Math 113 Notes–Spring 2015

Davis Foote

March 12, 2015

Day 1 : 01/20/15

Relation on a set
Formally, a subset of $S \times S$.

Functions
$f : A \to B$
Each element in A is sent to exactly one element of B
Domain: A
Codomain: B
Range: $\{f(a) : a \in A\}$
$1 - 1$ = Injective : $f(x_1) = f(x_2) \implies x_1 = x_2$
onto = Surjective : codomain = range, i.e. $\forall b \in B, \exists a \in A : f(a) = b$
both = bijective
Cardinality : Two sets have the same cardinality iff there exists a bijection between them

Partition
disjoint union of non-empty cells (subsets of S) which cover all of S.

Equivalence Relation on S A relation with three properties:
1. Reflexive: $x \sim x \forall x \in S$
2. Symmetric: $x \sim y \implies y \sim x$
3. Transitive: $x \sim y \wedge y \sim z \implies x \sim z$

Key example: integers mod n: $\mathbb{Z}_n$
Define an equivalence relation on $\mathbb{Z}$ by $a \sim b$ if $a - b$ is divisible by 4.
Equivalence classes:
$\bar{0} = \{\ldots, -4, 0, 4, 8, \ldots\}$
$\bar{1} = \{\ldots, -3, 1, 5, 9, \ldots\}$
$\bar{2} = \{\ldots, -2, 2, 6, 10, \ldots\}$
$\bar{3} = \{\ldots, -1, 3, 7, 11, \ldots\}$

Binary operation on a set S
how to combine 2 elements of S to get another element of set S
Formally, a map from $S \times S \to S$.
Two properties that they may have:
Commutativity: $a * b = b * a$
Associativity: $a * (b * c) = (a * b) * c$
Thm: Function composition is associative (proof in book)

nth roots of unity
complex solutions to $z^n = 1$
Evenly spaced around the unit circle and 1 is a root of unity for all n.

Day 2 : 01/22/15

$$\langle U, \cdot \rangle \cong \langle \mathbb{R}_{2\pi}, + \rangle$$
$$\langle U_n, \cdot \rangle \cong \langle \mathbb{Z}_n, + \rangle$$
$$\langle \{1, -1\}, \cdot \rangle \cong \langle \mathbb{Z}_2, + \rangle$$

Homomorphism Property (for a set with a binary operation):
If $\phi : \langle S, * \rangle \to \langle S', *' \rangle$, then ϕ is a **homomorphism** if

$$\phi(a * b) = \phi(a) *' \phi(b)$$

An **isomorphism** is a bijective homomorphism.

To prove that two sets under their respective binary operations are isomorphic,

1. Define some $\phi : S \to S'$
2. Check that ϕ is one-to-one
3. Check that ϕ is onto
4. Check that ϕ satisfies the homomorphism property

Structural Properties: If $\langle S, * \rangle$ has **structural property** P, then any $\langle S', *' \rangle$ which is isomorphic to $\langle S, * \rangle$ must also have property P.

Examples of Structural Properties

- Cardinality
- There exists an identity element e such that $e * x = x$ and $x * e = x$
- Commutativity
- There exists an element x with $x * x = x$

Day 3 : 01/27/15

Def: A **group** is a set G that is closed under a binary operation $*$ such that:

- $*$ is associative : $\forall a, b, c \in G : a * (b * c) = (a * b) * c$
- There exists an identity $e \in G$: $\forall g \in G : g * e = e * g = g$
- All elements have inverses: $\forall g \in G, \exists g^{-1} \in G : g * g^{-1} = g^{-1} * g = e$

Examples:

- $\langle \mathbb{Z}, + \rangle$
  - identity $= 0$
  - inverse of g is $-g$
  * Could replace $\mathbb{Z}$ with $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$
- $\langle \mathbb{Q}^*, \cdot \rangle$ where $Q^* = Q \ \{0\}$
  - identity $= 1$
  - inverse of g is $\frac{1}{g}$
  * Could replace $\mathbb{Q}^*$ with $\mathbb{R}^*$ or $\mathbb{C}^*$
- $\langle U_n, \cdot \rangle$
  - identity $= 1$
  - inverse of $e^{\frac{2\pi i}{n}} = e^{-\frac{2\pi i}{n}}$
- $\langle \mathbb{Z}_n, + \rangle$
  - identity $= \bar{0}$
  - inverse of $\bar{g} = n \bar{-} g = \bar{-}g$
- $\langle \{f : \mathbb{R} \to \mathbb{R}\}, + \rangle$
  - identity $= f(x) = 0 \forall x$
  - inverse of $f(x)$ is $-f$

Def: A group is **abelian** if its binary operation is commutative. All examples given so far are abelian.

A non-abelian example is matrix multiplication:

$$\langle \{\text{invertible } n \times n \text{ matrices}\}, \text{matrix multiplication} \rangle$$

A, B invertible, so A^{-1}, b^{-1} exist. Inverse of AB is $B^{-1}A^{-1}$, so closed under multiplication.

Another name for this group is $GL(n, \mathbb{R})$, i.e. **general linear group**

Thm (cancellation laws): If G is a group and $a, b, c \in G$ such that $a * b = a * c$ or $b * a = c * a$, then $b = c$.
Proof: Suppose $b * a = c * a$. Since G is a group, a has an inverse, a^{-1}.

$$\begin{aligned} (b * a) * a^{-1} &= (c * a) * a^{-1} \\ b * (a * a^{-1}) &= c * (a * a^{-1}) \\ b * e &= c * e \\ b &= c \end{aligned}$$

Thm: If G is a group and $a, b \in G$, then any equation of the form $ax = b$ or $xa = b$ has a unique solution.
Proof: Suppose $a * x = b$.

$$\begin{aligned} a^{-1} * (a * x) &= a^{-1} * b \\ (a^{-1} * a) * x &= a^{-1} * b \\ e * x &= a^{-1} * b \\ x &= a^{-1} * b \end{aligned}$$

So there exists at least one solution.
Suppose there are two solutions x_1, x_2 such that $a * x_1 = b$ and $a * x_2 = b$. Then $a * x_1 = a * x_2$ and by the cancellation laws $x_1 = x_2$, so there is at most one solution.

Note: Don't need to read about semigroups, monoids, left/right inverses for class

Note: In a group table, each element of G will appear in each row and column exactly once.

Day 4 : 01/29/15

Def:
Let G be a group. Then H is a **subgroup** of G if

(1) H is a subset of G

(2) H is closed under G's operation. $h_1 * h_2 \in H \forall h_1, h_2 \in H$

(3) H contains G's identity

(4) Inverses: If $h \in H$, then $h^{-1} \in H$

Alternatively, $H \subseteq G$, $H \neq \emptyset$, and $\forall a, b \in H, ab^{-1} \in H$.
In short, H is a subset of G that is also a group using the same operation.

Def:
A **cyclic subgroup** of G generated by $g \in G$ is denoted $\langle g \rangle$.

$$\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$$

Day 5 : 02/03/15

$$f : \mathbb{Z}_{12} \to U_{12}$$
$$\bar{k} \mapsto \left(e^{\frac{2\pi i}{12}}\right)^{2k}$$

This map is well-defined because

$$f(\bar{k}) = \left(e^{\frac{2\pi i}{12}}\right)^{2k} = \left(e^{\frac{2\pi i}{12}}\right)^{2k} \cdot \left(e^{\frac{2\pi i}{12}}\right)^{12n} = f(k + 6n)$$

$$f : \mathbb{Q} \to \mathbb{Q}$$
$$\frac{a}{b} \mapsto a$$

Not a well-defined map because

$$\frac{1}{2} = \frac{2}{4} \text{ but } f\left(\frac{1}{2}\right) = 1, f\left(\frac{2}{4}\right) = 2$$

Standard operations:

- For $\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}, \mathbb{Q}$, default is $+$
- For $\mathbb{R}^*, \mathbb{Q}^*, GL(n, \mathbb{R}), \mathbb{Z}_n^*, U_n, U$, default is $\cdot$

Def: A group is **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle$
Def: The **order** of a group is how many elements a group G has. It is ∞ if G is infinite, n if G has n elements.
Def: The **order** of $g \in G$ is the order of $\langle g \rangle$

Theorem: Every cyclic group is abelian.
Proof: Let G be a cyclic group with a generator g, i.e. $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Let $x, y \in G$. Then $x = g^a, y = g^b$ for some $a, b \in \mathbb{Z}$. $xy = g^a g^b = g^{a+b} = g^{b+a} = g^b g^a = yx$.

Theorem: A subgroup of a cyclic group is cyclic.
Proof: If $H = \{e\}$, $H = \langle e \rangle$. If $H \geq \{e\}$, then H has at least one $g^n \in H$, where $n \in Z^+$. Let m be the smallest positive integer such that $g^m \in H$. Let $g^n \in H$. If n is a multiple of m, then $n = mk$ for some $k \in \mathbb{Z}$, so $g^n = (g^m)^k$. If n is not a multiple of m, *show that m could not have been the smallest positive integer so $g^m \in \mathbb{Z}$*. **Use mod math**.

Classification of Cyclic Groups
If G is a cyclic group, then G is isomorphic to one of the following:

- $G \cong \mathbb{Z}$ if G is infinite
- $G \cong \mathbb{Z}_n$ if $|G| = n$

Let G be a cyclic group of order n. $G = \langle g \rangle$. If $H \leq G$ with $H = \left\langle g^k \right\rangle$, how big is H? Find $\gcd(k, n)$, call it d. Then $H = \left\langle g^d \right\rangle$, which has $\frac{n}{d}$ elements.

The number of generators of a cyclic group G of size n is $\phi(n)$

Day 6 : 2/05/15

Symmetric Groups

Def: A **permutation** of a set A is a bijection $A \to A$. Informally a reordering of the elements of A.
$[5] = \{1, 2, 3, 4, 5\}$
Two-line notation: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$
One-line notation: only write the second line. **No parentheses**.

Def: The **symmetric group** S_A on set A is the set of all permutations of A with the binary operation function composition. S_A is a group because

- Function composition is associative
- Identity permutation is $\sigma(a) = a$ for all $a \in A$
- Inverse of τ exists because permutations are bijective
- Closed under composition. If $\tau : A \to A$ and $\sigma : A \to A$, then $\tau \circ \sigma : A \to A$.

S_A is not abelian when $|A| \geq 3$.

Theorem: If $|A| = |B|$, then $S_A \cong S_B$.

Dihedral Groups

D_n is the symmetry group of a regular n-gon. In D_n, let r be the smallest rotation counterclockwise (i.e. $\frac{2\pi}{n}$ radians) and let s be reflection through the line containing 1 and the center.

$$D_n = \{e, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$$

They satisfy these rules:

- $r^n = e$
- $s^2 = e$
- $rs = sr^{-1}$

Day 7 : 2/10/15

Permutations - Notation

- Disjoint cycle notation

  Cycle notation built on **orbits**. If A is a set, $\sigma \in S_A$, then $a, b \in A$ are in the same orbit if and only if $b = \sigma^n(a)$ for some n. This is an equivalence relation:

  - $b = \sigma^0(b)$, so $b \sim b$
  - $b = \sigma^n(a) \implies a = \sigma^{-n}(b) = a$
  - $b = \sigma^n(a), c = \sigma^k(b) \implies c = \sigma^{n+k}(b)$

  Look up "group actions"

  Conventions:

  - Write the smallest element first in an orbit.
  - Don't bother writing singletons
  - Disjoint cycles

  Fact: Disjoint cycles commute. What if the cycles are not disjoint? Keep simplifying until they are.

  $$(5,1,2)(1,6,3,4)(2,7)(1,5,6) = (1)(2,7,5,3,4)(6) = (2,7,5,3,4)$$

  Remember to work from right to left. Permutation multiplication is composition of functions.

- Product of transpositions

  A **transposition** is a cycle of length 2 (swaps two things).

  $(a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \ldots (a_1, a_3)(a_1, a_2)$
  i.e. any cycle can be written as a product of transpositions.

  A given permutation can be written using different numbers of transpositions, but that number is either always odd or always even. We use this to classify **even and odd permutations**.

  Cycles of odd lengths are even transpositions and vice-versa.

  Theorem: In S_n, the subset of even permutations forms a subgroup of order $\frac{n!}{2}$.
  Proof: Normal subgroup proof. Size is shown because there is a bijection with odd permutations: $\sigma \mapsto (1,2)\sigma$.

  This group is called A_n, the **alternating group**.

Day 8 : 2/12/15

Lagrange's Theorem

If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Proof:

1. Know what cosets are
2. Show the cosets of H partition G
3. Show every coset has the same size as H.
4. Count $|G| =$ (size of coset)$\cdot$(number of cosets)
5. Conclude that $|G| = |H|\cdot$(number of cosets of H)

- Proof for 1 and 2:

  Define a relation $\sim_L$ where $a \sim_L b$ means a, b are in the same coset by $a \sim_L b$ iff $a^{-1}b \in H$. $\sim_L$ is an equivalence relation because:

  – $a \sim_L a$ because $a^{-1}a = e \in H$.
  – $a \sim_L b$ implies $a^{-1}b \in H$. $(a^{-1}b)^{-1} = b^{-1}a \in H$ since H is a group. So $b \sim_L a$.
  – $a \sim_L b$ and $b \sim_L c$ implies $a^{-1}b, b^{-1}c \in H$.
    Since H is a group, $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$.

- Proof for 3:

  The left cosets of H look like $aH = \{ah : h \in H\}$. Claim: $|H| = |aH|\ \forall a \in G$. Clearly $|aH| \leq |H|$. The ah_i are all different because if $ah_i = ah_j$ then $h_i = h_j$ but $h_i \neq h_j$ so ah_i are different. So $|H| \leq |aH|$ and therefore $|aH| = |H|$.

  Side note: Right cosets. $Ha = \{ha : h \in H\}$. In general, $aH \neq Ha$. Frequently we get different left and right coset partitions, but when G is abelian, they are always the same.

Corollary 1 to Lagrange's Theorem: If $|G|$ is a prime p, then G is cyclic.
Proof: Let $g \in G$ with $g \neq e$. How big is $\langle g \rangle$? The only choices are 1 and p, and it's not 1 because it has at least e and g in it. So $|\langle g \rangle| = p$ and $\langle g \rangle = G$.

Another statement of Lagrange's Theorem: If G is finite with order n, then the order of an element in G divides n.

Def: the **index** of H in G where $H \leq G$ is the number of cosets of H in G. Notation is $G : H$.

Theorem: If G is finite and $K \leq H \leq G$, then $(G : K) = (G : H)(H : K)$. **Proof:** By Lagrange's Theorem, when G is finite, $\frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|}$. Also true when G is infinite but I guess we're not getting into that now.

Day 9 : 2/24/15

Products of groups

Def: The **Cartesian product** of sets A and B is $A \times B = \{(a,b) : a \in A, b \in B\}$. We can take any finite product.

Def: The **internal direct product** of two groups G and H is the set $G \times H$ under the operation $(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$.

Proof that $G \times H$ is a group:

- Each component is associative
- Identity is (e_G, e_H)
- Inverse of (g,h) is (g^{-1}, h^{-1})
- Closed: $(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2) \in G \times H$

Theorem: $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m,n) = 1$.
Proof: Let $\gcd(m,n) = 1$. If we can find an element in $\mathbb{Z}_m \times \mathbb{Z}_n$ of order mn, that will do it. Consider $x = (\bar{1}, \bar{1})$. The first coordinate is zero when you add m copies of x. First time both are zero is $\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = mn$.
What if $d = \gcd(m,n) \neq 1$? Then, as shown, $(\bar{1}, \bar{1})$ is not a generator. Why can't (a,b) be a generator?
Claim: Order of (a,b) is less than or equal to $\frac{mn}{d}$. Adding $\frac{mn}{d}$ copies of (a,b) equals $(\frac{mn}{d} \cdot a, \frac{mn}{d} \cdot b)$. d divides both m and n, so $\frac{mn}{d}$ is equal to m times an integer and n times an integer. Therefore, in $\mathbb{Z}_m \times \mathbb{Z}_n$, the above is equal to $(0,0)$, so it has order at most $\frac{mn}{d}$.
Note: this proof also works for more than two factors. We check gcd of each pair of factors.

Example: $\mathbb{Z}_{60}$. What are some groups isomorphic to $\mathbb{Z}_{60}$? $60 = 2^2 \cdot 3 \cdot 5$.

- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_{15}$
- $\mathbb{Z}_{12} \times \mathbb{Z}_5$
- $\mathbb{Z}_3 \times \mathbb{Z}_{20}$

Note that $\mathbb{Z}_2 \times \mathbb{Z}_{30}$ is not isomorphic to these groups.

Theorem: The order of an element $(g,h) \in G \times H$ is the lcm of $|g|$ and $|h|$.

Def: A **finitely generated group** is a group which has a finite generating set. Examples: cyclic groups, D_n (generated by $\{r, s\}$), any finite group G (generated by itself). Nonexamples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

The Fundamental Theorem of Finitely Generated Abelian Groups: Every finitely generated abelian group is isomorphic to a finite product of cyclic groups. This product will be of the form

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$$

where the p_i are prime (possibly repeated) and $r_i \in \mathbb{Z}^+$. It could also have no finite factors (i.e. no $\mathbb{Z}_{p_i^{r_i}}$ factors). It could also have no infinite factors (i.e. no $\mathbb{Z}$ factors). Furthermore, this decomposition is unique up to reordering factors. The number of infinite factors is called the **Betti number** of this group.

What are all finitely generated abelian groups of order 8 up to isomorphism?

- $\mathbb{Z}_8$
- $\mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

$$\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_{25} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$$

In a finite abelian group, you can get a subgroup of any order allowed by Lagrange's Theorem, even though you can't necessarily get an element of any order.

Day 10 : 2/26/2015

More on FTFGAG

- Finite abelian groups of order $144 = 2^4 \cdot 3^2$:
  - $\mathbb{Z}_{16} \times \mathbb{Z}_9 \cong \mathbb{Z}_{144}$
  - $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9$
  - $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$
  - $\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3$
  - $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
  - $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

Day 12 : 3/5/2015

Factor Groups

Theorem: Suppose $H \leq G$. Left coset multiplication $(aH)(bH) = (ab)H$ is well-defined iff H is normal in G.
To check well-defined: If I use different names for my cosets, do I still get the same product?
If $a_H = a_2H$, $b_1H = b_2H$, we want $(a_1H)(b_1H) = (a_2H)(b_2H)$ so $(a_1b_1H) = (a_2b_2H)$. In other words, is $a_1b_1 \in (a_2b_2)H$?
$a_1 \in a_2H$, so $a_1 = a_2h_1$ for some $h_1 \in H$
$b_1 \in b_2H$, so $b_1 = b_2h_2$ for some $h_2 \in H$
So $a_1b_1 = a_2h_1b_2h_2$. $h_1b_2 \in Hb_2$. Since H is normal, $Hb_2 = b_2H$. Therefore $h_1b_2 = b_2h_3$ for some $h_3 \in H$. So $a_1b_1 = a_2b_2h_3h_2 \in (a_2b_2)H$.

Theorem: Suppose H is normal in G. Let G/H denote the set of cosets of H. Then G/H is a group using coset multiplication.

The First Isomorphism Theorem: If $\phi : G \to H$ is a groups homomorphism, then $G/\ker(\phi) \cong \text{im}\phi$.
Build this up: Make another map μ using ϕ. Let $K = \ker\phi$. $\mu : G/K \to \phi[G]$.
$gK \mapsto \phi(g)$

- One-to-one: $\ker\mu = \{gK : \phi(g) = \mu(gK) = e_H\}$. $\phi(g) = e_H$ iff $g \in \ker\phi = K$. But if $g \in K$, then $gK = eK$
- Onto: Everything in $\phi[G]$ comes from some $g \in G$. If $\phi(g) \in \phi[G]$ then $gK \mapsto \phi(g)$
- Homomorphism: $\mu(g_1K \cdot g_2K) = \mu(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \mu(g_1K)\mu(g_2K)$.

Theorem: The following are equivalent:

- H is normal in G
- $gH = Hg$ for all $g \in G$
- $gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H$
- $ghg^{-1} \in H$ for all $g \in G, h \in H$

Theorem: If G is a cyclic group and $H \leq G$, then G/H is a cyclic group.
Proof: Let $G = \langle g \rangle$. Then $H = \langle g^m \rangle$ Cosets (elements of G/H) are $g^k H$ (has repeats but lists everything). So what's a generator for G/H? Any $g^k H$ can be written as a power of gH, so $G/H = \langle gH \rangle$.

Fun fact: If G is abelian and H is normal in G, then G/H is abelian.

3/12/2015

Rings and Fields

- **Theorem:** In $\mathbb{Z}_n$, a nonzero element k is a zero divisor iff $\gcd(k,n) = d > 1$.
  Proof: $k \cdot \left(\frac{n}{d}\right) = \left(\frac{k}{d}\right) \cdot n = 0$

- **Theorem:** In a ring R, we have additive cancellation but multiplicative cancellation iff R has no zero divisors.
  Proof: Assume we have $ab = ac \implies b = c$ for $a, b, c \in R, a \neq 0$. WTS R has no zero divisors. Assume $ab = 0$. If $a = 0$, done. Otherwise, $a \neq 0$; rewrite our equation to $ab = a0$. By cancellation, $b = 0$. So R has no zero divisors.
  Suppose R has no zero divisors. Assume $ab = ac$ with $a \neq 0$. $ab - ac = a(b-c) = 0$. Since there are no zero divisors, $a = 0$ or $b - c$ is 0. By assumption $a \neq 0$, so $b - c = 0$ and therefore $b = c$.

- **Def:** An **integral domain** is a commutative ring which has no zero divisors.
  Corollary: Integral domains have cancellation laws, and a consequence is that you can solve (usually polynomial) equations by factoring.

- **Theorem:** If F is a field, then F is an integral domain.
  Proof: Fields are commutative rings by definitions. Only need to check there are no zero divisors. Suppose $ab = 0$. If $a = 0$, done. If not, $a \neq 0$ so a^{-1} exists in F. $ab = 0 \implies \frac{1}{a}ab = 0 \implies b = 0$. Thus G has no zero divisors and it's an integral domain.

- **Theorem:** Every finite integral domain is a field.
  Proof (in book): List elements $1, a_1, a_2, \ldots, a_k$. Think about any a from this list. Multiply everything on the left by a. Get $a, aa_1, aa_2, \ldots, aa_k$, which is a permutation of the elements.
  Corollary: In particular, if p is prime, Z_p is a field.

- **Def:** If there exists $n \in Z^+$ so that $a + \ldots + a = 0$ (n copies of a) for all $a \in R$, then the smallest such n is called the **characteristic** of R. If no such integer exists, then char $R = 0$. An equivalent definition is that the characteristic of R is the largest additive order of an element in $\langle R, + \rangle$.

- **Theorem:** It's enough to find the additive order of 1_R to find char R.