Week 1 Notes

Abstract Algebra

shaozewxy

May 2022

1.4 Matrix Groups

Defintion of a ***field***

A *field* is a set F with two operations $+$ and $\times$,

such that $(F, +)$ is an abelian group, and $(F - \{0\}, \times)$ is also an abelian group,

while also satisfying the distribution rule:

$$\forall a, b, c \in F, a \times (b + c) = a \times b + a \times c$$

Properties of Matrix Groups and Fields

These facts will be proven later.

1. If F is a field, and F is finite, then $|F| = p^m$ for some $p, m \in \mathbb{Z}$ and p a prime.
2. If $|F| = q$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2)...(q^n - q^{n-1})$

1.5 The Quaternion Group

Definition of the ***Quaternion Group***

The *Quaternion Group* us defined as:

$$Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$$

with product computed as:

$$\forall a \in Q_8, 1a = a1 = a$$

$$\forall a \in Q_8, (-1)(-1) = 1, (-1)a = a(-1) = -a$$

$$ii = jj = kk = -1$$

$$ij = k, ji = -k$$

$$jk = i, kj = -i$$

$$ki = j, ik = -j$$

The Quaternion Group is the smallest non-abelian group.

1.6 Homomorphisms and Isomorphisms

Examples

1. For any group $G, G \cong G$.

While the identity map is an obvious isomorphism between G and G, it is not necessarily the only such isomorphism.

2. The exponential map $\exp : \mathbb{R} \to \mathbb{R}^+$ defined by $\exp(x) = e^x$. This is an

isomorphism from $(\mathbb{R},+) \to (\mathbb{R}^+,\times)$.

This is so because this function has an inverse $\log_e(x)$ and $e^x e^y = e^{x+y}$.

3. We show that the isomorphism type of a symmetric group is dependent only on the cardinality of the underlying set being permuted.

Δ, Ω two nonempty sets with the same size, then $S_\Delta \cong S_\Omega$:

given $|\Delta| = |\Omega|$, then there exists a bijection θ between Δ, Ω. We can then define isomorphism $\phi : S_\Delta \to S_\Omega$ using θ:

$$\phi(\sigma) = \sigma' : \Omega \to \Omega, \sigma'(x) = \theta(\sigma(x))$$

Conversely, if $S_\Delta \cong S_\Omega$, then it is obvious that $|S_\Delta| = |S_\Omega|$, i.e., $|\Delta|! = |\Omega|!$, therefore $|\Delta| = |\Omega|$.

Properties about Isomorphisms

1. Any non-abelian group of order 6 is isomorphis to S_3.

In face, there are only two types of groups of order 6, S_3 and $\mathbb{Z}/6\mathbb{Z}$.

2. If $\phi : G \to H$ is an isomorphism, then:

$|G| = |H|$

G is abelian iff H is ableian.

$\forall x \in G, |x| = |\phi(x)|$.

Using these rules, we can determine some groups are not isomorphic conveniently:

S_3 and $\mathbb{Z}/6\mathbb{Z}$ are not isomorphic because one is abelian and one is not.

$(\mathbb{R}-\{0\},\times), (\mathbb{R},+)$ are not isomorphic because -1 has order 2 in $(\mathbb{R}-\{0\},\times)$ while no elements in $(\mathbb{R},+)$ has order 2.

3. G a finite group of order n with $A = \{s_1, ..., s_m\}$ generating G. H another group $B = \{r_1, ..., r_m\}$ elements of H. If any relation of A is also satisfied by

B by replacing s_i with r_i, then there is a unique homomorphism $\phi : G \to H$ which maps s_i to r_i.

This means to check isomorphism, we only need to check the presentation of G:

If B generates H, then ϕ is surjective, and if additionally, $|H| = |G|$, then ϕ is an isomorphism.

Examples

1. $D_{2n} = \langle r, s | r^n = s^2 = 1, sr = r^{-1}s \rangle$. Suppose H a group containing elements a, b with $a^n = b^2 = 1, ba = a^{-1}b$. Then $\exists$ homomorphism from D_{2n} to H mapping r to a and s to b.

Given $k|n$, the D_{2k} has a homomorphism to D_{2n}. Because $\{r_1, s_1\}$ generates D_{2k}, the homomorphism is surjective.

2. Between D_6 and S_3, with elements $a = (123), b = (12)$ satisfies $a^3 = 1, b^2 = 1, ba = ab^{-1}$. Then there is a homomorphism from D_6 to S_3 that sends $r \to a$, $s \to b$. Because S_3 is generated by a, b and $|S_3| = |D_6|$, then $D_6 \cong S_3$.