Math 4400
Week 4 – Tuesday
Algebraic structures + Lagrange's Theorem

Definition: A ring* is a set R equipped with

- An addition law $+$: $R \times R \xrightarrow{+} R$
  $(a, b) \mapsto a+b$
- A multiplication law $\cdot$: $R \times R \xrightarrow{\cdot} R$
  $(a, b) \mapsto a \cdot b$
- Distinguished elements $1 \in R$, $0 \in R$

* Last week we called this a number system. Some sources will call this a commutative ring.

Such that:

1. Addition satisfies the commutative and associative laws $((a+b)+c) = (a+(b+c))$
2. Multiplication satisfies the commutative ($a \cdot b = b \cdot a$) and associative laws
3. The distributive law holds $a(b+c) = ab + ac$.
4. For any $a \in R$, $a + 0 = a$ and $a \cdot 1 = a$.
5. For any $a \in R$, there is a unique element $-a \in R$ such that $a + (-a) = 0$.

Examples of rings:

1) Seen already: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$.

2) New example: If R is a ring, $R[x]$ is the ring of polynomials with coefficients in R in the variable x

E.g. x^2+5, x^3+x+1 in $\mathbb{Z}[x]$

$$(x^2+5)+(x^3+x+1) = x^3+x^2+x+6$$

$$(x^2+5)(x^3+x+1) = x^5+6x^3+x^2+5x+5$$

These rules make sense with coefficients in <u>any</u> ring.

Example: $(x^2+2)^2$ in $\mathbb{Z}/3\mathbb{Z}[x]$.

$$(x^2+2)(x^2+2) = x^4+2x^2+2x^2+2\cdot 2$$
$$= x^4+2x^2+2x^2+1 \text{ in } \mathbb{Z}/3\mathbb{Z}[x]$$

Definition: If R is a ring and $a \in R$, we say a is invertible (or has a multiplicative inverse) if there is an element $a^{-1} \in R$ such that $aa^{-1}=1$.

Note: There is at most one such element; "$a^{-1} = \frac{1}{a}$" if it exists.

Definition: If R is a ring then $R^\times$ is the set of invertible elements in R.

Examples:

- $\mathbb{Z}^\times = \{\pm 1\}$
- $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \mid 0 \le a < n,\ \gcd(a,n) = 1.\}$.

  (from last week)

Definition: An (abelian) <u>group</u> is a set A with an operation $* : A \times A \to A$

$$(a,b) \mapsto a * b$$

and a distinguished <u>identity element</u> $e \in A$ such that

1. $*$ is commutative and associative
2. $a * e = a$ for all $a \in A$
3. For any $a \in A$, there exists a unique element $b \in A$ such that $ab = e$.

   $(b = a^{-1})$

Examples:

- If $(\mathbb{Z}, +)$ $e = 0$ $\quad (\mathbb{R}^\times, \cdot)$ $e = 1$ $\quad ((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ $e = 1$

- For any ring R, $(R, +)$ $e = 0$ and $(R^\times, \cdot)$. $e = 1$

  If a and b have inverses

then $(ab)(b^{-1}a^{-1}) = 1$

Definition: If A is a group, the <u>order</u> of A, written $|A|$, is the number of elements in A.

Example: $|\mathbb{Z}| = \infty$ $\qquad$ $|\mathbb{Z}^\times| = 2$, $\mathbb{Z}^\times = \{\pm 1\}$

$|\mathbb{Z}/n\mathbb{Z}| = n$ $\qquad$ $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$

group under addition.

Euler's ϕ function, defined by $\phi(n) = \#$ of $0 \leq a < n$ such that $\gcd(a,n) = 1$.

If p prime, $|(\mathbb{Z}/p\mathbb{Z})^\times| = \phi(p) = p-1$.

$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$

Theorem (Lagrange): Suppose A is a finite group, $|A| = n$. Then for any $a \in A$, $a^n = e$.

a^n means $\underbrace{a * a * a \ldots * a}_{n}$

Example: If p is prime and $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \bmod p$ $\leftarrow p-1 = \phi(p) = |(\mathbb{Z}/p\mathbb{Z})^\times|$

$\Rightarrow a^p \equiv a \bmod p$ ($\leftarrow$ also true when $p \mid a$).

"Fermat's Little Theorem"
(Apply Lagrange to $(\mathbb{Z}/p\mathbb{Z})^\times$).

e.g. if $p=5$: $1^4 = 1 \equiv 1 \mod 5$ $\quad 2^4 = 16 \equiv 1 \mod 5$
$3^4 = 81 \equiv 1 \mod 5$ $\quad 4^4 = 256 \equiv 1 \mod 5$

Proof of Lagrange's Theorem:
Take $a \in A$ $\quad |A| = n$.
Step 1: I claim there is some $k > 0$ such that $a^k = 1$. Justification: Look $a, a^2, a^3, a^4, \ldots$ this is an infinite list, but each thing is in the finite set A. So two must be the same, $a^{k_1} = a^{k_2}$ for $k_2 > k_1$.

$$a^{k_1}(a^{-1})^{k_1} = a^{k_2}(a^{-1})^{k_1}$$
$$e = a^{(k_2 - k_1)} \qquad k_2 - k_1 > 0. \checkmark$$

Let me take the smallest such k. Then:
$1, a, a^2, \ldots a^{k-1}$ are k distinct elements of A.
If this is all of A then $k = n$ $\quad a^n = 1$.
Otherwise take some other element $x \rightsquigarrow$

$$\left.\begin{array}{l} 1, a, a^2, \ldots a^{k-1} \\ x, xa, xa^2, \ldots xa^{k-1} \end{array}\right\} \text{Claim these are all distinct.}$$

Need $xa^i \neq a^j$. If $xa^i = a^j$ then $x = a^{j-i} \rightsquigarrow$ can't happen.
$\rightsquigarrow$ Keep going and you get

$$\begin{array}{l} 1, a, a^2, \ldots, a^{k-1} \\ x, xa, xa^2, \ldots, xa^{k-1} \end{array} \rightsquigarrow \text{Keep going till I get everything in } A. \rightsquigarrow a^n = a^{rk}$$

$g, ga, ga^2, \ldots, ga^{k-1}$ $\vdots$ $\qquad n = |A| = \underset{\substack{\uparrow \\ \text{\# of rows.}}}{r}k$ $\qquad = (a^k)^r = e^r = e.$

In general, Lagrange in $(\mathbb{Z}/n\mathbb{Z})^\times$ implies that for any a coprime to n, $\quad a^{\phi(n)} \equiv 1 \bmod n.$

Useful to combine with:

Theorem: ① If p is prime and k is a positive integer, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

② If $m_1, \ldots, m_s$ are positive integers such that $\gcd(m_i, m_j) = 1$ for all $i \neq j$, then $\phi(m_1 m_2 \cdots m_s) = \phi(m_1)\phi(m_2)\cdots\phi(m_s)$.

<u>Proof</u> Exercise 1 on worksheet.