MATH H113: Honors Introduction to Abstract Algebra

2016-03-18

- Generators & Relations
- Rings

Homework for Apr. 1 will be assigned Mar. 29

Last time: we showed that if S is a set then the set $F(S)$ of all reduced words $(S_1^{\epsilon_1}, \ldots, S_n^{\epsilon_n})$ $(n \in \mathbb{N}, S_i \in S\ \forall i, \epsilon_i \in \{\pm 1\}\ \forall i)$ is a group, and satisfies the universal property for all groups G and all functions $\phi : S \to G$ there is a unique homomorphism $\Phi : F(S) \to G$ such that $f = \Phi \circ i$
See figure 1.
Here i takes s to $(s^1)\ \forall s \in S$.
Proof: Map $(s_1^{\epsilon_1}, \cdots, s_n^{\epsilon_n})$ to $\phi(s_1)^{\epsilon_1} \ldots \phi(s_n)^{\epsilon_1}$. Check that it's a homomorphism.

Examples:
0. $S \neq \emptyset$, then $F(S)$ has only the empty word so $F(S) = \{1\}$. 1. $S = \{x\}$ then $F(S) = \{(s^\epsilon, s^\epsilon, \ldots, s^\epsilon)\}$ length $n \in \mathbb{N}$, $\epsilon \in \{\pm 1\})$ This is $\mathbb{Z}$ because if $\epsilon = 1$ then $(s^\epsilon, \ldots, s^\epsilon) \mapsto n$, if $\epsilon = -1$ then $(s^\epsilon, \ldots, s^\epsilon) \mapsto n$. Finally, if $|s| > 1$ then $F(S)$ is infinite and non-abelian.

Generators and Relations

We can define what $\langle S|R\rangle$ where S is a set and R is a collection of *relations* of the form $w_1 = w_2$, with $w_1, w_2 \in F(S)$. Let R be $\{w_i = w_i' : i \in I\}$ where $w_i, w_i' \in F(S)\ \forall i$. Let N be the smallest norml subgroup of $F(S)$ containing $w_i, w_i^{-1}\ \forall i \in I$. So $N = \bigcap$ of all normal subgroups of $F(S)$ that contain $w_i^{-1}, w_i'\ \forall i \in I = \langle x w_i^{-1} w_i' x^{-1} : iinI, x \in F(S)\rangle$. Then $\langle S \mid R\rangle = F(S)/N$
Back to $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$ We showed all elements of $F(S)/N$ (N as above, $S = \{r, s\}$) can be written as $r^i s^j$ for some $i = 0, \ldots, n-1, j = 0, 1$. Then we showed that the these are all distinct in $F(S)/N$ by exhibiting a group G with elements r, s such that $\langle r, s\rangle = G$ and all relations are true in G.
That shows:
See fig 2.
that is 1-1 on the set $\{r^i s^j : 0 \leq i < n, j = 0, 1\}$. $\therefore N \not\ni r^i s^j (r^{i'} s^{j'})^{-1}$ with $0 \leq i < n$, $0 \leq i' < n$, $j, j' \in \{0, 1\}$, $i \neq i' or j \neq j'$. because $\Phi(N) = 1$ and these elements are distinct in G.
Actually $\langle S \mid R\rangle$ satisfies a universal property: we have a function $i : S \to \langle S \mid R\rangle$ (taking $s \in S$ to itself). For all groups G and all function $f : S \to G$ such that the elements $f(s) \in G$ $(s \in S)$ satsify all of the relations of R, there is a unique homomorphism $\Phi : \langle S \mid R\rangle \to G$ such taht $f = \Phi \circ i$

See fig 3.
Proof: From the universal property for $F(S)$, there is a unique $\psi : F(S) \to G$ such that $\psi(s) = f(s)\ \forall s \in S$. $\ker\psi \ni w_i^{-1}w_i'$ for relations $w_i = w_i'$ in R so $\ker\psi \supseteq N$ as in the def. of $\langle S \mid R\rangle$.
See fig 4.
Then we can define Φ $F(S)/N$ to G by $\Phi(xN) = \Psi(x)$ well defined because $n \subseteq \ker\psi$, and $\Phi(i(x)) = \Phi(\pi(j(s))) = \Phi(j(s)N) = \Psi(j(s)) = f(s)\ \forall s \in S$ (unique because for any other Φ', $\Phi' \circ \pi$ must be Ψ by uniqueness of the universal property of $F(S)$).

Rings

Definition: A *ring* $R =$ (more formally: $(R, +, \times)$ is a set R, together with binary operations $+$ and $\times$ such that:

i. $(R, +)$ is an abelian group. This is written additively, so $0 \in R$ is its identity element.
ii. $\times$ is associative:
$a \times (b \times c) = (a \times b) \times c\ \forall a, b, c \in R$
iii. distributive law holds
$a \times (b + c) = a \times b + a \times c$
$(b + c) \times a = b \times a + c \times a$
(doing multiplications before addition)

Examples:

1. $M_n(\mathbb{R})$ = set of all $n \times n$ matrices with entries in $\mathbb{R}$; $+$ is matrix addition, $\times$ is matrix multiplication (not commutative if $n \geq 2$).
2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/m\mathbb{Z}$
3. Any abelian group with $x \times y = 0\ \forall x, y \in A$ (the "trivial ring")
4. The "zero ring" $R = \{0\}$
5. $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$

We'll usually write $a \times b$ as ab

Definition: A ring R is commutative if multiplication (in R) is commutative:
$xy = yx\ \forall x, y \in R$
Example (1) is *not* commutative unless $n \leq 1$
Examples (2) - (5) are commutative

Definition: A ring R has an identity (element) (or, the ring has 1) if there is an element $1 \in R$ such that $x1 = 1x = x\ \forall x \in R$.
(3) does *not* have an identity element unless $A = \{0\}$
(5) does *not* have an identity element
A ring R can have at most one identity element: $1 = 11' = 1'$

Proposition: Let R be a ring with 1. Then $1 = 0$ (in R) $\iff$ R is the zero ring
Proof:

- "$\Longleftarrow$": obvious
- "$\Longrightarrow$": if $1 = 0$ then $x = 1x = 0x = 0\ \forall x \in R$, so $R \neq \{0\}$.

Usual algebra relations hold ($\forall a, b \in R$):
$0a = a0 = 0$
$(-a)b = a(-b) = -ab$
$(-a)(-b) = ab$
$-(-a) = a$
$(-1)a = -a$ if R has 1