# A First Course in Abstract Algebra

Brendan Matthews

February 5, 2026

## Chapter -2: What is this stuff used for

| Topic | It is used | What Part | Is it Physics |
|---|---|---|---|
| Combinatorics | yes | Group Actions: Burnside | no |
| Statistics | sparsely | Renormalisation group, Haar Measure | yes, dunno |
| Statistics | sparsely | Galois Fields: Fractional factorial design | no |
| Math | | | |
| Math | | | |
| Math | | | |
| Math | | | |

## Chapter -1

Group tables are dumb and playing sudoku doesn't guarantee associativity.

| $\circ$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 4 | 0 | 2 | 3 |
| 2 | 2 | 3 | 4 | 1 | 0 |
| 3 | 3 | 0 | 1 | 4 | 2 |
| 4 | 4 | 2 | 3 | 0 | 1 |

$D_3 = S_3$ but $D_n \neq S_n, \quad n \geq 4.$

# Moonshine Theory

A relation b/w sets $A, B$ is $R \subset A \times B$ -
A relation on $A$ is $R \subset A \times A$.

ex. The graph of a function is the subset

$$\{(x, f(x)) : x \in \mathrm{dom}(f)\} \subset \mathrm{dom}(f) \times \mathrm{codom}(f).$$

The graph of a function $f: \mathbb{R} \to \mathbb{R}$ is a relation on $\mathbb{R}$.

A function $\phi: X \to Y$ is a relation b/w $X$ and $Y$ such that for each $x \in X$, $\exists!\ y \in Y$ so that $(x, y) \in \phi \subset X \times Y$ or equivalently, $\phi(x) = y$.

The range of $\phi$ is $\phi(X) = \{\phi(x) : x \in X\}$.

ex. $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is a map from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$.

A partition of $S$ is a collection of nonempty disjoint subsets with union $S$. These define equivalence relations on $S$

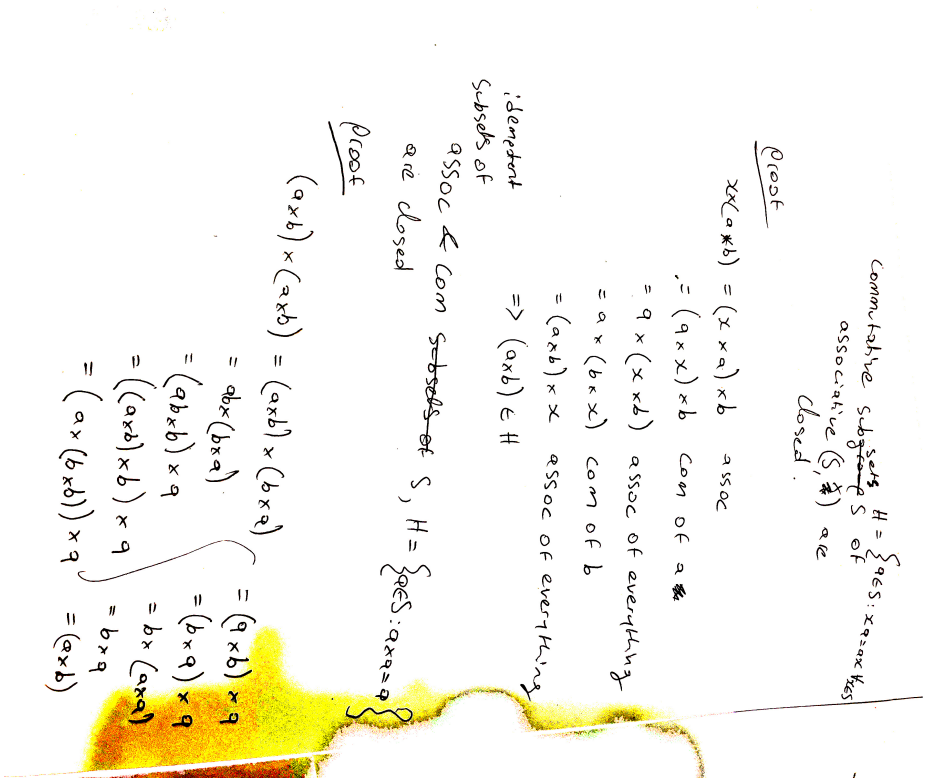
$x R_{eq} x$, $x R_{eq} y$ and $y R_{eq} z \Rightarrow x R_{eq} z$,

$x R_{eq} y \Rightarrow y R_{eq} x$.

# 1

A binary operation is a map $* : S \times S \to S$ and a subset $H$ of $S$ is closed under $*$ if the obvious thing happens. We say that $*$ is induced on $H$. There are $n^{n^2}$ binary ops on a set of size $n$ and $n^{\sum_n i} = n^{\frac{n(n+1)}{2}}$ commutative ones. The latter is because the number of elements of $S \times S$ that aren't predetermined by the condition is $n + (n-1) + \ldots + 1$ and schoolboy Gauss does the rest. Note that for finite $A, B$, number of maps from $A$ to $B$ is $|B|^{|A|}$.

Not every 2 element commuter is associative. Consider $aa = b,\ ab = b,\ ba = b,\ bb = a$ and $a\,(ab) = ab = b,\ (aa)\,b = bb = a$. 35 is rubbish.



Two binary algebraic structures $(R, *)\,, (S, +)$ are isomorphic, $R \simeq S$, if for each $x, y \in R$ with $x * y = z$, we have corresponding $x', y', z' \in S$ so that $x' + y' = z'$. That is, there exists a bijection $\phi : R \to S$ such that for all $x, y \in R$ with $x * y = z$,

$$\phi\,(x * y) = \phi\,(x) + \phi\,(y) = x' + y' = z' = \phi\,(z)\,.$$

Each point in $S$ is mapped to by exactly one point in $R$. Isomorphism is an equivalence relation.

*Proof.* $S \simeq S$ by identity map. If $R \simeq S$, then there exists $\phi : R \to S$, bijective and a homomorphism. So the inverse exists. The inverse is a homomorphism by injectivity of $\phi$:

$$\phi\left(\phi^{-1}(s_1) * \phi^{-1}(s_2)\right) \underset{\text{H prop of } \phi}{=} \phi\left(\phi^{-1}(s_1)\right) + \phi\left(\phi^{-1}(s_2)\right) = s_1 + s_2 = \phi\left(\phi^{-1}(s_1 + s_2)\right).$$

Transitivity is easy just compose the isos. □

## Theorem

Suppose there is an onto homomorphism $\phi : (R, +) \to (S, *)$ and an identity $e \in R$. Then $\phi(e) \in S$ is an identity.

*Proof.* Easy. □

Note that while the identity is always unique in $S$, we require that $\phi$ be an isomorphism for the preimage of the identity to be uniquely the identity of $R$.

## Theorem

Suppose $S$ is a **group** and $R, S$ have identities $e_R, e_S$. If there is a homomorphism $\phi : (R, +) \to (S, *)$, then $\phi(e_R) = e_S$.

*Proof.*

$$\phi(e_R) = \phi(e_R + e_R) = \phi(e_R) * \phi(e_R)$$

Apply inverse of $\phi(e_R)$. □

## Non Isomorphism Example

The function $\phi : \left(M_2(\mathbb{R}), \times\right) \to (\mathbb{R}, \times), \quad \phi(A) = \det(A)$ is not an isomorphism (in fact, no such isomorphism exists).

*Proof.* It is a homomorphism, $\det(AB) = \det(A)\det(B)$. But it isn't injective because matrix multiplication isn't commutative. Take

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

then

$$AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad BA = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

so that

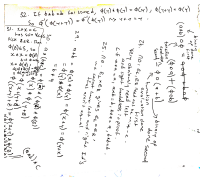
$$\phi(AB) = \phi(BA) = 1 \text{ but } AB \neq BA.$$

□

Another example that fails injectivity is the map under addition from functions with derivatives to their derivatives. Being a binary operation (or even a function at all) can fail with integrals even if everything else works.

### Disproof using stuff that's preserved under isomorphisms

We know the identity is preserved. So $\phi(f)(x) = xf(x)$ is not an isomorphism across $F = \{f : \mathbb{R} \to \mathbb{R} \,|\, f \text{ is smooth}\}$ under multiplication, $\phi(\mathbf{1})(2) = 2 \neq 1$, so $\phi(\mathbf{1}) \neq \mathbf{1}$, where $\mathbf{1} : \mathbb{R} \to \mathbb{R}$ is given by $\mathbf{1}(x) = 1$.



## Groups

Here are some:

$$(U, *) \text{ with } U = \{z \in \mathbb{C} : |z| = 1\}, \quad (U_n, *) \text{ with } U_n = \{z \in \mathbb{C} : z^n = 1\}$$

The invertible $n$ by $n$ matrices and the invertible linear maps on $\mathbb{R}^n$:

$$\mathrm{GL}(n, \mathbb{R}) \simeq \mathrm{GL}(\mathbb{R}^n)$$

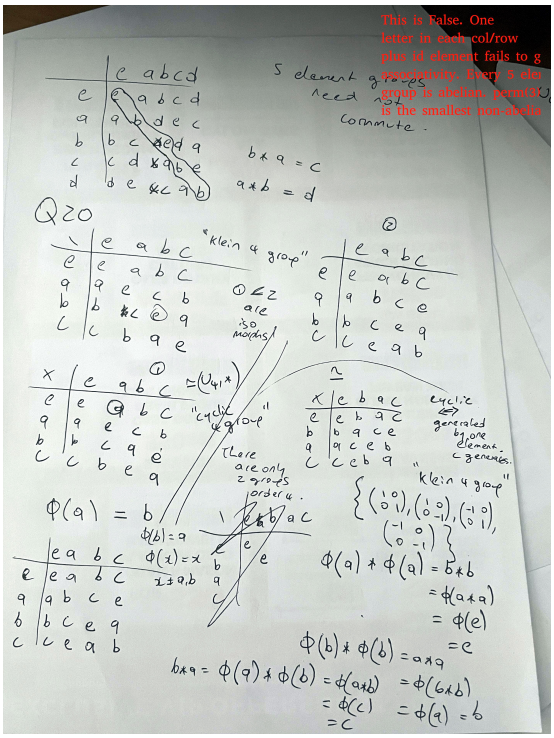
To get an isomorphism, map an invertible linear function $T : \mathbb{R}^n \to \mathbb{R}^n$ to a matrix using its action on the standard basis. Left inverses and identities plus associative is enough to define a group. Identity is a right identity:

$$\begin{aligned} x + e_L &= e_L + (x + e_L) \\ &= (x_{LL} + x_L) + \big(x + (x_L + x)\big) \\ &= x_{LL} + (x_L + x) + (x_L + x) \\ &= x_{LL} + e_L + (x_L + x) \\ &= (x_{LL} + x_L) + x \\ &= e_L + x \\ &= x. \end{aligned}$$

Left inverses are right inverses also,

$$x + x_L = e_L + x + x_L = (x_{LL} + x_L) + x + x_L = x_{LL} + e_L + x_L = x_{LL} + x_L = e_L.$$

It's easy to do the same argument with $\phi(e^{\pi}) = a > 0$. Bit weirder for $(U, *) \ncong \left(\mathbb{R}^*, *\right), a^2 = a * a = \phi(e^{\pi}) * \phi(e^{\pi}) = \phi\left(e^{2\pi}\right) = 1$ but $0 \notin \mathbb{R}^*$ and $a \neq 1$ since $\phi$ injective and $\phi\left(e^0\right) = 1$.

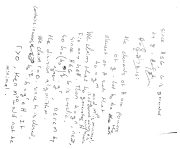



# Subgroups

Subgroups are closed, contain identity and inverses. An element $a$ generates $G$ if the cyclic subgroup $\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = G$. We say that $G$ is cyclic if there is some element that generates it. So obviously $\langle a \rangle$ is a cyclic group (its always a group). Any group with no proper nontrivial subgroups is generated by every non identity element (except the trivial group (or not, vacuous??)), so is cyclic.

# Cyclic Groups

Subgroup of a cyclic group is cyclic.



Pick any subgroup $H$ of the integers under addition. Then $H$ is cyclic, so some $h$ generates $H$. So $h \in \mathbb{Z}$ and we must have $H = h\,\mathbb{Z}$.

The following is unrelated. A finicky but easy enough proof tells ya that any cyclic group is isomorphic to the integers under addition or the integers under modular addition. The prior fact about subgroups of $\mathbb{Z}$ characterises subgroups of infinite cyclic groups, since their parents are isomorphic to $\mathbb{Z}$.

## The hard bit: Cyclic Subgroups

### Defn

The greatest common divisor of $m, n$ is the generator $d$ of the group

$$\{rm + sn : r, s \in \mathbb{Z}\}$$

### Theorem

Let $G = \langle\, a \,\rangle$ be a cyclic group of order $n$. Then the order of the subgroup generated by $a^m$ is $n/d$. Further, $\langle\, a^m \,\rangle = \langle\, a^p \,\rangle$ iff $\gcd(m, n) = \gcd(p, n)$.

*Proof.* Go read the first bit. The iff statement is badly explained. What they are saying is that $\left\{m \in \mathbb{Z}_n : \gcd(m, n) = d\right\} \subset \langle\, d \,\rangle$ since $d|m \implies m = kd = d^k \in \langle\, d \,\rangle$. Any subgroup with $n/d$ elements contains all elements $a^p$ of $G$ such that $\gcd(p, n) = d$. In the case of $\mathbb{Z}_n$, this is just integers $p$ with $\gcd(p, n) = d$. Then $\langle\, a^m \,\rangle$ contains $a^p$ and $\langle\, a^p \,\rangle \subset \langle\, a^m \,\rangle$ and similarly $\langle\, a^m \,\rangle \subset \langle\, a^p \,\rangle$ so $\langle\, a^m \,\rangle = \langle\, a^p \,\rangle$. That is to say, if the gcd's are the same then the subgroups are the same. If the subgroups are the same, they have the same number of elements, $n/d_1 = n/d_2 \implies d_1 = d_2$. □

### Corollary

For each divisor $d$ of $n$, where $n$ is the order of a cyclic group $G$, there is at most one subgroup of $G$.

### Corollary

Given any generator $a$ of $G$ of order $n$, the generators are $a^p$ such that $p$ is coprime with $n$.

**Defn**

The least common divisor of $m, n$ is the generator of the group

$$\left\{k \in \mathbb{Z} : m|k,\ n|k\right\}.$$

The smallest possible LCM is $mn$ because if $k|m$ then $mn = (ak)\, n = (an)\, k$ so $k|mn$. If $m, n$ are coprime then $m|nk$ implies $m|k$. In particular, if $n|k$ then $k = qn$ so $m|k$ implies $m|q$ so that $k = qn = (am)\, n = a\,(mn)$, i.e. $mn|k$.

**Theorem**

For positive integers $m, n$

$$\gcd(m, n) * \operatorname{lcm}(m, n) = mn.$$

*Proof.* Let $\operatorname{lcm}(m, n) = am = bn$. Then

$$\frac{mn}{\operatorname{lcm}(m, n)} * a = n, \quad \frac{mn}{\operatorname{lcm}(m, n)} * b = m$$

so it is a divisor of $a, b$, proving $\frac{mn}{\gcd(m,n)} \leq \operatorname{lcm}(m, n)$. Since $\frac{mn}{\gcd(m,n)}$ is a multiple of both $m$ and $n$, $\frac{mn}{\gcd(m,n)} \geq \operatorname{lcm}(m, n)$. □

**Theorem**

Abelian groups with cyclic subgroups $H, K$ of coprime orders $r$ and $s$ have a cyclic subgroup of order $rs$. More generally, there is a subgroup of order $\operatorname{lcm}(r, s)$.

*Proof.* We know that $H \cap K$ is a cyclic subgroup. So it must be generated by $x = h^p = k^q$. Let $m = |\langle x \rangle|$. Then $m = r/\gcd(p, r) = s/\gcd(q, s)$ so $m|r$ and $m|s$. Then $m|\gcd(r, s) = 1$ and $m = 1$. So $H \cap K$ is the trivial group. Now consider the group $Z = \{xy : x \in H, y \in K\}$ (it is a group since the whole group is Abelian). Since $H, K$ are finite cyclic groups, there generators $h, k$ of $H, K$. We define a bijection $f : \mathbb{Z}_r \times \mathbb{Z}_s \to Z$, $f(a, b) = h^a k^b$. if $f(a, b) = f(c, d)$, then $h^{a-b} = k^{d-c} = e$ since $H \cap K = \{e\}$. So $(a, b) = (c, d)$. Fix $z \in Z$. Then $z = xy = h^a k^b$ where $0 \leq a, b < r, s$ so $f(a, b) = z$. So $f$ is a bijection as asserted. There are $rs$ elements in $\mathbb{Z}_r \times \mathbb{Z}_s$ so the cardinality of $Z$ is $rs$. We claim that $Z$ is cyclic when $r, s$ are coprime and $gh$ generates $Z$. Since $r, s$ are coprime there exist integers $m_1, m_2$ so that $1 = m_1 r + m_2 s$. Fix $z \in Z$ and write $z = h^a k^b$. Then we have

$$\begin{aligned}
(hk)^{bm_1 r + am_2 s} &= h^{bm_1 r + am_2 s} * k^{bm_1 r + am_2 s} \\
&= h^{am_2 s} * k^{bm_1 r} \\
&= h^{a(1 - m_1 r)} * k^{b(1 - m_2 s)} \\
&= h^a * k^b \\
&= z.
\end{aligned}$$

N.B. The Chinese remainder theorem applies here. □

*Proof.* Easier proof. Consider $\langle\, hk \,\rangle$. This group is cyclic since it is generated by $hk$. The order is no more than $rs$, since $(hk)^{rs} = e^s * e^r = e$. Suppose $p < rs$ was the order of $\langle\, hk \,\rangle$. Then $h^p = k^{-p}$ so that $h^p \in H \cap K$. So $|\langle\, h^p \,\rangle| = d | r, s$ which implies $d = 1$, $\langle\, h^p \,\rangle = \{e\}$. It follows that $h^p = k^p = e$, so $r, s | p$ (because they are the orders of $H, K$). Then $p = ar$, so $s|a$ and $p = brs$, $rs|p$ which gives a contradiction, $p \geq rs$. □

**Lemma for General Statement**

Given $r, s$ we can construct coprime $a, b$ so that $a|r$, $b|s$ and $ab = \operatorname{lcm}(r, s)$.

*Proof.* Write $\operatorname{lcm}(r, s) = d * \frac{r}{d} * \frac{s}{d}$ and

$$d = {p_1}^{a_1} \dots {p_n}^{a_n} * {q_1}^{b_1} \dots {q_m}^{b_m}$$

where $p_i \not| r/d$ and $q_i | r/d$. Then $q_i \not| s/d$. Consider

$$a = {p_1}^{a_1} \dots {p_n}^{a_n} * r/d, \quad b = {q_1}^{b_1} \dots {q_m}^{b_m} * s/d.$$

N.B. if $ab|m$ then $a|m$, $b|m$ contrapositive is if neither divide $m$ then their product doesn't. □

**Proof for General Statement**

By the lemma, we can construct coprime divisors $a, b$ of $r, s$ with $ab = \operatorname{lcm}(r, s)$ so that for $r = a\,\delta_1$, $s = b\,\delta_2$ and $\langle\, h^{\delta_1} \,\rangle \leq \langle\, h \,\rangle$, $\langle\, k^{\delta_2} \,\rangle \leq \langle\, k \,\rangle$ we have

$$|\langle\, h^{\delta_1} \,\rangle| = r/\gcd(\delta_1, r) = r/\,\delta_1 = a, \quad |\langle\, k^{\delta_2} \,\rangle| = s/\gcd(\delta_2, s) = s/\,\delta_2 = b.$$

**Example**

There is a generator of $\mathbb{Z}_{36}$ because it has subgroups $\langle\, 2 \,\rangle$, $\langle\, 3 \,\rangle$ with 12 and 18 elements. We write $12 = 6 * 2$ and $18 = 6 * 3$, then separate factors to get $6 = 3 * 2$, $a = 2 * 12/6 = 4$, $b = 3 * 18/6 = 9$ so that $12 = 4 * 3$ and $18 = 9 * 2$. We take these new factors $3, 2$ and raise existing generators to them. We then have $\langle\, 3^3 \,\rangle = \langle\, 9 \,\rangle$ of order 4 and $\langle\, 2^2 \,\rangle = \langle\, 4 \,\rangle$ of order 9. So we can generate $\mathbb{Z}_{36}$ with $9 + 4 = 13$.

## Cayleigh Digraphs

A group has a correspondence with a digraph with the following properties:

If ya start at some point and get to some other point in two ways then the two ways will lead to the same destination from any point

.

Theres one of each generator arc to and from each point.

.

Some utter nonsense about only one arc going from a to b.

.

There exists an arc from a to b.

When a generator is an involution we use undirected graph edges. An obvious implication of this is that in a group, if $a, b, \ldots, x, y$ are involutions then $(ab \ldots xy)^{-1} = y^{-1}x^{-1} \ldots b^{-1}a^{-1} = yx \ldots ba$. Pick a vertex $V$. If all pairs of arcs from $V$ go to the same vertex regardless of the order they are chosen then the group is commutative.

# 2 Orbits, Lagrange all that Jazz

## 2.1 Perm Groups

A permutation is a bijection of a set with itself. If $A, B$ are finite sets of the same order, there is a bijection $f$ and the permutation groups $S_A$ and $S_B$ are isomorphic. The isomorphism is $\phi \circ \sigma = f \circ \sigma \circ f^{-1}$. Its a homo because $\phi \circ (\sigma \circ \tau) = f \circ (\sigma \circ \tau) \circ f^{-1} = f \circ \sigma \circ \left(f^{-1} \circ f\right) \circ \tau \circ f^{-1} = (\phi \circ \sigma) \circ (\phi \circ \tau)$.

### 2.1.1 Cayleighs Theorem

Every group is isomorphic to a subgroup of the group of permutations on the set. Its not hard just finicky definitions and pedantry in the one to one but only onto the image stuff. Just notice that multiplication by an element permutes the elements in a group. This allows a well defined function (not an iso) $\phi : G \to S_G$. The inverse of left multiplication by an element is just left multiplication by the inverse of that element. Multiplication by the identity gives the identity permutation aka the identity map. We have closure, permutations of permutations are permutations. So $\phi(G)$ is a subgroup of $S_G$. The cancellation law says $\phi$ is injective. So $G$ is isomorphic to the subgroup $\phi(G)$ of $S_G$ (weird statement but yeah).

N.B. When computing the order of a permutation, check more than one element...

N.B. Right regular representations use the inverse element not the element itself.

## 2.2 Orbits, Cycles, Parity of perms, Alternating Group

Orbits are the equivalence classes of elements of a group under a permutation. Cycles are permutations with at most one orbit with order greater than 1. Transpositions swap two elements and fix the rest (cycles of order 2). Theorem: Permutations are composed of either an odd or an even number of these. The alternating group is the subgroup of $A_n$ of $S_n$ made up of the even permutations. The odd permutations don't form a subgroup because the identity permutation is even.

Claim: if $H \leq S_n$, $n \geq 2$ then all or half $\delta \in H$ are even.

If they all are, done.

If not, Let $\delta \in H$ be odd.

Let $\phi$ : evens in $H$ $\longrightarrow$ odds in $H$ be given by

$\phi(\text{even}) = \delta \cdot \text{even} \in \text{odds}$.

Claim $\phi$ is injective

If $\delta \cdot \text{even}_1 = \delta \cdot \text{even}_2$ the cancellation law in $S_n$ and $H$ says that $\text{even}_1 = \text{even}_2$.

Claim $\phi$ is onto.

Well $\delta^{-1} \in H$, cause $H \leq S_n$.

Now $\delta^{-1}$ is odd (prove it) so for any odd $\in$ odds, $\delta^{-1} \cdot \text{odd}$ is even and ($\delta\delta^{-1} = Id = \text{even}$ $\therefore$ same parity)

$\phi(\delta^{-1} \cdot \text{odd}) = \delta\delta^{-1} \cdot \text{odd} = \text{odd}$.

Claim: Let $\sigma$ be a cycle of length $n$. $\sigma^r$ is a cycle iff $\gcd(n,r) = 1$.

Write $\sigma^r = (1, 1+r, \ldots, 1+mr)$ (mod $n$). The last element $1+mr$ is chosen so that $m$ is minimal and $1+mr \equiv 1 \bmod n \iff mr \equiv 0 \bmod n$. Since $\sigma^r$ permutes the same elements as $\sigma$, we need that the largest orbit of $\sigma^r$ has length $n$ for $\sigma^r$ to be a cycle. Since $mr$ is a multiple of both $n$ and $r$, this happens iff $\operatorname{lcm}(n,r) = nr \iff m = n$.

## 2.3 Cosets, Lagrange's Theorem

You oughta know why a group of prime order is cyclic. Lagrange's theorem says nothin about infinite order groups. $(\mathbb{R},+) \simeq \left(\mathbb{R}^+,\times\right)$ has no nontrivial finite subgroups, because any $x \neq e$ generates an infinite order subgroup. But $(\mathbb{R},\times)$ has the subgroup $\{-1,1\}$.

**Definition**

The index of a subgroup $H \leq G$ is the number of left cosets, $(G:H)$.

**Lemma**

(Left) cosets of a subgroup are unique.

*Proof.* Let $A$ and $B$ be families of left cosets of $H \leq G$, indexed by $a_\lambda, b_\delta$. Pick any $a_\lambda H \in A$. Since $B$ covers $G$, we have $a_\lambda \in b_\delta H$ for some $b_\delta H \in B$, so we can write $a_\lambda = b_\delta h$ for some $h \in H$. We claim that $a_\lambda H = b_\delta H$, which implies that $a_\lambda H \in B$ and furthermore $A \subset B$. Fix $x \in a_\lambda H$. Then $x = a_\lambda h_x = b_\delta h h_x \in b_\delta H$ since $H$ is closed, so $a_\lambda H \subset b_\delta H$. Fix $x \in b_\delta H$. Then $x = b_\delta h_\delta = a_\lambda h^{-1} h_\delta \in a_\lambda H$, so $a_\lambda H = b_\delta H$. We have shown that $A \subset B$ and a similar argument shows that $B \subset A$, so $A = B$. □

**Theorem**

Let $G, H, K$ be FINITE groups with $K \leq H \leq G$. Then $(G:K) = (G:H)\,(H:K)$.

*Proof.* Cosets are equivalence classes and $G$ is finite, so write $G = \bigcup_{i=1}^{m} a_i H$ and $H = \bigcup_{j=1}^{n} b_j K$. Fix $g \in G$. Then write $g = a_i h$ and $h = b_j k$ (being in a coset is an equivalence relation, T0.22 says that eq relations partition a set). Then $g = a_i b_j k \in \bigcup a_i b_j K$. So $\left\{a_i b_j K\right\}$ covers $G$. We need to show that $\left\{a_i b_j K\right\}$ is a partition of $G$. Suppose that $x = a_i b_j k_1 = a_k b_l k_2$ for some $k_1, k_2 \in K$. Then $x \in a_i H \bigcap a_k H$, which is nonempty iff $a_i = a_k$. Use the cancellation law to get $y = b_j k_1 = b_l k_2$. Then $y \in b_j K \bigcap b_l K$, which is nonempty iff $b_j = k_l$. So $\left\{a_i b_j K\right\}$ is a partition of $G$ into left cosets of $K$. There's only one of those, so $|\left\{a_i b_j K\right\}| = (G:K)$ and clearly $|\left\{a_i b_j K\right\}| = mn = (G:H)\,(H:K)$. □

# 3 Homomorphisms, Quotients, Actions and Burnie

The subgroup generated by the set $\{a_i : i \in I\}$ in $G$ is the minimal subgroup of $G$ containing $\{a_i : i \in I\}$. If the subgroup is $G$ itself, $\{a_i : i \in I\}$ generates G. Since the set of finite products of the $a_i$'s is a subgroup containing $\{a_i : i \in I\}$, it must contain the subgroup generated by them, since that subgroup is minimal. It is clear that the set of finite products is in the minimal subgroup. So they are equal and we don't need to worry about an element being an infinite product of the generators of a group. A corollary of this is that two homomorphisms that agree on the output of generators of a group agree everywhere.

## Factor Groups

We claim that $\mathbb{Z}_4 \times \mathbb{Z}_2 / \{0\} \times \mathbb{Z}_2 = \mathbb{Z}_4 \times \mathbb{Z}_2 / H \simeq \mathbb{Z}_4$. Since the projection $\phi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ given by $\phi(a, b) = a$ has kernel $H$ and image $\mathbb{Z}_4$,

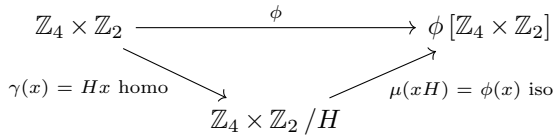



**Fig: Canonical morphisms**

there is a canonical isomorphism from the quotient to $\phi(\mathbb{Z}_4 \times \mathbb{Z}_2) = \mathbb{Z}_4$ via $\mu\left((a, b) H\right) = \phi(a, b)$. The moral of the story is that if we can find a homomorphism with a kernel matching our quotient, we can construct an isomorphism with the image of the homomorphism. It doesn't really matter what space we embed $\phi(G)$ in, so long as $\phi$ is still a homomorphism. We could just as easily have defined $\phi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_8$, $\phi(a, b) = 2a$. In that case the image of $\phi$ would be a subgroup of $\mathbb{Z}_8$ isomorphic to $\mathbb{Z}_4$.

### Simple Groups

A simple group is a NONTRIVIAL group with no proper nontrivial normal subgroups. Here is an incredibly awkward proof that $A_n,\ n \neq 1, 2, 4$ is simple.

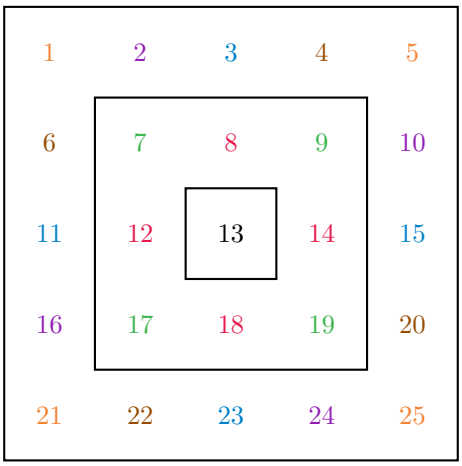
**Lemma 1.** *Any permutation can be expressed as a product of disjoint cycles.*

*Proof.* Let $\sigma \in S_n$. Let $O_1, \ldots, O_m$ be the orbits of $\sigma$, where $1 \leq m \leq n$. For each $1 \leq i \leq m$ define the cycle

$$\mu_i(x) = \begin{cases} \sigma(x), & x \in O_i \\ x, & \text{otherwise.} \end{cases}$$

Then the cycles are disjoint and $\sigma = \mu_1 \ldots \mu_m$. □

This theory is something you can use when coding. Rotation of an $n \times n$ matrix by 90 degrees is a permutation on the elements in the matrix. For a five by five matrix there are 7 distinct orbits illustrated by different colours:




if you want to apply the rotation $\sigma_{90}$ in place, you can start by writing

$$\sigma_{90} = (1,5,25,21)\,(2,10,24,16)\,(3,15,23,11)\,(4,20,22,6)\,.$$

Each cycle is then a product of transpositions, e.g. $(1,5,25,21) = (21,25)\,(25,5)\,(5,1)$. A transposition $(a,b)$ can be done in place with xor via $a \to a \oplus b$ then $b \to a \oplus b = (a \oplus b) \oplus b = a \oplus (b \oplus b) = a \oplus 0 = a$ then $a \to b \oplus a = a \oplus (a \oplus b) = b$.

**Lemma 2.** *Let $N$ be a nontrivial normal subgroup of $A_n$, where $n \geq 5$. Then $N$ contains a 3-cycle.*

*Proof.* Pick $\sigma \in N$ with $\sigma \neq \iota$. Using the lemma, we can write $\sigma$ as a product of disjoint cycles. If $\sigma$ is itself a 3-cycle, we're done. If the product contains product of two cycles, where at least one cycle is of length greater than 3, we can write

$$\sigma = \mu_1\,(a_1,\ldots,a_r)\,\mu_2,$$

where each factor is disjoint from the others. Since $N$ is normal, $\sigma^{-1}\,(a_1,a_2,a_3)\,\sigma\,(a_3,a_2,a_1) = (a_1,a_3,a_2)$ is in $N$. If it does not, then there are three cases. Suppose the product is of the form

$$\sigma = \mu_1\,(a_1,a_2,a_3)\,\mu_2,$$

where $\mu_1, \mu_2$ are products of transpositions and the factors are disjoint. Then $\sigma^2 = (a_1,a_3,a_2) \in N$, so $N$ contains a 3-cycle. Suppose

$$\sigma = \mu_1\,(a_1,a_2,a_3)\,(a_4,a_5,a_6)\,\mu_2,$$

where the factors are disjoint. Let $\tau = \sigma^{-1}\,(a_1,a_2,a_4)\,\sigma\,(a_4,a_2,a_1) = (a_1,a_4,a_2,a_6,a_3) \in N$. Then $\tau^{-1}\,(a_1,a_4,a_2)\,\tau\,(a_1,a_4,a_2)^{-1} = (a_1,a_2,a_4) \in N$. Finally, suppose $\sigma$ is a product of disjoint transpositions. Then, given that $\sigma$ cannot itself be expressed as a 3-cycle, write

$$\sigma = \mu\,(a_1,a_2)\,(a_3,a_4)\,,$$

where $\mu$ is the product of an even number (possibly zero) of disjoint transpositions. Let $\tau = \sigma^{-1}(a_1, a_2, a_3)\sigma(a_3, a_2, a_1) = (a_1, a_3)(a_2, a_4) \in N$. Pick $a_i \in A_n \setminus \{a_1, a_2, a_3, a_4\}$. Then $\tau(a_1, a_3, a_i)\tau(i, a_3, a_1) = (a_1, a_3, a_i)$, so $N$ contains a 3-cycle. □

**The alternating groups are simple for** $n \neq 1, 2, 4$.

*Proof.* The group $A_3$ is of prime order, so simple. If $n \geq 5$, let $N$ be a nontrivial normal subgroup of $A_n$. Then $N$ contains a 3-cycle by the lemma, call it $(r, s, i)$. Fix $j$ between 1 and $n$. Then $(r, s, j) = (r, s)(i, j)(r, i, s)(r, s)(i, j) = A(r, s, i)^2 A^{-1} \in N$. It is then possible to generate any 3-cycle $(i, j, k)$ with the squaring trick and the computation $(r, i, s)(r, s, k) = (s, k, i)$. Namely, $(s, j, k)(s, k, i) = (i, j, k)$. Fix $A \in A_n$. Write $A = \delta_1 \dots \delta_k$ where

$$\delta_k = \left(\delta_{k_1}, \delta_{k_2}\right)\left(\delta_{k_3}, \delta_{k_4}\right) = \begin{cases} \iota, \text{ if } \left(\delta_{k_1}, \delta_{k_2}\right) = \left(\delta_{k_3}, \delta_{k_4}\right) \text{ as transpositions,} \\ \text{A permutation of } \left(\delta_{k_1}, \delta_{k_2}, \delta_{k_3}\right), \text{ if } \left|\left\{\delta_{k_1}, \delta_{k_2}\right\} \cap \left\{\delta_{k_3}, \delta_{k_4}\right\}\right| = 1, \\ \left(\delta_{k_1}, \delta_{k_2}, \delta_{k_3}\right)\left(\delta_{k_2}, \delta_{k_3}, \delta_{k_4}\right), \text{ otherwise.} \end{cases}$$

Then $A$ is a finite product of elements in $N$, so $A_n \subset N$ and $A_n = N$. □

## Group Actions are a bit strange

A $G$-set isomorphism is a bijection $\phi : X \to Y$ with $g\phi(x) = \phi(gx)$.

**Theorem 1.** *Suppose $X$ is a **transitive** $G$-set. Fix $x_0 \in X$ and let $L$ be the set of left cosets of the subgroup $G_{x_0}$ fixing $x_0$. Then $X$ is isomorphic to $L$.*

*Proof.* Let $\phi : L \to X$ be given by $\phi\left(\delta G_{x_0}\right) = \delta x_0$. Then $\phi$ is well defined, for if $\delta_1 G_{x_0} = \delta_2 G_{x_0}$, then $\delta_2 = \delta_1 g$ and $\delta_2 x_0 = \delta_1 g x_0 = \delta_1 x_0$. Suppose that $\delta_1 x_0 = \delta_2 x_0$. Then ${\delta_1}^{-1}\delta_2 x_0 = x_0$, so ${\delta_1}^{-1}\delta_2 \in G_{x_0}$. So $\delta_2 \in \delta_1 G_{x_0}$ and $\delta_1 G_{x_0} = \delta_2 G_{x_0}$ and $\phi$ is injective. Fix $x \in X$. Since $X$ is transitive, $\exists g \in G$ such that $gx_0 = x$ so that $\phi\left(gG_{x_0}\right) = gx_0 = x$, so $\phi$ is a bijection. It is easy to see that $g_1\phi\left(g_2 G_{x_0}\right) = \phi\left(g_1 g_2 G_{x_0}\right)$, so $\phi$ is an isomorphism. □

**Corollary 1.** *The orbit of element $x \in X$ is $G$-set isomorphic to the collection of left cosets of the stabiliser subgroup $G_x$.*

**Theorem 2.** *Let $X$ be any $G$-set. Then $X$ is (index ignoring $G$-set) isomorphic to a disjoint union of left coset $G$-sets. A disjoint union is a cheaty way to write a union of not disjoint sets as disjoint ones by indexing them.*

*Proof.* Since the orbits $O_i$ for $i \in I$ of $X$ are transitive $G$-sets, the prior theorem says that each orbit is ($G$-set) isomorphic to the set $L_{x_i}$ of left cosets of the subgroup fixing some $x_i \in O_i$. We will denote the isomorphisms between $O_i$ and $L_{x_i}$ by $\phi_i$ for $i \in I$. We define $L'_{x_i} = \left\{(x, i) : x \in L_{x_i}\right\}$ so that the collection of sets $L'_{x_i}$ for $i \in I$ is disjoint. We claim that $X \simeq \bigcup_{i \in I} L'_{x_i}$. Let $\phi : X \to \bigcup_{i \in I} L'_{x_i}$ be given by $\phi = \delta \circ \psi$ where $\psi : X \to X \times I$ is given by $\psi(x) = (x, j)$ where $j$ is the index of the orbit $O_j$ containing $x$ and $\delta : X \times I \to X \times I$ is given by $\delta(x, j) =$

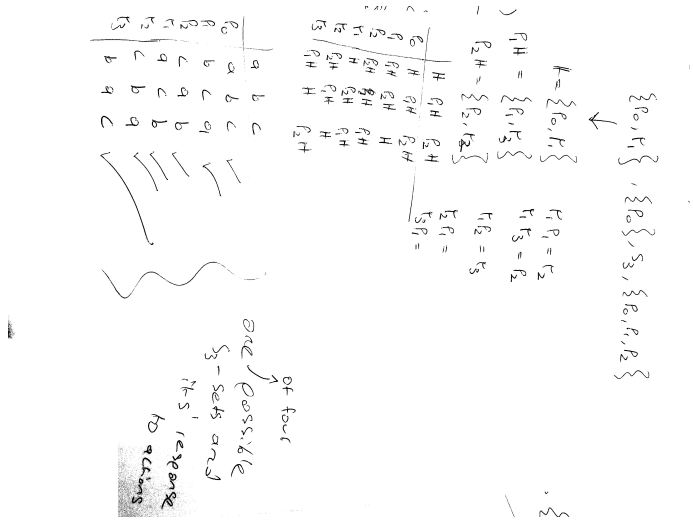
$\left(\phi_j(x), j\right)$. It's clear that $\psi$ is injective. Suppose that $\delta(a,b) = \delta(c,d)$. Then $\phi_b = \phi_d$, and injectivity of $\delta$ follows from injectivity of $\phi_b$. Since $\delta$ and $\psi$ are injective, $\phi$ is also. Fix $a \in \bigcup_{i\in I} L'_{x_i}$. Then $a \in L'_{x_j}$ for some $j \in I$, so write $a = (x, j)$ where $x \in L_{x_j}$. Since $\phi_j$ is onto $L_{x_j}$, we can write $a = \left(\phi_j(x), j\right)$ for some $x \in O_j$. Then $\phi(x) = (\delta \circ \psi)(x) = \delta(x, j) = \left(\phi_j(x), j\right) = a$, so $\phi$ is onto. Now we need to show that $\phi$ is a $G$-set isomorphism. Fix $x \in X$ and $g \in G$ and let $x \in O_j$. Then since $\phi_j$ is a $G$-set isomorphism and $gx \in O_j$, $g\phi(x) = g\left(\phi_j(x), j\right) := \left(g\phi_j(x), j\right) = \left(\phi_j(gx), j\right) = \phi(gx)$. □

**Theorem 3.** *$H, K$ are conjugate subgroups of $G$ iff the collections of their left cosets are isomorphic as $G$-sets.*

*Proof.* Reasonably doable. □

These are weird theorems but they are quite useful. E.g. How many transitive $S_3$-sets are there and what do they look like? Well theorem 1 says that any such $S_3$-set $X$ must be isomorphic to the cosets of a subgroup of $S_3$ that fixes one of the elements in $X$. There are six subgroups of $S_3$. The two element subgroups of $S_3$ are conjugate subgroups of each other, so theorem 3 says that the corresponding left coset collections are isomorphic as $S_3$-sets. So we need only consider the actions on the left cosets of the following subgroups:

$$\{\rho_0\},\ S_3,\ \{\rho_0, \rho_1, \rho_2\},\ \{\rho_0, \mu_1\}.$$



Two $G$-sets are isomorphic when we can relabel elements in one of their action tables to get the other table.

# Rings and Fields

## Rings of Polynomials

We claim that the only units in $D[x]$ are the units of the integral domain $D$.

*Proof.* Let $f(x), g(x) \in D[x]$ and write

$$f(x) = a_n x^n + \ldots + a_0, \quad g(x) = b_m x^m + \ldots + b_0.$$

Then

$$\begin{aligned} fg(x) &= \sum_{j=0}^{n+m} x^j \sum_{w=0}^{j} a_w b_{j-w} \\ &\Longrightarrow \\ \text{coeff}\left(x^{n+m}\right) &= \underbrace{a_0 b_{n+m} + \ldots + a_{n-1} b_{m+1}}_{0} + a_n b_m + \underbrace{a_{n+1} b_{m-1} + \ldots + a_{n+m} b_0}_{0} \end{aligned}$$

Since $D$ is an integral domain and $a_n, b_m \neq 0$, the product $a_n b_m \neq 0$. In particular, if $n+m \geq 1$ then $fg(x) \neq 1$. The contrapositive is that if $fg(x) = 1$, then $n + m < 1 \iff n = m = 0$. □

More or less the same argument says that $D[x]$ is itself an integral domain.

**Theorem 4.** *Suppose that $F$ is a FINITE field. Then $p_F = F^F$.*

*Proof.* Well $f \in F^F$ is uniquely defined by its values on $\{a_1, \ldots, a_n\} = F$. So for $g(x) = \sum_{i=1}^{n} c_i g_i(x)$, where

$$c_i = f(a_i)(a_i - a_1)^{-1} \ldots (a_i - a_{i-1})^{-1} \quad (a_i - a_{i+1})^{-1} \ldots (a_i - a_n)^{-1} \in F$$

and

$$g_i(x) = (x - a_1) \ldots (x - a_{i-1}) \quad (x - a_{i+1}) \ldots (x - a_n) \in p_F,$$

we have $g(a_1) = g_1(a_1) + 0 \ldots + 0 = f(a_1) * 1 * \ldots * 1 = f(a_1)$ and so on for $a_2, \ldots, a_n$ by construction. So $f(a) = \phi_a\left(g(x)\right) \in p_F$. □

## Factorisation of Polynomials Over a Field

N.B. reducible doesn't mean zeros exist, e.g. $\left(x^2 + 1\right)^2$ is reducible.

**Theorem 5.** *Deg 2,3 poly's are reducible iff they have zeros.*

*Proof.* It's not deep. □

**Theorem 6.** *A polynomial of degree $m$ has at most $m$ zeros.*

**Corollary 2.** *Any FINITE subgroup $G$ of the multiplicative group of a field $F$ is cyclic.*

*Proof.* Well $G \simeq \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_n}$ where $d_i$ are powers of primes. Let $m = \operatorname{lcm}(d_1, \ldots, d_n)$. Then $|G| \geq m$. Since $d_i | \ |G|$, $g^{|G|} = 1$, since each component evaluates to the multiplicative identity. So every $g \in G$ is a solution to $x^m - 1 = 0$ in $F$. Theorem says $m \geq |G|$, we then have $m = |G|$, so $d_i$ are (powers of) unique primes. So $G \simeq \mathbb{Z}_{|G|}$ which is cyclic. □

**Lemma 3.** *For any non-constant polynomials*

$$p(x) = a_{m+k}x^{m+k} + \ldots + a_0, \quad g(x) = b_m x^m + \ldots + b_0$$

*in a commutative ring with unity where $b_m$ is a unit, we can write*

$$p(x) = g(x)\, q(x) + r(x),$$

*where $r(x) = 0$ or $r(x)$ has a smaller degree than $g(x)$.*

*Proof.* Read the book 23.1. □

**Theorem 7.** *A polynomial $p(x)$ in a commutative ring with unity $R[x]$ has a zero iff the zero factors into $p(x)$.*

*Proof.* If $(x - m)$ is a factor then it is obvious that $m$ is a zero. If $m$ is a zero, then use the lemma to write

$$p(x) = (x - m)\, q(x) + r(x).$$

Then $r(x) = 0$ or has degree zero but that can't happen since $p(m) = 0$. □

**Theorem 8.** *A primitive polynomial $f(x) \in \mathbb{Z}[x]$ is reducible iff $f(x)$ is reducible in $\mathbb{Q}[x]$. Primitive means the gcd of the coefficients is 1.*

**Theorem 9.** *The Eisenstein criterion says that if $a_n \neq 0 \in \mathbb{Z}_p$ and $a_0 \neq 0 \in \mathbb{Z}_{p^2}$ while $a_{n-1}, \ldots, a_0 = 0 \in \mathbb{Z}_p$, then $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$.*

*Proof.* Let $d = \gcd(a_n, \ldots, a_0)$. Then $f(x)/d$ is primitive and so Theorem 8 says we can work in $\mathbb{Z}[x]$. Let

$$f(x)/d = (b_r x^r + \ldots + b_0)(c_s x^s + \ldots + c_0).$$

Since $d | a_0, a_n$, $d \neq 0 \in \mathbb{Z}_{p^2}, \mathbb{Z}_p$ and so $d$ is a unit in the ring $\mathbb{Z}_{p^2}$. We can use cancellation to see that

$$b_0 c_0 d = a_0 = 0 \in \mathbb{Z}_{p^2} \iff b_0 c_0 = 0 \in \mathbb{Z}_{p^2}.$$

In particular, the condition that $a_0 \neq 0 \in \mathbb{Z}_{p^2}$ tells us that one of $b_0, c_0$ must not be equal to zero in $\mathbb{Z}_p$. Let's go ahead and assume it's $b_0$. Then let $m$ be the smallest integer such that $c_m \neq 0 \in \mathbb{Z}_p$. Then

$$a_m = db_0 c_m + db_1 c_{m-1} + \ldots + \begin{cases} db_r c_{m-r} \text{ if } m > r \\ db_s c_0 \end{cases}$$

Since $d, b_0, c_m \neq 0 \in \mathbb{Z}_p$ while the terms that follow contain $c_{m-i}$ which are zero, $a_m \neq 0 \in \mathbb{Z}_p$ and so $m = n = s$ and $r = 0$. So

$$f(x) = db_0 \left(c_n x^n + \ldots + c_0\right),$$

only trivial factorisations can occur and $f(x)$ is irreducible. □

Eisenstein is more usable if we consider $f(x+a)$ and reversed coefficient $f(x)$ but its not the best for random polynomials.

**Corollary 3.** *The Cyclotomic polynomials* $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \ldots + 1$ *are irreducible because Eisenstein says that* $\Phi_p(x+1)$ *is irreducible. Actually* $p$ *need not be prime, the roots are roots of unity.*

**Theorem 10.** *If* $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ *with* $a_0 \neq 0$ *has a rational zero, it has an integer zero* $m$ *dividing* $a_0$*.*

*Proof.* Well the greatest common divisor of the coefficients is one so we are allowed to use Theorem 8. Then Theorem 7 says

$$f(x) = (x-m)\left(x^{n-1} + \ldots - m^{-1}a_0\right).$$

□

The whole shebang about Theorem 8 is only needed because we are talking about rational zeros. For $\mathbb{Z}_n[x]$, we would see that if $m$ is a zero then $(x-m)$ is a factor and $m$ must divide $a_0$ in $\mathbb{Z}_n$. N.B. however that divisors of $a_0$ in $\mathbb{Z}_n$ need not be divisors of $a_0$ in $\mathbb{Z}$. E.g. $1, 2, 4, 5$ are divisors of $4 \in \mathbb{Z}_6$ and $5$ is a zero of $x^2 + 5x + 4$ but $5 \not| 4 \in \mathbb{Z}$. For $\mathbb{Z}_p$ there is no free lunch, every nonzero element is a divisor of $a_0$.