MATH H113: Honors Introduction to Abstract Algebra

2016-02-05

- Symmetric groups and cycles
- Matrix groups
- Homomorphisms

Homework due 2016-02-12

- 1.3: 8, 10, 11
- 1.4: 10
- 1.5: 3
- 1.6: 2, 9, 18, 19
- 1.7: 8, 12, 18

D_8

n	1	2	3	4	5	6	7	8
$r(n)$	8	1	2	3	4	5	6	7
$s(n)$	1	8	7	6	5	4	3	2
$r \circ s$	8	7	6	5	4	3	2	1

In Cycle Notation

$r = (1\ 8\ 7\ 6\ 5\ 4\ 3\ 2)$
$s = (1)(2\ 8)(3\ 7)(4\ 6)(5)$
$rs = (1\ 8\ 7\ 6\ 5\ 4\ 3\ 2)(2\ 8)(3\ 7)(4\ 6) = (1\ 8)(2\ 7)(3\ 6)(4\ 5)$
It will be proved later: except for the changes of:

i. eliniminating or adding 1-cycles
ii. permuting the order of the cycles (as above)
iii. starting the cycles at a different point

the writing of an element of S_n as a product of disjoint cycles is unique. $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$

The inverse of a cycle $(a_1\ a_2\ \ldots\ a_m)$ is $(a_m\ a_{m-1}\ \ldots\ a_1)$.

Exercise 15: The order of a product of disjoint cycles is the least common multiple (lcm) of the lengths of the cycles.

First: The order of a cycles $\tau = (a_1\ a_2\ \ldots\ a_m)$ is m. To see this:
if $m > 1$ then $\tau(a_1) = a_2 \neq a_1$, so $\tau \neq 1$
if $m > 2$ then $\tau^2(a_1) = a_3 \neq a_1$, so $\tau^2 \neq 1$
by induction if $m > i$ the $\tau^i(a_1) = a_{1+i} \neq a_1$ so $\tau^i \neq 1$
$\therefore |\tau| \geq m$.
But $\tau^m(a_1) = \tau(\tau^{m-1}(a_1)) = \tau(a_m) = a_1$
$\tau^m(a_2) = \tau^2(\tau^{m-2}(a_2)) = \tau^2(a_m) = \tau(a_1) = a_2$
etc.
so $\tau^m = 1 \therefore |\tau| = m$.

So suppose $\sigma \in S_n$ is a product $\sigma = \tau_1, \tau_2, \ldots, \tau_r$ of disjoint cycles of lengths $m_1, m_2, \ldots, m_r$, respectively.
Induction on r:
if $r = 0$, then $\sigma = 1$ (empty product) and $|\sigma| = 1$ and $\mathrm{lcm}(\phi) = 1$.
if $r = 1$, then $|\tau| = m_1$ and $\mathrm{lcm}(m_1) = m_1$
Inductive step: $\tau = \rho\tau_r$ where $\rho = \tau_1, \ldots, \tau_{r-1}$ commutes with τ_r and $|\rho| = \mathrm{lcm}(m_1, \ldots, m_{r-1})$ and $|\tau_r| = m_r$, so by an exercise, $|\tau| = \mathrm{lcm}(|\rho|, |\tau_r|) = \mathrm{lcm}(\mathrm{lcm}(m_1, \ldots, m_{r-1}), m_r) = \mathrm{lcm}(m_1, \ldots, m_r)$.

Matrix Groups

Definition: A *field* F is an ordered triple $(F, +, \cdot)$, where $+$ and $\cdot$ are commutative binary operations, such that:

1. $(F, +)$ is an abelian group. This is written additively, and its identity element is written as 0
2. $(F^\times, \cdot)$ is an abelian group, where $F^\times = F \setminus \{0\}$. This group is written multiplicatively and its identity element is written 1.
3. The distributive law holds:
   $a(b + c) = ab + ac\ \forall a, b, c \in F$.
   Note: $a \times 0 = 0 \times a = 0\ \forall a \in F$. This follows from the distributive law, because $a \cdot 1 = a \cdot (1 + 0) = a \cdot 1 + a \cdot 0$.
   Now cancel $a \cdot 1$
   Also $0 \cdot a = a \cdot 0 = 0$ because $\cdot$ is commutative.
   Also $a \cdot 1 = a\ \forall a \in F$:
   true if $a \neq 0$ because 1 is the identity in $F^\times$
   true if $a = 0$ because of $a \times 0 = 0 \times a = 0$

Examples of Fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}\ \forall$ primes p (we'll see this later, but use it now).
You can do linear algebra over any field F. In particular, a square matrix M with entries in F is invertible $\iff$ $\det(M) \neq 0$, and the formulas for M^{-1} (in terms of minors) still works, as well as $\det(MN) = \det(M)\det(N)$.

Definition: Let F be a field, and let $n \in \mathbb{Z}_{>0}$ (or even $n \in \mathbb{N}$). Then $\mathrm{GL}_n(F)$ is the group whose elements are the invertible $n \times n$ matrices with entries in F,

and whose operation is matrix multiplication.
(If $n = 0$, $\mathrm{GL}_0(F)$ = the trivial group = $\{[]\}$ $\det([]) = 1$).
Comment: For all fields F, $\mathrm{GL}_2(F)$ is nonabelian, because
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ but $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.
Similarly for $n > 2$ (see figure 2) don't commute.
Also: $\mathrm{GL}_1(F) = F^\times \leftarrow$ (when mentioning $F^\times$ as a group, $(F^\times, \cdot)$ is meant).
Also, $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ is a finite group $\forall$ fields F and $\forall n \in \mathbb{N}$.

Read Section 1.5 (the Quaternion Group) (it's a non-abelian group of order 8).

Homomorphisms

Definition: Let $(G, \star)$ and $(H, \cdot)$ be groups. A homomorphism ϕ from G to H is a function $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \cdot \phi(y)$ $\forall x, y \in G$ (multiplication is preserved)
(usually $\phi(xy) = \phi(x)\phi(y)$ is written).
Examples:

1. Let F $((F, +, \cdot))$ be a field and let $n \in \mathbb{N}$ then $\det : \mathrm{GL}_n(F) \to F^\times$ is a homomorphism because $\det(M) \neq 0$ $\forall M \in \mathrm{GL}_n(F)$ and $\det(MN) = \det(M)\det(N)$ $\forall M, N \in \mathrm{GL}_n(F)$.
2. For any $n \in \mathbb{Z}_{>0}$, $m \mapsto \bar{m}$ is a homomorphism from $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ (by definition of $+$ on $\mathbb{Z}/n\mathbb{Z}$, $\overline{a+b} = \bar{a} + \bar{b}$).