Lecture 15: Presentation

Thursday, November 15, 2018 5:12 PM

How can we show $\langle X|R\rangle \simeq G$ where G is, say, a given finite gp?

As we mentioned in the previous lecture there is no general method to answer this question; but here is a common strategy.

Step 1. Find a generating set $\overline{X}$ of G that satisfies the given relations R; that means $\exists$ an onto function $f: X \to \overline{X}$ s.t. after "evaluating" elements of R w.r.t. f we end up getting e. (In Steps 2 and 3, it will be made more formal.)

Step 2. Using universal property of free groups we get a group homomorphism $\hat{f}: F(X) \to G$ s.t. $\hat{f}|_X = \overline{f}$. In particular $\overline{X} \subseteq \operatorname{Im} \hat{f}$, and so $\hat{f}$ is onto.

Step 3. Since $\overline{X}$ satisfies R, $R \subseteq \ker \hat{f}$; and so $\langle \bigcup_{g \in F(X)} gRg^{-1} \rangle \subseteq \ker \hat{f}$. Therefore

$$F(X)/\langle \bigcup_{g\in F(X)} gRg^{-1}\rangle \xrightarrow[\text{onto}]{} F(X)/\ker \hat{f} \xrightarrow{\simeq} \operatorname{Im}\hat{f} = G$$

we get an onto group homomorphism $\Phi: \langle X|R\rangle \to G$.

Lecture 15: Presentation

Tuesday, November 13, 2018 4:59 PM

Step 4. Try to show Φ is injective; we often go about this showing

$|\langle X|R\rangle| \leq |G|$ (when G is finite).

Ex. $\langle a | a^n \rangle \simeq \mathbb{Z}/_{n\mathbb{Z}}$.

Pf. $\mathbb{Z}/_{n\mathbb{Z}} = \langle 1 \rangle$ and $n\,1 = 0$; and so by Steps 1-3 $\exists$ an onto group homomorphism $\Phi: \langle a \mid a^n \rangle \longrightarrow \mathbb{Z}/_{n\mathbb{Z}}$, $\Phi(a) = 1$.

$\langle a \mid a^n \rangle = \{ a^k \mid k \in \mathbb{Z} \} = \{ a^k \mid 0 \leq k < n \}$ implies

$$|\langle a | a^n \rangle| \leq n = |\mathbb{Z}/_{n\mathbb{Z}}|;$$

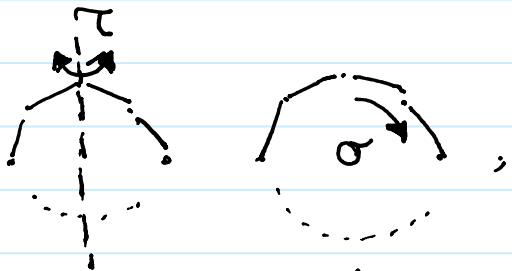
and so Φ is a bijection, and claim follows. ∎

Ex. $\langle a, b \mid a^2, b^n, aba^{-1} = b^{-1} \rangle \simeq D_{2n}$.

this means $aba^{-1}b$ as a relation.

Pf.

Recall that $D_{2n} = \langle \tau, \sigma \rangle$ where



and $\tau\sigma\tau^{-1} = \sigma^{-1}$ (*). Since $\tau^2 = \sigma^n = id.$ and (*), τ and σ satisfy the given relations. Therefore by Steps 1-3 $\exists$ an onto group homomorphism $\Phi: \langle a, b \mid a^2, b^n, aba^{-1} = b^{-1} \rangle \longrightarrow D_{2n}$.

By induction on k, $a^k b a^{-k} = b^{(-1)^k}$; and so $a^k b^l a^{-k} = b^{(-1)^k l}$.

Lecture 15: Presentation

Tuesday, November 13, 2018 1:42 AM

Therefore $a^k b^l = b^{(-1)^k l} a^k$. This implies we can reorder powers of $\underline{a}$ by powers of $\underline{b}$. And so any element can be written as a power of $\underline{a}$ times a power of $\underline{b}$. Hence

$$\langle a,b \mid a^2, b^n, aba^{-1} = b^{-1} \rangle = \{ a^k b^l \mid k,l \in \mathbb{Z} \}$$

$$= \{ a^k b^l \mid 0 \le k \le 1,\ 0 \le l \le n-1 \}$$

(as $a^2 = b^n = 1$)

And so $|\langle a,b \mid a^2, b^n, aba^{-1} = b^{-1} \rangle| \le 2n = |D_{2n}|$

And so ϕ is onto. ∎

As part of your HW assignment, you will prove that

$$\langle X_1 | R_1 \rangle * \langle X_2 | R_2 \rangle \simeq \langle X_1 \sqcup X_2 \mid R_1 \sqcup R_2 \rangle ; \text{ and so}$$

$$\left\langle \overline{\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}}, \overline{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}} \right\rangle \simeq \mathbb{Z} * (\mathbb{Z}/2\mathbb{Z}) \simeq \langle a \rangle * \langle b \mid b^2 \rangle \simeq \langle a,b \mid b^2 \rangle.$$

Lecture 15: Historical remark on algebra

Tuesday, November 13, 2018 8:32 AM

Historically algebra was developed to study zeros of polynomials. Kharazmi wrote a book and gave algorithms to find zeros of degree 1 and deg. 2 polynomials. In 11 century Khayyam gave geometric methods of finding zeros of deg. 3 polynomial by means of intersection of conic curves. In 16 century Italian mathematicians Tartaglia and Cardano finished the case of deg. 3 polynomials and Cardano's student, Ferrari solved the case of deg. 4 polynomials. In 1824, Abel showed that there is no solution in radicals to the general poly. eq. of deg. ≥ 5. In 1832, Galois gave an elegent treatment of understanding zeros of a single variable poly.; and he essentially said the group of symmetries of zeros is the key tool to study them.

Then algebra grew in two (related) directions: understanding zeros of multi-variable polynomials (using geometric intuitions); And trying to prove Fermat's last conjecture (finding zeros of

Lecture 15: Historical remark on algebra

Sunday, December 2, 2018 1:09 PM

$X^n+y^n-z^n=0$ in $\mathbb{Z}$ or equivalently zeros of X^n+Y^n-1 in $\mathbb{Q}$.)

These were motivations to study (mostly) commutative, unital rings.

Def. A set R with two binary operations and $0, 1$ is called a (unital) ring if

- $(R,+,0)$ is an abelian group with neutral element 0.
- $(R,\cdot,1)$ is a monoid with the identity. (Associativity)
- (distribution) $a\cdot(b+c)=a\cdot b+a\cdot c$

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

Ex. Suppose R is any unital ring. The matrix ring $M_n(R)$ with entries in R is $\{[a_{ij}]_{\substack{1\le i\le n\\ 1\le j\le n}} \mid a_{ij}\in R\}$ and

$$[a_{ij}]+[b_{ij}]:=[a_{ij}+b_{ij}],\quad [a_{ij}]\cdot[b_{ij}]:=\left[\sum_{k=1}^{n} a_{ik}\,b_{kj}\right].$$

One can check that $M_n(R)$ is a unital ring. Notice that, for $n\ge 2$, $M_n(R)$ is not commutative; that means there are two matrices x, y s.t. $xy\neq yx$. For instance $\begin{bmatrix}0&1\\0&0\end{bmatrix}\begin{bmatrix}0&0\\1&0\end{bmatrix}\neq\begin{bmatrix}0&0\\1&0\end{bmatrix}\begin{bmatrix}0&1\\0&0\end{bmatrix}$.

Lecture 15: Monoid ring

Sunday, December 2, 2018 1:40 PM

Suppose $(M, \cdot)$ is a monoid, and R is a unital ring. The monoid ring

$$RM := \left\{ \sum_{m \in M} r_m m \;\middle|\; r_m = 0 \text{ except for finitely many } m \in M \right\}$$

Here $\sum_{m \in M} r_m m$ is just a formal sum to help us remember $+$ and $\cdot$:

- $\left(\sum_{m \in M} r_m m\right) + \left(\sum_{m \in M} r'_m m\right) = \sum_{m \in M} (r_m + r'_m) m$
- $\left(\sum_{m \in M} r_m m\right) \cdot \left(\sum_{m \in M} r'_m m\right) = \sum_{m, m' \in M} r_m r'_{m'} mm'$

  ↓ having distribution

  $$= \sum_{m \in M} \left(\sum_{m_1 m_2 = m} r_{m_1} r'_{m_2} \right) m .$$

When M is a group, RM is called a group ring.

- When M is not abelian, RM is not commutative.
- Group ring $\mathbb{C}G$ is an important tool to study representations of a finite group. When G is infinite, one has to introduce analysis. So it is useful to view elements of the monoid ring RM as functions $f: M \to R$. In this point of view to avoid

confusion with pointwise multiplication of functions, the ring multiplication is denoted by $*$, and it is called convolution.

$(f_1 * f_2)(m) := \sum_{m = m_1 m_2} f_1(m_1) f_2(m_2)$ and

$\operatorname{Supp} f_i := \{m \in M \mid f_i(m) \neq 0\}$ is finite.

When M is countable and $R = \mathbb{C}$, we can consider

$\ell^1(M) := \{f : M \to \mathbb{C} \mid \sum_{m \in M} |f(m)| < \infty\}$ and using Fubini one can show, if $f_1, f_2 \in \ell^1(M)$, then $f_1 * f_2$ is well-defined and $f_1 * f_2 \in \ell^1(M)$. This forms a Banach algebra and has the group ring $\mathbb{C}M$ as a bring.

An important example of monoid rings is $R(\mathbb{Z}^{\geq 0})^n$. In this case we often view $(\mathbb{Z}^{\geq 0})^n$ in multiplicative form using a set of indeterminants $x_1, \dots, x_n$:

$(\mathbb{Z}^{\geq 0})^n \xrightarrow{\sim} \{x_1^{i_1} \cdots x_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{Z}^{\geq 0}\}$

$(i_1, \dots, i_n) \longmapsto x_1^{i_1} \cdots x_n^{i_n}$. And so

$R(\mathbb{Z}^{\geq 0})^n$ can be viewed as $\{\sum_{\vec{i} \in (\mathbb{Z}^{\geq 0})^n} a_{\vec{i}} x_1^{i_1} \cdots x_n^{i_n} \mid a_{\vec{i}} = 0$ except for finitely many$\}$

Lecture 15: Polynomial ring

Tuesday, December 4, 2018 7:35 PM

This is denoted by $R[x_1, \ldots, x_n]$ and is called the polynomial ring with coefficients in R and indeterminants $x_1, \ldots, x_n$. It is often useful to think about it inductively as well:

$$R[x_1, \cdots, x_n] = (R[x_1, \cdots, x_{n-1}])[x_n].$$

An important technique of studying ring of polynomials is by viewing polynomials $R[x_1, \cdots, x_n]$ as functions $R^n \longrightarrow R$; but this should be done with extra care as two poly. might give us the same function. For instance distinct polynomials $x, x^2, \cdots \in (\mathbb{Z}/2\mathbb{Z})[x]$ are equal as functions $\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$.