G acts on G?

Definition 1.9

There are 8 different types of actions

1. $g(s) = s$, left action (trivial)
2. $g(s) = gs$
3. $g(s) = sg^{-1}$
4. $g(s) = gsg^{-1}$, adjoint action

Note that all of these are left actions of the group, then similarly there are also 4 right group actions. $S \times G \to S$

1. $sg = s$
2. $sg = sg$
3. $sg = g^{-1}s$
4. $sg = g^{-1}sg$

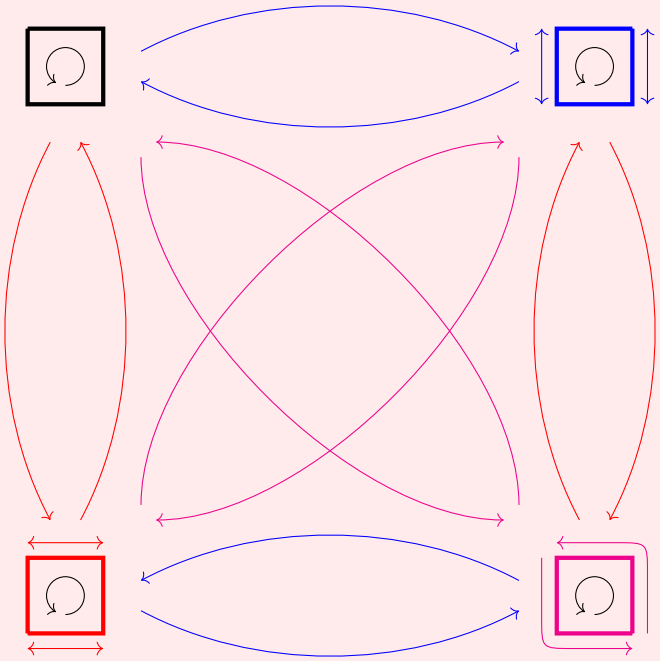
Remark 1.10

$g(s) = gs, g(s) = sg^{-1}, sg = sg, sg = g^{-1}s$ does not preserve group operation of S.

We let G act on $S(= G)$ by $g(s) = gs$. This means G into subset of all permutations of $S(= G)$. Now we want to add extra "structure" to S so G is exactly symmetries of S with this structure.
Extra structure is **right** action of G on S. We now have 3 copies of G

1. Set $S(= G)$.
2. G acting on **right** on $S \leftarrow$ part of structure
3. G acting on **left** on $S \leftarrow$ symmetry group

Example 1.11 (Cayley Graph of 4 elements)



We get colored (directed) graph arrow gives **right** action of G, which is not the same as the **left** action.

Remark 1.12

Goals of group theory

1. Classify all groups
2. Given a group G, find all ways G acts on something.

Example 1.13

Linear representation = actions of G over vector space.
Permutation = actions of G over on a set.

Definition 1.14

A homomorphism $f : G \to H$ map preserving group structure. i.e. $f(gh) = f(g)f(h)$.
A isomorphism is a homomorphism that is a bijection.
The kernel of f is the set of elements such that it maps to the trivial element of H

Example 1.15

Consider the function

$$\exp : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^*, \cdot \rangle$$

exp is a isomorphism from $\mathbb{R}$ to $R_{>0}$

Example 1.16

Consider the function

$$\exp : \langle \mathbb{C}, + \rangle \to \langle \mathbb{C}^*, \cdot \rangle$$

kernel = elements $2\pi in, n \in \mathbb{Z}$.

Example 1.17 (Number Theory)

Consider $\mathbb{Z}/4\mathbb{Z}$ integers mod 4. and $(\mathbb{Z}/5\mathbb{Z})^*$ nonzero integers mod 5 under multiplication.

Example 1.18

Consider the function :

$$\det : GL_n(\mathbb{R}) = \mathbb{R}^*$$

is a homomorphism.
kernel = $SL_n(\mathbb{R})$ = special linear group.

Theorem 1.19 (Lagrange's Theorem)

If H is a subgroup of G, order of H divides order of G. (G is finite)

Lemma 1.20

2 cosets either are the same or disjoint.

Proof. If $aH \cap bH = \varnothing$, then the proof is done.
Now we suppose $aH \cap bH \neq \varnothing$, then we know that $ah_1 = bh_2$ for some element in aH and bH. We compute $ah_1 = bh_2 \implies h_1 = a^{-1}bh_2 \implies a^{-1}b = h_1h_2^{-1} \implies a^{-1}b \in H$. Then we know that $aH = bH$.
We can use a similar argument to show that this works for the right cosets as well. This is left as an exercises to the reader. ■

Lemma 1.21

Any cosets have the same size.

Proof. We can simply prove that $\phi : h \mapsto bh$ is bijective, therefore $|H| = |bH|$.
This proof is trivial and is left as an exercise to the reader. (Hint: prove that ϕ is injective and say it's surjective by construction) ■

Proof. Suppose G acts on S. Pick $s \in S$, put H =set of elements fixing s such that $hs = s$, then H is a subgroup of G.
Given a subgroup H of G, we can find set S acted on by G, $s \in S$. H = things fixed in S.
Given $g, h(H \subseteq G)$. S = left cosets of H.
we get action of G on set of cosets by putting $g(aH) = (ga)H$. (well-defined left as an exercise)
Therefore $|G| = |H| \times$ number of cosets. Therefore the order of H divides the order of H. ■

Theorem 1.22

If $g \in G$, then the order of g divides divides order of G.

Corollary 1.23

If G is prime order, it is cyclic

Proof. Pick any element $g \neq 1$. Order divided p, so p is primes. so G = powers of g ■

Example 1.24

List of all groups

1. Order 1 : Trivial group
2. Order 2 : 1 group $\mathbb{Z}/2\mathbb{Z}$, $0, 1$.
3. Order prime p : Integer $\mod p$.
4. Order 4 : Cyclic group $\mathbb{Z}/4\mathbb{Z}$ and symmetry of a rectangle. These are not isomorphic as the symmetry group of rectangle does not have a element of order 4.
5. Classify all groups with $g^2 = 1$ for all g. We want to show that group is abelian, or $gh = hg$ for all $g, h \in G$. This follows because $ghgh = (gh)^2 = 1 = h^2g^2 = hhgg \implies hg = gh$. Since G is abelian, we can write group operation as $+$. Notice that G is a vector space over field of order 2, namely $\mathbb{Z}/2\mathbb{Z}$. so h has a basis, and is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$($n$-dimensional vector space) to some n. So there is only 1 other group of order 4.

Definition 1.25

Suppose G, H are groups, then the product(sum) of the group is defined as follows

$$G \times H = \text{set of pairs}(g, h)$$

and the operation is defined as

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$$

Example 1.26

symmetry of rectangle is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 1.27

$\mathbb{C}^* = S \times \mathbb{R}_{>0}$, where S is the circle group. Notice that this is the polar decomposition of complex numbers.

Definition 1.28

The product(sum) of groups are elements $(g_1, g_2, \ldots)$ such that all but finite number of g_i are trivial.

Example 1.29

$\mathbb{Q}^* =$ infinite sum of groups $\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/3\mathbb{Z} + \mathbb{Z}/5\mathbb{Z} + \dots$. This follows by fundamental theorem of arithmetic.

Exercise 1.30

Find graph whose symmetry group is $\mathbb{Z}/5\mathbb{Z}$.

Example 1.31

groups of order 6: the symmetries of triangles and the cyclic group $\mathbb{Z}/6\mathbb{Z}$ and the product of the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. But there is a direct isomorphism between $\mathbb{Z}_6$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\mathbb{Z}_3$, namely

$$\phi : 1 \mapsto (1, 1)$$

Remark 1.32

Similarly, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$, where m, n are coprime. This is also the Chinese remainder theorem.

Definition 1.33

S_n is the symmetry group, the set of all permutations of $\{1, 2 \dots, n\}$.

Example 1.34

Symmetries of a triangle is isomorphic to S_3.

Proposition 1.35

S_3 is non-abelian.

Proof. Note that $(12)(23) = (123)$ and $(23)(12) = (132)$. ■

Question 1.36

Suppose H is a subgroup of G. Let G/H be the left cosets aH of H for $a \in G$. Is G/H a group?

Answer 1.37. Define $(aH)(bH) := abH$ and $ah_1bh_2 \equiv ab \pmod{H}$.

Problem 1.38

This need not be well-defined, and the groups needs to be abelian.

Answer 1.39. We want to know if $aHbH = abH$. This holds true if $Hb = bH$, or the left and right cosets are equal. Equivalently, we can see that $bHb^{-1} = H$. Therefore G/H is a group if the left cosets are right cosets.

Definition 1.40

H is a **normal** subgroup of G if $gHg^{-1} = H$ for all $g \in G$.

Example 1.41

Consider S_3 and the subgroup $H := \{\mathbb{I}, (12)\}$. The left cosets are

$$H, (23)H, (132)H$$

the right cosets are

$$H, H(23), H(132)$$

we will run into trouble if we try to make a group from G/H

Remark 1.42

There is a clever bijection from left cosets to right cosets, namely

$$\phi : aH \to Ha^{-1}$$

Therefore the number of right cosets is equal to the right cosets.

Definition 1.43

The index of H in G, denoted as $|G : H|$, is the number of left/right cosets of H in G.

Remark 1.44

Do not define $|G : H|$ as $\frac{|G|}{|H|}$ as $|H|$ might be ∞. For example $|2\mathbb{Z}| = \infty$.

Theorem 1.45 (Cayley's Theorem)

Suppose d divides $|G|$, then G has a element of order d if d is prime.

Proof. First we consider the abelian case. Pick an element $g \in G$ of prime order q. If $q = p$, then we are done. if $q \neq p$. Look at $G/\langle g \rangle$ of order $|G|/q$, which is divisible by p. So $G/ < g >$ has element a of order p by induction. put b to be the element of G whose image is a.
Second we consider nonabelian case. Look at the **adjoint action** of G on **itself**,

$$g(h) = ghg^{-1} \qquad \text{conjugate at } h \text{ by } g$$

Split up G into orbits h_1, h_2 in some orbit if $g(h_1) = h_2$ for some g. Then

$$\text{the number of orbits of } h = \frac{\text{order of } h}{\text{subgroup fixing } h}$$

If the denominator is less than G, then we can assume that this is not divisible by p, otherwise it has element of order p by induction.
We can assume each conjugacy class is either of size divisible by p or contains just one element in the center of the group, which commutes with every elements in the group.
Then the number of elements on center is equal to the order of G therefore it has elements of order p by the abelian case.

■

Definition 1.46
Orbit

Example 1.47
Let $G := S_3$. The orbit of G are

$$\{\mathbb{I}\}, \{(12), (23), (31)\}, \{(123), (132)\}$$

Example 1.48
Take $H_1 = \{\mathbb{I}, (123), (132)\}, H_2 = \{I, (12)\} \subseteq S_3$. Let $S_3 = H_1H_2$ but $S_3 \neq H_1 \times H_2$ since H_1, H_2 does not commute. H_1 is normal as it's index 2, therefore we only have two cosets H_1, aH_1 where $a \notin H_1$. We then get the action of H_2 on H_1 by

$$g(h) = ghg^{-1} \qquad h \in H_1, g \in H_2$$

Question 1.49
Suppose given any groups A, B, actions of B on A. Can we form a group containing A, B so this action is given by conjugation?

Answer 1.50. Yes. Consider the set $A \times B$

$$(a_1, b_1) \times (a_2, b_2) = (a_1\, b_1(a_2), b_1b_2)$$

This is the **semi-direct product of** A, B, denoted as

$$A \rtimes B.$$

Now we can classify group of order 6. By cayley, we now have elements g of order 3 and h of order 2. Let $A = \langle g \rangle, B = \langle h \rangle$. Notice that A is normal in G since it has index 2. so B acts on A by conjugation. as we get two actions

$$ghg^{-1} = h, ghg^{-1} = h^{-1}$$

Therefore there is only two groups of order 6, the abelian one and the nonabelian one.

Remark 1.51

This applies to groups of order $2p$, where p is a prime.

Now consider groups of order 8:
Case 1: all elements has order 2, then the group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$
Case 2: Some element g has order 4. Then take $A = \langle g \rangle$. G/A has order 2, so A is normal so it's ismorphic to $\mathbb{Z}/2\mathbb{Z}$. We obtain

$$1 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Problem 1.52

Given A, B and action of B on A, what is G.

Answer 1.53. We can have $A \times B, A \rtimes B$ or something else.

$$1 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

$$1 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

If G is a product of the group then it's called a split exact sequence, otherwise it's called a non-split exact sequence.

Take

$$1 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

One possible g is $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ Suppose a is a generator of $\mathbb{Z}/4\mathbb{Z}$. Pick $b \in G$ so image of b is nontrivial in $\mathbb{Z}/2\mathbb{Z}$. We know $b^2 \in \mathbb{Z}/4\mathbb{Z}$. If $b^2 = 1, a, a^2, a^3$. We also know bab^{-1} is a generator of $\mathbb{Z}/4\mathbb{Z}$ so $bab^{-1} = a$ or a^3. Then we have the following table

$b^2 =$	$bab^{-1} = a$	$bab^{-1} = a^3$
Splits	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = D_4$
a	$\mathbb{Z}/8\mathbb{Z}$	group collapses
a^2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$	Q_8
a^3 changes to a^{-1}	D_4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Remark 1.54
$\mathbb{R}^* \supseteq S^0, \mathbb{C}^* \supseteq S^1, \mathbb{H}^* \supseteq S^3$, where S^n are n-dimensional spheres.

Remark 1.55 (Digression on video games)
Let S^3 acts on $\mathbb{R}^3$ by conjugation

$$g(v) = gvg^{-1}$$

which gives gives a rotation of $\mathbb{R}^3$. And we obtain the homomorphism

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow S^3 \longrightarrow GL_3(\mathbb{R}) \longrightarrow 1$$

And quaternion and significantly faster than 3×3 matrices.

Remark 1.56
There is only five groups of order 8, namely $D_8, Q_8, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\mathbb{Z}/2\mathbb{Z}$.

Problem 1.57
How many ways to arrange 8 rook on chessboard so no rooks attack each other?

Answer 1.58. Notice that the first row has 8 choices, second row has 7 choices, etc, etc – a totalof 8! ways.

Problem 1.59
How many ways up to symmetry?

Answer 1.60. Clearly the symmetry of the chessboard is isomorphic to D_8. First guess is

$$\frac{8!}{8}$$

But this is not right! There is some arrangement that have less than 8 symmetries.

Theorem 1.61 (Burnside's Theorem)
Suppose group G acts on set S, then # orbit is equal to the number of fixed points, namely

$$\frac{1}{|G|} \sum_{a \in G} |S^g|$$

where S^g is the point fixed by g.

Remark 1.62

For this problem, $G = D_8, S =$ all ways to arrange 8 rooks.

Proof. Cont the set of pairs (g, s) with $g(s) = s$.
Method 1: For each g there are $|S^g|$ possible value of S. so we get a total of

$$\sum_{g \in G} |S^g|$$

Method 2: Look at each orbit of G on S. Pick some s in orbit, # of possible element of G = # of elements of G fixing S, which forms a subgroup H of G.
So the total number of pairs = # elements of orbit $\times$ size of subgroup fixing one element. so altogether we get # orbit$\times|G| = \sum_{g \in G} |S^g|$. ■

Remark 1.63

G might have might have many elements. Instead of summing every elements. We can just sum over the conjugacy classes.

Definition 1.64 (Informal Definition)

two elements of G is called **conjugate** if they sort of look the same.

Example 1.65

Let G be the rotation of the cube. We then can classify them

1. Trivial rotation
2. Spin around 2 opposite corners. spin by 1/3 rotation. (8)
3. Spin by 1/2 revolution fixing 2 opposite edges. (6)
4. Rotate by 1/4 by the center of face. (4)
5. Rotate by axis for 1/2 revolution. (3)

Definition 1.66

a, b are called **conjugate** if $a = gbg^{-1}$ for some $g \in G$.This equivalence relation forms equivalence classes called **conjugacy classes**.

Proposition 1.67

If $a, b \in G$ are conjugate, then a, b have the same number of fixed points.

Proof. If $gag^{-1} = b$. Then g takes fixed points of a to fixed points of b. We have

$$as = s \implies (gag^{-1})gs = gs$$

so b fixes (gs). ■

Let c_n denote the number of ways to arrange n rooks on $n \times n$ board symmetric under reflection of diagonal corners. We have the recurrence relationship

$$C_n = C_{n-1} + (n-1)C_{n-2}$$

For $n = 8$ this gives us $C_n = 764$.
We now go back to find the conjugacy classes of D_8

1. Trivial $(8! = 40320)$
2. Reflection by diagonal corners. (764)
3. Rotation by $90°$. (6×2)
4. Flip by axis. (0)
5. Rotation by $180°$. $(8 \times 6 \times 4 \times 2)$

Adding them all of gives us 5282 ways.

Remark 1.68
For large number of groups, having conjugacy classes reduce significant amount of time.

Remark 1.69
To count number of orbits we can cheat : weight each element s in S by $\frac{1}{|H|}$, where H is the group elements fixing s. weighted number of orbits is $\frac{|S|}{|G|}$.

Let consider groups of order 9. Which is kind of boring. Then let's classify order p^2.

Definition 1.70
The **center** of G is

$$Z(G) = \{z \in G : zg = gz \quad \forall g \in G\}$$

Theorem 1.71
If G has prime power order, $p^n > 1$, then the center of G is nontrivial.

Example 1.72

S_3 has trivial center.

Proof. Look at adjoint action of G on G, where $g(s) = gsg^{-1}$. Then the orbits is equal to conjugacy classes. Suppose $s \in G$. We have two cases

1. orbit of s has size 1. Then clearly $s \in Z(G)$.
2. Orbit has size 1, then size must be p^k for some $k \geq 1$.

Therefore we have

$$|\text{center}| = |G| - \sum |\text{orbits of size} > 1|$$

Since the right hand side is divisible by p, the left hand side must also be divisible p, since $|\text{center}| \geq 1$, it must be nontrivial. ■

Lemma 1.73

Suppose G is group, let Z be the center of G. If G/Z is cyclic then $G = Z$ so G is abelian.

Proof. Suppose g is element of G whose image generates G/Z. Any two elements of the form $z_1 g^{n_1}, z_2 g^{n_2}$ commutes. ■

Therefore any group of order p^2 has center of order p or p^2. Suppose G has order p^2. If center Z has order p, then $|G/Z| = p$, and must be cyclic by previous works. Therefore any group of order p^2 is abelian. We have two cases now

1. G has element of order p^2.
2. All elements satisfy $g^p = 1$. Then G (additively forms a vector space over of $\mathbb{F}$), therefore $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Example 1.74

Groups of order 10, by previous class notice that it's of the form $2p$. Therefore the only possibilities are $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $D_{10} = (\mathbb{Z}/5\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$.

Recalled tat D_{2n} is the symmetries of n-gon. Notice that D_{2n} is generated by a, b of order2. If a group is generated by a, b with $a^2 = 1, b^2 = 1, (ab)^n = 1$. Then G is a quotient of dihedral of D_{2n}. all elements of g forms a finite sequence of a, b :

$$g = ababbaabbababa$$

Proposition 1.75

Any element (a, b) with $a^2 = b^2 = 1$ is a dihedral group.

Corollary 1.76

Suppose $a, b \in G$ for a finite group G, $a^2 = b^2 = 1$. Then either a is conjugated to b or there is some $c \neq 1, ca = ac, cb = bc$. Look at H generated by a, b, which is dihedral, so D_{4n} or D_{4n+2}.

Theorem 1.77

There is five different groups of order 5 up to isomorphism: $\mathbb{Z}/12\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}, D_{12}, A_4, \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$