1. Let $\alpha = (3, 4, 1)(5, 2, 1, 3)$ be a permutation (in cycle notation). Express α as a product of disjoint cycles. What are the order and the parity of α? Explain. Simplify α^{2019}.

$$\boxed{\alpha = (1\ 4)(2\ 3\ 5)}$$

Ruffini's theorem $\Rightarrow$ $|\alpha| = \mathrm{lcm}\left(|(1,4)|, |(2\ 3\ 5)|\right)$

$= \mathrm{lcm}(2,3) = \boxed{6}$

$p_1 = \text{Parity}\left((1,4)\right) = \text{odd}$

$p_2 = \text{Parity}\left((2\ 3\ 5)\right) = \text{even}$

$\text{Parity}(\alpha) = p_1 + p_2 = \text{odd} + \text{even} = \boxed{\text{odd}}$

$$\alpha^{2019} = (1\ 4)^{2019}(2\ 3\ 5)^{2019}$$

disjoint cycles commute!

$2019 \equiv \begin{cases} 1 \bmod 2 \\ 0 \bmod 3 \end{cases}$ $\quad \therefore \alpha^{2019} = \boxed{(1\ 4)}$

2. Prove that any group of prime order is cyclic.

Suppose $|G| = p$ - prime.

Let $x \in G$, $x \neq e$.

By Lagrange's theorem,

$|\langle x \rangle|$ divides $|G| = p$.

$\therefore$ $|\langle x \rangle| = 1$ or p

But since $x \neq e$ $|\langle x \rangle| = p$

$\therefore$ $\langle x \rangle = G$ ☺

3. Suppose $m, n, k \in \mathbf{N}$ with $\operatorname{lcm}(m,n) = k$. Define a group homomorphism $\varphi\colon \mathbf{Z} \to \mathbf{Z}_m \oplus \mathbf{Z}_n$ by $\varphi(i) = [i \bmod m, i \bmod n]$. Prove that $\ker\varphi = k\mathbf{Z}$. What does the first isomorphism theorem tell you about the image of φ? What can you say about $\mathbf{Z}_m \oplus \mathbf{Z}_n$ if $\gcd(m,n) = 1$?

Let $\pi_m : \mathbb{Z} \to \mathbb{Z}_m$

$\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ be the natural projection.

Universal property of product:

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl, bend right, "\pi_m"'] \arrow[d, "\exists!\,\phi"] \arrow[dr, bend left, "\pi_n"] & \\ \mathbb{Z}_m & \mathbb{Z}_m \oplus \mathbb{Z}_n \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & \mathbb{Z}_n \end{tikzcd}$$

$$\begin{aligned}
\ker\phi &= \{ i : \phi(i) = 0_{\mathbb{Z}_m \oplus \mathbb{Z}_n} \} \\
&= \{ i : [i \bmod m, i \bmod n] = [0,0] \} \\
&= \{ i : i \equiv 0 \bmod m \ \& \ i \equiv 0 \bmod n \} \\
&= \{ i : m \mid i \ \& \ n \mid i \} \quad \text{(all common multiples of } m,n\text{)} \\
&= \{ i : \operatorname{lcm}(m,n) \mid i \} \quad \text{(see midterm 1)} \\
&= \{ i : k \mid i \} = k\mathbb{Z}
\end{aligned}$$

1st isomorphism thm: $\dfrac{\mathbb{Z}}{\ker\phi} \cong \operatorname{image}(\varphi)$

$\therefore \operatorname{image}(\varphi) \cong \dfrac{\mathbb{Z}}{k\mathbb{Z}} = \boxed{\mathbb{Z}_k}$

If $\gcd(m,n) = 1$, $k = \operatorname{lcm}(m,n) = mn$

$$\underbrace{\operatorname{image}(\phi)}_{k = mn} \subseteq \underbrace{\mathbb{Z}_m \oplus \mathbb{Z}_n}_{mn}$$

$\therefore \operatorname{image}(\phi) = \mathbb{Z}_m \oplus \mathbb{Z}_n$ (ϕ is onto)

$$\boxed{\therefore \mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}}$$

4. Let F be a field. Show that the set of all polynomials in $F[x]$ with zero constant term is a maximal ideal. What is the quotient ring?

Let $I = \{ p \in F[x] : p(x) = a_0 + a_1 x + \cdots + a_n x^n, \text{ with } a_0 = 0 \}$

$(p(x) = a_1 x + \cdots + a_n x^n)$

$(p(x) = x(a_1 + \cdots + a_n x^{n-1})$

$\Rightarrow I = xF[x] \ (= \langle x \rangle)$

$a_0 = p(0)$

$\downarrow$

$= \{ p \in F[x] : p(0) = 0 \}$

Define $\varepsilon : F[x] \to F$ by $\varepsilon(p) = p(0)$

ε is a ring hom: $\varepsilon(p+q) = (p+q)(0) = p(0) + q(0)$
$= \varepsilon(p) + \varepsilon(q)$

$\varepsilon(p \cdot q) = (p \cdot q)(0) = p(0) \cdot q(0)$
$= \varepsilon(p) \cdot \varepsilon(q)$

$\ker \varepsilon = I$. Also ε is onto:
Given $a \in F$, $\varepsilon(a) = a(0) = a$ ☺

↑const. polynomial

1st isomorphism theorem: $\dfrac{F[x]}{\ker \varepsilon} \cong \operatorname{image}(\varepsilon) = F$

Since F is a field, $\ker \varepsilon$ is a max. ideal. ☺

<u>Direct proof</u> $t \cdot 0 = 0$ so $0 \in I$

If $p, q \in I$, $p = xp'$, $q = xq'$ for some p' & q'

so $p - q = xp' - xq' = x(p' - q') \in I$

$\therefore$ I is a subgroup of $F[x]$. If $p \in I$, $q \in F[x]$

$p = xp'$ for some p' so $pq = xp'q \in I$

$\therefore$ I is an ideal

Suppose J is an ideal of $F[x]$, $I \subsetneq J$.

Let $p \in J \setminus I$, $p(x) = a_0 + a_1 x + \dots + a_n x^n$

Since $p \notin I$, $a_0 \neq 0$

$$a_0 = \underbrace{p(x)}_{\in J} \underbrace{- a_1 x - \dots - a_n x^n}_{\in I \subseteq J} \in J$$

Since a_0 is a unit, $J = F[x]$ ☺

Given a const. $a \longleftrightarrow a + I$

$$a_0 + \underbrace{a_1 x + \dots + a_n x^n}_{\in I} + I$$

$$= a_0 + I$$

$\therefore$ We have a 1-1 corresp. between $\dfrac{F[x]}{I}$ & F

(easy to show it's an iso.)

Sp 2008 Final # 6

$$A = \{ [i,j] \in \mathbb{Z} \oplus \mathbb{Z} : i \text{ is even} \}$$

(i) $[0,0] \in A$

(ii) if $[x,y]$ & $[u,v] \in A$, then $x = 2x'$, $u = 2u'$ for some x', u'.

Then $[x,y] - [u,v] = [x-u, y-v] = [2x' - 2u', y-v]$
$= [2(x'-u'), y-v] \in A$

$\therefore$ A is a subgroup of $\mathbb{Z} \oplus \mathbb{Z}$.

(iii) Given $[x,y] \in A$, $[u,v] \in \mathbb{Z} \oplus \mathbb{Z}$

$x = 2x'$ for some x'

$[x,y][u,v] = [xu, yv] = [2x'u, yv] \in A$

$\therefore$ A is an ideal.

Claim A is maximal. Suppose $J \subseteq \mathbb{Z} \oplus \mathbb{Z}$ is an ideal, $A \subsetneq J$.

Let $[u,v] \in J \setminus A$. Since $[u,v] \notin A$, u is odd

So $u = 2u' + 1$ some u'

$$[u,v] = [2u'+1, v] = [2u', v] + [1, v]$$

$$[1,1] = [1,1] - [1,v] + [1,v] = \underbrace{[1,1] - [1,v]}_{\substack{[0,1-v] \\ \in A \subseteq J}} + \underbrace{[u,v]}_{\in J} - \underbrace{[2u',v]}_{\in A \subseteq J}$$

$\therefore [1,1] \in J$ $\therefore J = \mathbb{Z} \oplus \mathbb{Z}$ ☺

Slick proof: define $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}_2 \oplus \mathbb{Z}$

by $\phi([i, j]) = [i \bmod 2, 0]$

(easy to show ϕ is a hom)

$\ker \phi = \{ [i, j] : \phi[i, j] = [0 \bmod 2, 0] \}$

$= \{ [i, j] : i \text{ is even} \} = A$

$\therefore$ $\ker \phi$ is an ideal.

1st iso thm: $\dfrac{\mathbb{Z} \oplus \mathbb{Z}}{A} \cong \text{image } \phi = \mathbb{Z}_2 \oplus \{0\} \cong \mathbb{Z}_2$

Since $\mathbb{Z}_2$ is a field, A is maximal.

(8) prove $x^p + x + 1$ and $2x + 1$ determine the same function $\mathbb{Z}_p \to \mathbb{Z}_p$

By little Fermat's theorem $x^p \equiv x \bmod p$

So $x^p + x + 1 = x + x + 1 = 2x + 1$ ☺

Sp 2009 Final #5 A Finite integral domain is a field.

Suppose R is a finite integral domain.

Pf 1 Let $a \in R, a \neq 0$. By the pigeonhole principle

$\{0, a, a^2, \dots\}$ cannot be all distinct.

$\therefore \exists\, i < j \qquad a^i = a^j \Rightarrow \cancel{a^i} = \cancel{a^i}\, a^{j-i}$

$a^{j-i} = 1$

$a \cdot a^{j-i-1} = 1$

$\therefore$ a is a unit

$\therefore$ R is a field ☺

If $ax = ay$ and $a \neq 0$
then $x = y$

Pf: $ax = ay \Rightarrow ax - ay = 0$

$\Rightarrow a(x-y) = 0$

Since R is a domain
and $a \neq 0$ $x - y = 0$ ☺

Pf 2 Let $a \in R$, $a \neq 0$

Define a function $f: R \to R$ by $f(x) = ax$

Then f is 1-1: If $f(x) = f(y)$, $\cancel{a}x = \cancel{a}y$ ☺
(domain)

Since R is finite, f is onto.

$\therefore \exists\, a' \in R \quad \underbrace{f(a')}_{aa'} = 1$

$\therefore$ a is a unit

$\therefore$ R is a field.

8 $A = \{ p \in \mathbb{Z}_m[x] : p(0) = 0 \}$

Let $p(x) = a_0 + a_1 x + \dots + a_n x^n$

Then $p(0) = a_0$

So $p(0) = 0 \iff p(x) = a_1 x + \dots + a_n x^n$

$= x(a_1 + \dots + a_n x^{n-1})$

$\iff p(x) \in x\mathbb{Z}_m[x] = \langle x \rangle$ ☺

Define $\varepsilon : \mathbb{Z}_m[x] \to \mathbb{Z}_m$ by $\varepsilon(p) = p(0)$

then ε is a hom (easy), $\ker \varepsilon = A$,

ε is clearly onto.

1^{st} iso thm: $\dfrac{\mathbb{Z}_m[x]}{A} \cong \mathbb{Z}_m$

A is prime $\iff$ m is prime (so $\mathbb{Z}_m$ is a domain)

A is max $\iff$ m is prime (so $\mathbb{Z}_m$ is a field)

If m is prime, A is both prime & max.

If m is not prime, A is neither prime nor max.