1. Sketch the subgroup lattice for $\mathbf{Z}_{20}$. For each subgroup, list all the elements and indicate all possible generators of the subgroup.

Positive divisors of 20 : 1, 2, 5, 4, 10, 20

Possible generators underlined.

Recall $\langle k_1 \rangle = \langle k_2 \rangle \iff \gcd(k_1, m) = \gcd(k_2, m)$:)

$\langle 1 \rangle = \mathbb{Z}_{20} = \{0, \underline{1}, 2, \underline{3}, 4, 5, 6, \underline{7}, 8, \underline{9}, 10, \underline{11}, 12, \underline{13}, 14, 15, 16, \underline{17}, 18, \underline{19}\}$

$\langle 2 \rangle = 2\mathbb{Z}_{20} = \{0, \underline{2}, 4, \underline{6}, 8, \underline{10}, 12, \underline{14}, 16, \underline{18}\}$

$\langle 5 \rangle = 5\mathbb{Z}_{20} = \{0, \underline{5}, 10, \underline{15}\}$

$\langle 4 \rangle = 4\mathbb{Z}_{20} = \{0, \underline{4}, \underline{8}, \underline{12}, \underline{16}\}$

$\langle 10 \rangle = 10\mathbb{Z}_{20} = \{0, \underline{10}\}$

$\langle 0 \rangle = 0\mathbb{Z}_{20} = \{0\}$

2. Suppose $\alpha = (4,3,7,8,9)(1,3,7,5,2)(2,7,6)$ is a permutation in cycle notation.

(a) Express α as a product of disjoint cycles.

(b) Find the order of α. Explain.

(c) Find the parity of α. Explain.

(d) Simplify α^{659}

(a) $\alpha =$ [[1,7,6],[2,5],[3,8,9,4]]

(b) By Ruffini's theorem $|\alpha| = \text{lcm}(\underbrace{3,2,4}_{\text{orders of cycles}}) = 12$

(lengths)

(c) Discriminant = sum of $\underbrace{\text{sizes}}_{\text{lengths} - 1}$ of cycles $= 2+1+3 = 6$, so α is even

(d) lemma: If G is a group, $a \in G$, $|a| = m$, and $n \equiv r \bmod m$, then $a^n = a^r$

Pf: Since $\exists q \in \mathbb{Z}$ $n - r = qm$, $n = r + qm$, so

$a^n = a^{r+qm} = (a^m)^q \cdot a^r = e^q a^r = a^r$ ☺

Since disjoint cycles commute $\alpha^{659} = (1,7,6)^{659}(2,5)^{659}(3,8,9,4)^{659}$.

Since $659 = 3 \bmod 4$, $2 \bmod 3$, $1 \bmod 2$

$\alpha^{659} = (1,7,6)^2(2,5)(3,8,9,4)^3 = (1,7,6)^{-1}(2,5)(3,8,9,4)^{-1}$

= [[1,6,7],[2,5],[3,4,9,8]]

3. (a) How many group homomorphisms are there from $\mathbf{Z}$ to $\mathbf{Z}_9 \times \mathbf{Z}_{25}$? Explain.
(b) How many of these are surjective? Explain.
(c) How many of these are injective? Explain.

(a) If $f: \mathbb{Z} \to \mathbb{Z}_9 \times \mathbb{Z}_{25}$ is a group hom., $f(k) = f(k \cdot 1) = k f(1)$

so f is uniquely determined by $f(1)$,

so $|\mathrm{Hom}[\mathbb{Z}, \mathbb{Z}_9 \times \mathbb{Z}_{25}]| = 9 \cdot 25 = 225$

(b) For f to be surjective $f(1)$ must be a generator of $\mathbb{Z}_9 \times \mathbb{Z}_{25}$

so a unit in $\mathbb{Z}_9 \times \mathbb{Z}_{25}$, so $f(1) = [i, j]$ where $i \in U(9)$, $j \in U(25)$

Euler totient: $\varphi(9) = 9 - 3 = 6$, $\phi(25) = 25 - 5 = 20$

So $6 \cdot 20 = 120$ surjective homs.

(c) By the pigeon hole principle, none are injective,

because $\mathbb{Z}$ is infinite and $\mathbb{Z}_9 \times \mathbb{Z}_{25}$ is finite.

4. Suppose R is a finite commutative ring with unity and $a \in R, a \neq 0$. Show that a is either a zero divisor or a unit (but not both).

(i) Exclusivity : In a c.r.u there are no zero divisors among units

If x is a unit and $ax = 0$, then $a = a \cdot 1 = a x x^{-1} = 0 \cdot x^{-1} = 0$

[thm 12.1.1 p.247]

(ii) Suppose R is a finite c.r.u.

Let $z \in R$ be a nonunit and define

$f : R \to R$ by $f(x) = zx$. Since z is not a unit

$1 \notin$ image f, so f is not onto.

Since R is finite, f is not 1-1.

so $\exists\, x_1 \neq x_2 \quad zx_1 = zx_2$,

so $z(x_1 - x_2) = 0$, so z is a zero divisor.

Alt. proof of (ii): Let $a \in R$, $a \neq 0$ and is not a zero div.

Then $\forall n \geq 1 \quad a^n \neq 0$ and is not a zero divisor.

Pf. by induction on n: If $n = 1$, $a^n = a$ ☺

For $n > 1 \quad a^n = a \cdot a^{n-1} \neq 0$. If $a^n b = 0$, $a a^{n-1} b = 0$

so $a^{n-1} b = 0$, so $b = 0$ ☺

Since R is finite, by the pigeonhole principle

$a, a^2, \ldots$ are not all distinct, so $\exists\, j > i \quad a^j = a^i$,

so $a^i(a^{j-i} - 1) = 0$, so $a^{j-i} = 1$, so $a a^{j-i-1} = 1$, so $a \in U(R)$ ☺

5. Let A be the set of all polynomials in $\mathbf{Z}[x]$, whose coefficients are divisible by 3.

(a) Show the A is an ideal of $\mathbf{Z}[x]$

(b) Is A a maximal ideal of $\mathbf{Z}[x]$? Explain.

(a) $0 \in A$:)

If $p, q \in A$ $p(x) = a_0 + \dots a_n x^n$, $q(x) = b_0 + \dots b_n x^n$, then

$\forall i \ \exists a_i', b_i' \in \mathbb{Z}$ $a_i = 3a_i'$ $b_i = 3b_i'$, so

$(p-q)(x) = a_0 - b_0 + \dots (a_n - b_n)x^n = 3\left(a_0' - b_0' + \dots (a_n' - b_n')x^n\right)$, so $p - q \in A$

Absorption: If $p \in A$, $s \in \mathbb{Z}[x]$, since $3 \mid p$, $3 \mid ps$, so $ps \in A$

(b) Let $B = \{ p \in \mathbb{Z}[x] : 3 \mid p(0) \}$. Then B is an ideal of $\mathbb{Z}[x]$.

Pf: $3 \mid 0$. If $p, q \in B$, $s \in \mathbb{Z}[x]$, $(p-q)(0) = p(0) - q(0)$, so $p - q \in B$.

Also $(pr)(0) = p(0)r(0) = 0 \cdot r(0) = 0$, so $pr \in B$ (and similarly $rp \in B$)

Also $A \subseteq B$: If $p \in A$, $p = a_0 + \dots a_n x^n$, then $3 \mid a_0 = p(0)$:)

$A \neq B$: $3 + x \in B \setminus A$ $\qquad$ $B \neq \mathbb{Z}[x]$: $1 \notin B$

Fancy proof: $a_0 + \dots a_n x^n \longmapsto a_0 \bmod 3 + \dots a_n \bmod 3\, x^n$ gives a

surjective ring isomorphism $\mathbb{Z}[x] \to \mathbb{Z}_3[x]$ with kernel $= (3\mathbb{Z})[x] = A$.

By the 1st isomorphism theorem $\mathbb{Z}[x]/A \cong \mathbb{Z}_3[x]$,

which is not a field (x is not a unit in $\mathbb{Z}_3[x]$) :)