Groups

Groups and subgroups

Definitions

A *group* G is a set equipped with an associative binary operation, an identity element for this operation, and which has inverses. A *subgroup* $H \leq G$ is a subset closed under the group operations. It is sufficient that H be non-empty and closed under $(x, y) \mapsto xy^{-1}$.

If $H \leq G$ then $G/H = \{gH \mid g \in G\}$ is the set of left-cosets of H. The left-cosets partition G into subsets of equal size.

Lagrange's Theorem

If H is a subgroup of the finite group G then the order of H divides the order of G, i.e.

$$|G| = |H| \cdot |G/H|.$$

Note that while the condition $a \mid |G|$ is necessary for the existence of a subgroup of order a, it is not sufficient.

Group homomorphisms

A group homomorphism $\theta : G \to H$ is a map preserving the group structure, i.e.

$$\begin{aligned} \theta(1) &= 1 \\ \theta(xy) &= \theta(x)\theta(y) \\ \theta(x^{-1}) &= \theta(x)^{-1} \end{aligned}$$

for every $x, y \in G$. It is sufficient to check that $\theta(xy^{-1}) = \theta(x)\theta(y)^{-1}$.

Normal subgroups

A subgroup H of a group G is *normal* if $gHg^{-1} = H$ for all $g \in G$. We write $H \lhd G$ to mean H is a normal subgroup of G. A group G is *simple* if it has no non-trivial subgroups (i.e. other that $1 \lhd G$ and $G \lhd G$).

For example, any subgroup of index 2 is normal. In particular, $A_n \lhd S_n$. A_n is simple for all $n \geq 5$ — we shall prove this later for the case $n = 5$.

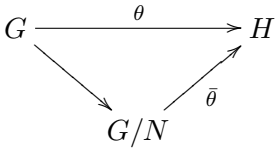
A subgroup $H \leq G$ is normal iff the map $(aH, bH) \mapsto abH$ is well-defined. Then G/H is a group with this operation and the quotient map $G \to G/H$ is a group homomorphism.

Kernels

If $\theta : G \to H$ is a homomorphism, then $\ker(\theta) = \{a \in G \mid \theta(a) = e\} \lhd G$. Also, if $H \lhd G$ then H is the kernel of the quotient homomorphism $G \to G/H$, so a subgroup $H \leq G$ is normal iff it is the kernel of some homomorphism $G \to K$ for some group K.

Universal property

Suppose $N \lhd G$ and $\theta : G \to H$ is such that $N \leq \ker(\theta)$. Then there is a unique map $\bar{\theta} : G/N \to H$ such that the diagram

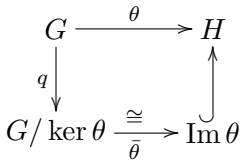


commutes.

The isomorphism theorems

1st Isomorphism Theorem

Let $\theta : G \to H$ be a group homomorphism. Then $\ker\theta \lhd G$ and $\operatorname{Im}\theta \leq H$, and there is an isomorphism $\bar{\theta} : G/\ker\theta \to \operatorname{Im}\theta$, so that θ factors as



2nd Isomorphism Theorem

If $H \leq G$ and $K \lhd G$ then

- $HK \leq G$
- $K \lhd HK$ and $H \cap K \lhd H$
- $HK/K \cong H/H \cap K$.

Proof

Consider the surjective homomorphism $\theta : H \to HK/K$ defined by $\theta(h) = hK$, with kernel $H \cap K$, and apply the 1st Isomorphism Theorem.

3rd Isomorphism Theorem

If $N \lhd G$ then $H \mapsto H/N$ is a bijection between

- the intermediate subgroups H with $N \leq H \leq G$
- the subgroups of G/N.

Under this bijection a normal subgroup $K \lhd G$ with $N \leq K \leq G$ corresponds exactly to $K/N \lhd G/N$ and

$$(G/N)/(K/N) \cong G/K.$$

Group actions

Definitions

A *(left) action* of a group G on a set X is a map $G \times X \to X$, $(g, x) \mapsto g \cdot x$, such that

$$e \cdot x = x$$
$$g \cdot (h \cdot x) = (gh) \cdot x$$

for all $g, h \in G$ and all $x \in X$. A group action induces a homomophism $\phi : G \to S_X$ given by

$$\phi(g)(x) \mapsto g \cdot x.$$

The action is called *faithful* if $\ker \phi = \{1\}$.

Orbits

Let G be a group acting on a set X and let $x \in X$. Then the *orbit* of x under the action is

$$\mathrm{Orb}_G(x) = O(x) = \{g \cdot x \mid g \in G\} = Gx.$$

The orbits of the elements of X are equivalence classes under the equivalence relation $x \sim y$ iff $g \cdot x = y$ for some $g \in G$. The group action is said to be *transitive* if there is only one orbit.

Stabilizers

If G acts on a set X and $x \in X$ then the *stabilizer* of x under G is

$$\mathrm{Stab}_G(x) = G_x = \{g \in G \mid g \cdot x = x\}.$$

This is a subgroup of G. The stabilizers of elements in the same orbit are conjugate to one another. In fact

$$\mathrm{Stab}_G(g \cdot x) = g \,\mathrm{Stab}_G(x) g^{-1}.$$

Orbit–Stabilizer Theorem

Suppose G acts on X and $x \in X$. Then there is a bijection $O(x) \to G/G_x$ and hence

$$|G| = |G_x| \cdot |O(x)|.$$

Proof

Consider the map $O(x) \to G/G_x$ defined by

$$g \cdot x \;\longmapsto\; gG_x.$$

Then

$$g \cdot x = h \cdot x \quad \Longleftrightarrow \quad (h^{-1}g) \cdot x = x \quad \Longleftrightarrow \quad h^{-1}g \in G_x \quad \Longleftrightarrow \quad gG_x = hG_x,$$

and so this map is well-defined and injective. But it is clearly surjective and so it is a bijection, as required.

Conjugacy actions

Definition

The *conjugacy action* of a group G on itself is given by

$$(g, h) \longmapsto ghg^{-1}.$$

Conjugacy classes

The *conjugacy class* of $h \in G$ is the orbit of g under the conjugacy action, i.e.

$$\mathrm{ccl}(h) = \{ghg^{-1} \mid g \in G\}.$$

This is $\{h\}$ iff $h \in Z(G)$.

The *conjugacy class* of $H \leq G$ is the orbit of H under the conjugacy action on subgroups, i.e.

$$\mathrm{ccl}(H) = \{gHg^{-1} \mid g \in G\}.$$

This is $\{H\}$ iff $H \lhd G$.

A subgroup is normal iff it is the union of conjugacy classes of its elements, since a subgroup is normal iff it is 'closed under conjugation from outside'.

Centralizers and normalizers

The *centralizer* of $h \in G$ is the stabilizer of h under the conjugacy action, i.e.

$$C_G(h) = \{g \in G \mid ghg^{-1} = h\}.$$

The *normalizer* of $H \leq G$ is the stabilizer of H under the conjugacy action on subgroups, i.e.

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

The normalizer of H is the largest subgroup containing H in which H is normal, $H \lhd N_G(H)$.

The centre

The *centre* of G, written $Z(G)$, is the kernel of the conjugacy action, i.e.

$$\begin{aligned} Z(G) &= \{g \in G \mid ghg^{-1} = h \text{ for all } h \in G\} \\ &= \{g \in G \mid gh = hg \text{ for all } h \in G\} \\ &= \bigcap_{g \in G} C_G(g). \end{aligned}$$

The centre of G is normal in G. The conjugacy action is faithful iff $Z(G) = \{1\}$.

Permutation groups

Recall

There is a homomorphism $\epsilon : S_n \to \{\pm 1\}$ with $\ker \epsilon = A_n$, the set of even permutations.

The conjugacy classes of elements in S_n correspond to the cycle types of elements in S_n, i.e. the conjugacy class of $x \in S_n$ is precisely the set of element of S_n with the same cycle type as x.

Theorem

A_5 is simple.

Proof

Observe the following:

1. Suppose that $H \leq S_n$. Then either
   (a) $H \leq A_n$, or
   (b) $H \not\leq A_n$, in which case let $\tau \in H \setminus A_n$. Then τ is odd and so for any $\sigma \in H$, we either have $\sigma \in H \cap A_n$ or $\tau^{-1}\sigma \in H \cap A_n$. Hence σ is in one of the cosets $H \cap A_n$ or $\tau(H \cap A_n)$, and so $H \cap A_n$ is a subgroup of H of index 2.
2. Suppose S_n acts on a set X. Let $x \in X$ and let $H = \mathrm{Stab}_{S_n}(x)$. Then $H \cap A_n = \mathrm{Stab}_{A_n}(x)$. Now by the Orbit–Stabilizer Theorem we have
$$|\operatorname{Orb}_{S_n}(x)| = |S_n|/|H|$$
$$|\operatorname{Orb}_{A_n}(x)| = |A_n|/|H \cap A_n|.$$
   By by the above point, either $H \leq A_n$, in which case we have $|\operatorname{Orb}_{A_n}(x)| = \frac{1}{2}|\operatorname{Orb}_{S_n}(x)|$, or $H \not\leq A_n$, in which case $|\operatorname{Orb}_{A_n}(x)| = |\operatorname{Orb}_{S_n}(x)|$.

We now consider the sizes of the conjugacy classes of elements of A_5 in S_5 and then in A_5.

Cycle type	Size in S_5	Size in A_5
e	1	1
(1 2 3)	20	20
(1 2)(3 4)	15	15
(1 2 3 4 5)	24	12, 12

1. $|C_{S_5}((1\ 2\ 3))| = 120/20 = 6$, so $C_{S_5}((1\ 2\ 3)) = \langle (1\ 2\ 3), (4\ 5)\rangle \not\leq A_5$ and the orbit does not split.
2. Since 15 is odd, the orbit of (12)(34) cannot split.
3. $|C_{S_5}((1\ 2\ 3\ 4\ 5))| = 120/24 = 5$, so $C_{S_5}((1\ 2\ 3\ 4\ 5)) = \langle (1\ 2\ 3\ 4\ 5)\rangle \leq A_5$ and the orbit splits in A_5.

Now consider that a normal subgroup contains e and is a union of conjugacy classes. But, by inpection, no sum of 1 and any subset of 20, 15, 12 and 12 divides 60, so A_5 has no normal subgroups and hence is simple.

Remark

The icosahedral group R — the group of symmetries of the icosahedron — is isomorphic to A_5.

For we can show that $|R| = 60$ and R acts faithfully on the 5 "co-ordinate axes", giving an injective homomorphism $R \hookrightarrow S_5$. But then if R were not equal to A_5 we would have $R \cap A_5$ an index 2 subgroup of A_5, contradicting the simplicity of A_5. So $R \cong A_5$, as claimed.

Classical groups

For any field $\mathbb{F}$ we have the following groups:

- $\mathrm{GL}_n(\mathbb{F}) = \{$ invertible $n \times n$ matrices over $\mathbb{F}$ $\}$
- $\mathrm{SL}_n(\mathbb{F}) = \{$ $n \times n$ matrices over $\mathbb{F}$ with determinant 1 $\}$
- $\mathrm{PGL}_n(\mathbb{F}) = \mathrm{GL}_n(\mathbb{F})/Z$, where $Z = Z(\mathrm{GL}_n(\mathbb{F})) = \{\lambda I \mid \lambda \in \mathbb{F}^*\}$
- $\mathrm{PSL}_n(\mathbb{F}) = \mathrm{SL}_n(\mathbb{F})/Z$, where $Z = Z(\mathrm{SL}_n(\mathbb{F})) = \{\lambda I \mid \lambda^n = 1\}$

These are called the (*projective*) *general* and *special linear groups*.

If $\mathbb{F} = \mathbb{F}_q$ is a finite field, then these four groups are finite, and we may easily calculate their orders. In general, $\mathrm{PSL}_n(\mathbb{F})$ is simple and non-abelian. The exceptions are when $n = 2$ and $\mathbb{F} = \mathbb{F}_2$ or $\mathbb{F}_3$.

Abelian groups

By convention we use additive notation when dealing with abelian groups. In fact, an additive abelian group is precisely a $\mathbb{Z}$-module.

Definition

An abelian group A is *finitely generated* if there is a finite set of elements $a_1, \ldots, a_n$ in A such that any $a \in A$ may be written as a finite sum $a = \sum \lambda_i a_i$ of the a_i.

Note that $\mathbb{Q}$ is not finitely generated as an additive abelian group.

Structure theorem

Any finitely generated abelian group A can be written

$$A \cong \mathbb{Z}^k \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

with $d_1 \mid d_2 \mid \cdots \mid d_m$. If A is finite, then it may be written as

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

or alternatively, by the Chinese Remainder Theorem, it may be written as a product of cyclic groups $\mathbb{Z}/p^m\mathbb{Z}$ of prime power order.

p-groups and the class equation

The class equation

Consider the conjugacy action of G on G. The orbits under this action are the conjugacy classes. Suppose the distinct conjugacy classes are $G_1, \ldots, G_h$. Then h is called the class number and if we let

$$n_i = |G_i| = |G : C_G(x_i)|$$

where $x_i \in G_i$, then we have the *class equation*

$$|G| = n_1 + \cdots + n_h.$$

By convention, $G_1 = \{e\}$ and so we have

$$|G| = 1 + n_2 + \cdots + n_h.$$

Theorem

If $|G| = p^n$ then $|Z(G)| > 1$.

Proof

Otherwise the class equation is

$$p^n = 1 + n_2 + \cdots + n_h$$

where, by the Orbit–Stabilizer Theorem, $p \mid n_i$ for each $i \geq 2$.

Corollary

Any group of order p^2 is abelian.

Proof

If $|G| = p^2$ then by the theorem above $|Z| = p$ or p^2. If $G = Z$ then G is abelian, so assume that $|Z| = p$. Then G/Z is cyclic, with generator xZ, say. But then $G = \langle x, Z \rangle$, and so G is abelian since x commutes with every element of Z.

Corollary

If $|G| = p^n$ then there is a sequence

$$1 = Z_0 \leq Z_1 \leq Z_2 \leq \cdots \leq Z_k = G$$

with each $Z_i \lhd G$ and with

$$Z_{i+1}/Z_i = Z(G/Z_i).$$

Proof

Set $Z_0 = 1$ and $Z_1 = Z(G)$ and then inductively choose Z_{i+1} such that $Z_{i+1}/Z_i = Z(G/Z_i)$. By the theorem above this series is strictly increasing and so terminates.

Theorem (Cauchy)

Suppose a prime p divides the order of a finite group G. Then G contains an element of order p.

Proof

We proceed by induction on $|G|$. The base case is $|G| = p$, in which case $G \cong C_p$ and we're done. Now for the inductive step. One of the following possibilities occurs:

- $Z(G) \neq 1$. Then Z contains an element z, say, of prime order q. If $q = p$, we're done. Otherwise $|G/\langle q \rangle| = |G|/q$, so $p \mid |G/\langle z \rangle|$ and so by the induction hypothesis there is an element $b\langle z \rangle \in G/\langle z \rangle$ of order p. Then $b^p \in \langle z \rangle$ and so b has order p or order pq, whence b^q has order p and we are done.
- $Z(G) = 1$. Let $C_2, \ldots, C_h$ be the non-$\{e\}$ conjugacy classes. Consider the centralizers $C(x_2), \ldots, C(x_h) \leq G$. Then we claim that p divides some $|C(x_k)|$, and so we're done by the induction hypothesis. For suppose not. Then p divides each $n_2, \ldots, n_h$ and we have $p \mid |G| = 1 + n_2 + \cdots + n_h$ — a contradiction.

Definition

A p-group is a group all of whose elements have order p^k for some k.

Corollary

A finite group is a p-group if and only if it has order p^n for some n.

Sylow's theorems

Sylow p-subgroups

Suppose that $|G| = p^m s$ with $p \nmid s$. Then a subgroup H of G is a *Sylow p-subgroup* if $|H| = p^m$.

Sylow's Theorems

Let G be a finite group, with $|G| = p^n s$ where $p \nmid s$. Then

1. Sylow p-subgroups of G exist.
2. Any two Sylow p-subgroups of G are conjugate.
3. If there are n_p Sylow p-subgroups of G, then $n_p \equiv 1 \pmod{p}$.

Remarks

It follows that n_p is the index in G of $N_G(P)$, for some Sylow p-subgroup P of G. But then since $P \leq N_G(P)$ we see that $p^n \mid N_G(P)$ and so $n_p \mid s$.

Moreover, if $n_p = 1$ then the unique Sylow p-subgroup is normal in G, and hence G is not simple.

Proof

1 & 3. Let $\mathcal{X} = \{X \subseteq G \mid |X| = p^m\}$ and let G act on $\mathcal{X}$ by left multiplication.

Pick $X \in \mathcal{X}$ and let $H = \mathrm{Stab}_G(X)$. Then $HX = X$, so X is a union of right cosets of H and hence H has order p^k for some k. So either $p \mid |\operatorname{Orb}(X)|$ or else $|H| = p^m$ and $|\operatorname{Orb}(X)| = s$. Hence if n_p is the number of Sylow p-subgroups, we have

$$|\mathcal{X}| = \sum |\mathcal{O}_i| + n_p s,$$

where $p \mid |\mathcal{O}_i|$ for each i. Thus $|\mathcal{X}| \equiv n_p s \pmod{p}$. But considered modulo p

$$\begin{aligned} & (x+y)^p = x^p + y^p \\ \Rightarrow \quad & (x+y)^{p^m} = x^{p^m} + y^{p^m} \\ \Rightarrow \quad & (x+y)^{p^m s} = \left(x^{p^m} + y^{p^m}\right)^s = x^{p^m s} + s x^{p^m(s-1)} y^{p^m} + \cdots \end{aligned}$$

and so $|\mathcal{X}| = \binom{p^m s}{p^m} \equiv s \pmod{p}$. Therefore $n_p s \equiv s \pmod{p}$ and so $n_p \equiv 1 \pmod{p}$.

2. Let P and Q be Sylow p-subgroups of G, and let $\mathcal{P}$ be the conjugacy class of P in G. Then

$$|\mathcal{P}| = \frac{|G|}{|N_G(P)|},$$

and since $P \leq N_G(P)$ we have that $p^m \mid |N_G(P)|$ and so $|\mathcal{P}| \mid s$.

Consider the conjugacy action of Q on $\mathcal{P}$. The order of a Q-orbit divides $|Q| = p^m$ and so p divides the order of all Q-orbits except those of order 1. But

$$\sum |\mathcal{O}_i| = |\mathcal{P}|$$

and so since $p \nmid s$ there must exist a Q-orbit $\{P'\}$ of order 1.

Now $P' \lhd N_G(P')$ and $Q \leq N_G(P')$. It follows by the 2nd Isomormorphism Theorem that

$$P'Q \leq N_G(P') \leq G$$

and

$$\frac{|P'Q|}{|P'|} = \frac{|Q|}{|P' \cap Q|}.$$

Now the left-hand side is not divisible by p and so neither is the right-hand side. Hence the right-hand side is equal to 1, so $P' \cap Q = Q$ and so $Q \leq P'$. But then $Q = P'$ since both are of order of p^m, and so $Q \in \mathcal{P}$, as required.

Corollary to the proof

Any p-subgroup of G is contained in some Sylow p-subgroup.

Proof

As above, taking P a Sylow p-subgroup and Q an arbitrary p-subgroup.

Rings and Invariant Theory

Rings

A *ring*[1] R is a set equipped with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ such that R is an abelian group under $+$ and $\times$ is associative, commutative and has an identity element, and such that the distributivity laws

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

hold for all elements $a, b, c \in R$.

If R is a ring, $x \in R$ is a *unit* if it has a multiplicative inverse, i.e. if there exists $\bar{x} \in R$ such that $x\bar{x} = \bar{x}x = 1$. The collection of units in R form a multiplicative group, denoted R^*.

A ring R is a *field* if $R^* = R \setminus \{0\}$.

Remark

If R is a ring with $1 = 0$, then $R = \{0\}$, the zero ring. Note that $\{0\}$ is not a field.

Ring homomorphisms

A *ring homomorphism* $\theta : R \to S$ is a map preserving the ring structure, i.e. such that

$$\begin{aligned} \theta(0) &= 0 \\ \theta(1) &= 1 \\ \theta(a + b) &= \theta(a) + \theta(b) \\ \theta(-a) &= -\theta(a) \\ \theta(ab) &= \theta(a)\theta(b). \end{aligned}$$

For any ring R, there is a unique homomorphism $\phi : \mathbb{Z} \to R$.

For any ring R, there is a unique homomorphism $\theta : R[X] \to R$ such that θ maps R to R and X to a. θ is the evaluation of the polynomial at a.

Subrings

A *subring* S of a ring R is a subset which contains 0 and 1 and is closed under the ring operations.

If S is a subring of R then the inclusion $S \hookrightarrow R$ is a ring homomorphism. Further, if $\theta : R \to S$ is a ring homomorphism then $\operatorname{Im}\theta$ is a subring of S.

Ideals

An *ideal* $I \lhd R$ in a ring R is a subset which contains 0 and is closed under addition and multiplication from outside. An ideal $I \lhd R$ is *proper* if $I \neq R$.

[1] Actually, this is a *commutative ring* — all the rings we will deal with are commutative.

Note that for any ring R, $R \lhd R$ and $\{0\} \lhd R$. Also note that if an ideal $I \lhd R$ is also a subring of R, then $1 \in I$ and so $I = R$.

If $a \in R$ then $(a) = \langle a \rangle = \{ra \mid r \in R\} \lhd R$ is the *principal ideal* generated by a.

If $a_1, \ldots, a_n \in R$ then $(a_1, \ldots, a_n) = \{\sum r_i a_i \mid r_i \in R\} \lhd R$ is a *finitely generated* ideal in R.

If $I, J \lhd R$ then $I \cap J$, $I + J = \{a + b \mid a \in I, b \in J\}$ and $IJ = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_j \in J\}$ are all ideals in R.

Characteristic

Recall that for any ring R there is a unique homomorphism $\phi : \mathbb{Z} \to R$. Then $\ker \phi \lhd \mathbb{Z}$ and so $\ker \phi = (n)$ for some $n = 0, 1, \ldots$. Then n is the *characteristic* of the ring R.

Quotient rings

If $I \lhd R$ then the cosets $R/I = \{a + I \mid a \in R\}$ form a ring — the *quotient ring*. The *quotient map* $q : R \to R/I$ is a ring homomorphism.

Isomorphism theorem

If $\theta : R \to S$ is a ring homomorphism then $\ker \theta \lhd R$, $\operatorname{Im} \theta \leq S$ and there exists an isomorphism $\bar{\theta} : R/\ker \theta \to \operatorname{Im} \theta$ so that θ factors as

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ \downarrow & & \uparrow \\ R/\ker \theta & \xrightarrow{\bar{\theta}} & \operatorname{Im} \theta \end{array}$$

Fields and integral domains

Recall the definition of a field.

A *integral domain* is a ring R if $0 \neq 1$ and whenever $ab = 0$ in R then $a = 0$ or $b = 0$. Any field is an integral domain.

Any finite integral domain is a field, as for any $a \neq 0 \in R$ the map given by left-multiplication by a is a group homomorphism with trivial kernel, so it is injective and hence bijective, and so a has an inverse.

If R is an integral domain then so is $R[X]$ — consider the leading term of the product of two polynomials in $R[X]$.

The remainder theorem

If R is a ring, $f(X) \in R[X]$ and $a \in R$ such that $f(a) = 0$, then

$$f(X) = (X - a)g(X)$$

for some $g(X) \in R[X]$.

Proof

If

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

and $f(a) = 0$, then

$$0 = a_0 + a_1a + a_2a^2 + \cdots + a_na^n$$

and so subtracting we get

$$\begin{aligned} f(X) &= a_1(X-a) + a_2(X^2-a^2) + \cdots + a_n(X^n-a^n) \\ &= a_1(X-a) + a_2(X-a)(X+a) + \cdots + a_n(X-a)(X^{n-1} + \cdots + a^{n-1}) \\ &= (X-a)g(X) \end{aligned}$$

for some $g(X) \in R[X]$.

If R is an integral domain then a polynomial of degree n in $R[X]$ has at most n roots. This is proved by induction on n, using the remainder theorem and the fact that if

$$f(X) = (X-a)g(X)$$

then any root of f is either a or a root of $g(X)$ (since R is an integral domain).

Theorem

A finite subgroup of the multiplicative group of units of a field (or integral domain) is cyclic.

Proof

Let K be a field and let $G \leq K^*$ with $|G| = n$.

1. Let m be the lowest common multiple of the orders of the elements of G. By Lagrange's Theorem $m \mid n$. But all the elements of G are roots of the polynomial $X^m - 1$ in K. But $X^m - 1$ has at most m distinct roots, so $m \geq n$ and so $m = n$.
2. From the structure theorem for abelian groups we know that $G \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_k}$ for $d_1 \mid d_2 \mid \cdots \mid d_k$. So if the

   ...

The field of fractions

Definition and proof of existence.

Maximal and prime ideals

Definitions. Equivalence to quotient ring being a field or integral domain.

Principal Ideal Domains

Definition.

Euclidean domains

Definition. $k[X]$ is Euclidean. Euclidean $\Rightarrow$ PID.

Primes and irreducibles

Definitions. In a domain, prime $\Rightarrow$ irreducible. In a PID, irreducible $\Rightarrow$ prime.

Definition of a Noetherian ring. Any PID is Noetherian.

Factorization into irreducibles is possible in a PID.

A PID is a UFD.

In a PID, a non-zero prime ideal is maximal.

Unique Factorization Domains

The content. Gauss' Lemma and Eisenstein's Irreducibility Criterion.

If R is a UFD then so is $R[X]$.

Noetherian Rings

Hilbert's Basis Theorem: If R is noetherian then so is $R[X]$.

Invariant Theory

Idea

We have a vector space V over k and a group G of k-automorphisms of V. We want to find invariants, i.e. functions $f : V^m \to k$ such that

$$f(gv_1, \ldots, gv_m) = f(v_1, \ldots, v_m).$$

In other words, f is a function which is constant on the orbits of the G-action.

More abstractly, we have a ring R (of functions on V^m) and an action of G on R, and we seek to characterize

$$R^G = \{a \in R \mid ga = a \text{ for all } g \in G\}.$$

We will usually have $m = 1$, $V \cong \mathbb{C}^n$ and $R = \mathbb{C}[X_1, \ldots, X_n]$ the ring of polynomial functions on V.

Examples

1. The group $G = S_n$ acting on the polynomial ring $\mathbb{C}[X_1, \ldots, X_n]$.

   The invariant ring is generated by the elementary symmetric polynomials, and so

   $$\mathbb{C}[X_1, \ldots, X_n]^{S_n} = \mathbb{C}[e_1, \ldots, e_n],$$

   where e_i is the ith symmetric polynomial. This is a polynomial ring in the e_i.

2. The group $G = C_n$ generated by the matrix $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)$ acting on $\mathbb{C}[X, Y]$ by

   $$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} : \sum \lambda_{rs} X^r Y^s \longmapsto \sum \lambda_{rs} X^r Y^s \zeta^{r-s}.$$

   The only monomials fixed by every $g \in G$ are of the form $X^r Y^s$ where $n \mid r - s$. Any linear combination of these monomials is an invariant. Any such monomial is either

   $$X^r Y^{kn+r} = (XY)^r (Y^n)^k$$
   $$\text{or} \qquad X^{kn+s} Y^s = (XY)^s (X^n)^k,$$

   i.e. is a polynomial in XY, X^n and Y^n. Therefore

   $$\mathbb{C}[X, Y]^{C_n} = \mathbb{C}[XY, X^n, Y^n].$$

   This is not a polynomial ring, since $(XY)^n = X^n Y^n$.

3. The group $G = D_{2n}$ generated by a matrix $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)$ as before and the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, where

   $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : \sum \lambda_{rs} X^r Y^s \longmapsto \sum \lambda_{rs} X^s Y^r.$$

For any invariant we must have (in addition to the constraint in (2)) that $\lambda_{rs} = \lambda_{sr}$ for all r and s. Thus we have the linear combinations of

$$X^r Y^r$$
$$X^r Y^s + X^s Y^r \qquad \text{where } n \mid r - s.$$

But $(X^r Y^r) = (XY)^r$, and something of the form $X^r Y^s + X^s Y^r$, with $n \mid r - s$ is of the form

$$(XY)^r (X^{kn} + Y^{kn}).$$

But now observe that

$$X^{(k+1)n} + Y^{(k+1)n} = (X^n + Y^n)(X^{kn} + Y^{kn}) - (XY)^n (X^{(k-1)n} + Y^{(k-1)n}$$

and so the invariant ring is

$$\mathbb{C}[X, Y]^{D_{2n}} = \mathbb{C}[XY, X^n + Y^n].$$

This is a polynomial ring.

Better explanation at start of lecture 13.

Remark

$h \in R^G$ iff all the homogeneous parts of h are in R^G.

Main result

If G is any finite subgroup of $\mathrm{GL}_n(k)$, with k of characteristic zero, then

$$R^G = \mathbb{C}[X_1, \ldots, X_n]^G$$

is finitely generated.

Symmetric functions

The symmetric group acts on $\mathbb{C}^n$ by permuting coordinates. Write $\Lambda = \mathbb{C}[X_1, \ldots, X_n]^{S_n}$ for the ring of symmetric functions.

Theorem

$$\Lambda = \mathbb{C}[X_1, \ldots, X_n]^{S_n} = \mathbb{C}[e_1, \ldots, e_n],$$

where e_i is the ith elementary symmetric function. Further, $\mathbb{C}[e_1, \ldots, e_n]$ is a polynomial ring.

Proof

Put the (reverse?) lexicographic ordering on the monomials, so

$$X_1^{r_1} \cdots X_n^{r_n} > X_1^{s_1} \cdots X_n^{s_n}$$

iff the first i with $r_i \neq s_i$ has $r_i > s_i$. For $f \in \mathbb{C}[X_1, \ldots, X_n]$, let $\mathrm{hm}(f)$ be the highest monomial in f with respect to this ordering. Then

- If $f \in \Lambda$ then $\mathrm{hm}(f) = X_1^{r_1} \cdots X_n^{r_n}$ has $r_1 \geq r_2 \geq \cdots \geq r_n$.
- hm is multiplicative: $\mathrm{hm}(fg) = \mathrm{hm}(f)\,\mathrm{hm}(g)$ for all f, g.
  Therefore $\mathrm{hm}(e_1^{k_1} \cdots e_n^{k_n}) = X_1^{k_1+\cdots+k_n} X_2^{k_2+\cdots+k_n} \cdots X_n^{k_n}$.

Let $f \in \Lambda$ be a homogeneous polynomial. Let $\mathrm{hm}(f) = X_1^{r_1} \cdots X_n^{r_n}$. Then let $g = f - ae_1^{r_1-r_2} e_2^{r_2-r_3} \cdots e_n^{r_n}$. So $g \in \Lambda$ with $\mathrm{hm}(g) < \mathrm{hm}(f)$. By induction on $\mathrm{hm}(f)$ we see that $f \in \mathbb{C}[e_1, \ldots, e_n]$.

Now, suppose that $h(Z_1, \ldots, Z_n)$ is a non-zero polynomial. Consider the monomial $Z_1^{k_1} \cdots X_n^{k_n}$ in h such that

$$X_1^{k_1+\cdots+k_n} \cdots X_n^{k_n}$$

is greatest. Then in $h(e_1, \ldots, e_n)$ the highest monomial is

$$X_1^{k_1+\cdots+k_n} \cdots X_n^{k_n}$$

and so $h(e_1, \ldots, e_n) \neq 0$. Thus $\mathbb{C}[e_1, \ldots, e_n]$ is a polynomial ring.

Symmetric powers

The symmetric powers are $p_i = X_1^i + \cdots + X_n^i$. We can obtain recurrence relations for these. Note that

$$E(t) = \prod_{i=1}^{n} (1 + X_i t) = 1 + e_1 t + \cdots + e_n t^n.$$

Now consider

$$\frac{E'(t)}{E(t)} = \frac{d}{dt} \{\log E(t)\} = \sum_{i=1}^{n} \frac{X_i}{1 + X_i t} = p_1 - p_2 t + p_3 t^2 - \cdots$$

Thus

$$E'(t) = (e_1 + 2e_2t + 3e_3t^2 + \cdots) = (p_1 - p_2t + p_3t^2 - \cdots)(1 + e_1t + e_2t^2 + \cdots + e_nt^n).$$

So

$$\begin{aligned} e_1 &= p_1 \\ 2e_2 &= p_1e_1 - p_2 \\ 3e_3 &= p_1e_2 - p_2e_1 + p_3 \end{aligned}$$

and so on.

The alternating group

We want to find the invariant ring of $A_n \leq S_n$.

see lecture notes.

Noether's method

This is a method for finding a finite generating set for an invariant ring. Let k be a field of characteristic zero, let $R = k[X_1, \ldots, X_n]$ and let G be a finite subgroup of $\mathrm{GL}_n(k)$ acting on R as explained. Let $N = |G|$. Consider the following.

1. Take any $a \in R$. Consider the polynomial in $R[t]$

$$p_a(t) = \prod_{\sigma \in G} (t - \sigma a) = t^N - c_1 t^{N-1} + c_2 t^{N-2} - \cdots$$

   and the c_i are the elementary symmetric functions in the conjugates $(\sigma a)_{\sigma \in G}$ of a. Clearly $c_i \in R^G$.

2. The (Reynolds) averaging operator ρ is defined by

$$\rho(a) = \frac{1}{N} \sum_{\sigma \in G} \sigma a.$$

   $\rho : R \to R^G$ as is additive. Also, if $a \in R^G$ and $b \in R$ then $\rho(ab) = a\rho(b)$, i.e. ρ is R^G-linear, since

$$\rho(ab) = \frac{1}{N} \sum_{\sigma \in G} \sigma(ab) = \frac{1}{N} \sum_{\sigma \in G} \sigma(a)\sigma(b) = a\rho(b).$$

Then the following give a generating set of invariants

1. The coefficients c_i of the polynomials $p_{x_i}(t)$
2. Elements $\rho(X_1^{r_1} \cdots X_n^{r_n})$ for all monomials $X_1^{r_1} \cdots X_n^{r_n}$, with $\max r_i < N$.