Math 113 Notes–Spring 2015

Davis Foote

April 28, 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 $\operatorname{lcm}(m, n) = \frac{mn}{\gcd(m,n)} = mn$.
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 $\mathbb{Z}_{p_i^{ri}}$ 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.

3/31/2015

Euler's ϕ

- **Def:** Let $\phi(n)$ be Euler's phi function, i.e. $\phi(n)$ =the number of units in Z_n = how many integers in $1 \ldots n$ are relatively prime to n.

- **Euler's Theorem**: If a is relatively prime to m (i.e. a is a unit in Z_m), then $a^{\phi(m)} \equiv 1 \mod m$

- **Proof:** $a^{\phi(m)} \equiv 1 \mod m \Leftrightarrow \overline{a^{\phi(m)}} = \overline{1}$ in $\mathbb{Z}_m$ The right hand side is true because the units of Z_m form a group under multiplication. The order of this group is $\phi(m)$. Since the order of $\overline{a}$ divides the order of the group, $\overline{a^{\phi(m)}} = \overline{a}^{\phi(m)} = \overline{1}$.

- **Special case: Fermat's Little Theorem:** If p is prime and $a \not\equiv 0 \mod p$, then $a^{p-1} \equiv 1 \mod p$.

- **Theorem:** Let $m \geq 2$ be an integer, and let $a, b \in Z$ and $d = \gcd(a, m)$. Then the congruence $ax \equiv b \mod m$ has
  - no solutions if d does not divide b
  - d equivalence classes mod m as solutions if d divides b

- **Proof:** Don't need to memorize; basically a lot of arithmetic with integers.

4/9/2015

Section 23

Don't worry about Eisenstein proof.

Theorem: Let F be a field. If $p(x)$ is irreducible in $F[x]$, and $p(x)|r(x) \cdot s(x)$ for some $r(x), s(x) \in F[x]$, then $p(x)|r(x)$ or $p(x)|s(x)$. Essentially, irreducible polynomials are "like primes" in $\mathbb{Z}$. Proof will be presented next time.

Theorem: Factoring is unique in $F[x]$ up to reordering factors and relocating constants. More formally: every nonconstant $f(x) \in F[x]$ can be factored as a product of irreducibles in $F[x]$, and this is unique (up to the same stuff).
Proof: Suppose $f(x) \in F[x]$ is nonconstant. If $f(x)$ is irreducible, QED. If not, then $f(x)$ can factor into two smaller degree factors $f(x) = g(x)h(x)$. If g, h are both irreducible, QED. If not, factor whichever ones are irreducible. Repeat until only irreducibles remain. This must happen because each time we factor, degrees are decreased, but degrees are always nonnegative integers so we must eventually stop. We end up with $f(x)$ as a product of irreducible polynomial factors $g_1(x) \cdots g_k(x)$.
To verify uniqueness, suppose we have two factorizations of f: the one above, and another $h_1(x) \cdots h_l(x)$. $g_1(x)$ is a factor of f, so $g_1(x)|h_1(x) \cdots h_l(x)$. Since $g_1(x)$ is irreducible, from the above theorem, $g_1(x)$ must divide one of the h_i, say $h_m(x)$ for some m. So $h_m(x) = g_1(x)u_1(x)$. Since h_m is irreducible, either g_m or u must be a constant. g_m is not, so u_1 is, and hence g_1 and h_m are constant multiples of each other. $F[x]$ is an integral domain, sowe can cancel g_1 and h_m, yielding $g_2(x) \cdots g_k(x) = h_1(x) \cdots u_1 \cdots h_l(x)$. Repeat the above with all the g_i so all that remains on the RHS is a product of constants.

Section 26

Recall: A ring homomorphism is a map $\phi : R \to S$ such that $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$. Remember that we define rings to necessarily have unity.

Theorem: If $\phi : R \to S$ is a ring homomorphism, then

- $\phi(0_R) = 0_S$
- $\phi(1_R) = 1_S$
- $\phi(-a) = -\phi(a)$
- $\phi[\text{subring of } R] = \text{subring of } S$
- $\phi^{-1}[\text{subring of } s] = \text{subring of } R$

Proof: All are straightforward.

Def: For a ring homomorphism $\phi : R \to S$, the **kernel** is $\ker \phi = \phi^{-1}(0_S)$.

Theorem: Let $K = \ker \phi$. Then if $\phi(r) \in \mathrm{im} \phi$ then $\phi^{-1}(\phi(r)) = r + K = K + r$ (additive coset of K).

4/14/2015

Ideals

- **Def:** An **ideal** I of a ring R is an additive subgroup of R such that for all $x \in I, r \in R$, $rx, xr \in I$.

  Ideal criteria:

  - $I \subseteq R$
  - nonempty $(0 \in I)$
  - $\forall a, b \in I : a - b \in I$
  - $\forall r \in R : \forall x \in I : ar, ra \in I$

  Subring criteria: first three are the same, last is replaced with $\forall a, b \in S : ab \in S$

  Easy examples of ideals:

  - $I = \langle x \rangle =$ "R-multiples of x" $= \{rx : r \in R\}$

  If F is a field, there are only 2 ideals, F and $\{0\}$.

  In a trivial ring, $0 = 1$, but otherwise, $0 \neq 1$.

  In general, a ring $R \neq \{0\}$ has at least two ideals, R itself and $\{0_R\}$

- **Theorem:** The kernel of a ring homomorphism $\phi : R \to S$ is always an ideal of R.

  Proof: $K = \ker \phi = \phi^{-1}\{0_S\} = \{r \in R : \phi(r) = 0_s\}$. Check the four criteria.

  We will see later that this is biconditional, that is I is an ideal of R if and only if there exists a ring homomorphism $\phi : R \to\ ?$ with $\ker \phi = I$

- **Theorem:** If R is a ring and I is an ideal of R, then the set $R/I = \{r + I : r \in R\}$ forms a ring of the cosets with $+, \cdot$ given by:

  - $(a + I) + (b + I) = (a + b) + I$
  - $(a + I) \cdot (b + I) = ab + I$

  Proof: The addition bit we've already proved because $\langle R, + \rangle$ is an abelian group and $\langle I, + \rangle$ is a subgroup and thus normal. So cosets $r + I$ form and additive group. WTS if $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$, then $(a_1 + I)(b_1 + I) = (a_2 + I)(b_2 + I)$. $x + I = y + I$ iff $x - y \in I$. $a_1 = a_2 + d_a$ for some $d_a \in I$ and $b_1 = b_2 + d_b$ for some $d_b \in I$. $a_1b_1 = (a_2 + d_a)(b_2 + d_b) = a_2b_2 + d_ab_2 + a_2d_b + d_ad_b$.
  $a_1b_1 - a_2b_2 = d_ab_2 + a_2d_b + d_ad_b$, which is a sum of terms in the ideal. So $a_1b_1 + I = a_2b_2 + I$ and therefore coset multiplication is well-defined.
  The last things we need are:

  - Multiplicative identity: $1_R + I$
  - Distributive laws: Just do it.
  - Associativity for multiplication: $((a+I)(b+I))(c+I) = (ab+I)(c+I) = (ab)c+I = a(bc)+I = (a+I)(bc+I) = (a+I)((b+I)(c+I))$. I.e. just do it.

- **Theorem:** An ideal is always a kernel.

  Proof: Take $\phi : R \to R/I$ with $r \mapsto r+I$. Check that ϕ is a ring homomorphism by checking the two requirements. Check that the kernel of ϕ is I.

- Analogies:

  - Groups ↔ Rings
  - Subgroups ↔ Subrings (get properties of the big one for free)
  - Normal subgroups ↔ Ideals (use primarily to make factor groups/rings)

- **First Isomorphism Theorem for Rings:** If $\phi : R \to S$ is a ring homomorphism, then $R/\ker\phi \cong \mathrm{im}\phi$ under the isomorphism $\mu : R/I \to \mathrm{im}\phi$ with $r+I \mapsto \phi(r)$.

  From groups, we already know its bijective and has the additive homomorphism property. We only need to check the multiplicative homomorphism property.

4/16/2015

Maximal ideals

- **Theorem:** If $\phi : R \to S$ is a ring homomorphism, and I is an ideal of $\phi[R]$, then $\phi^{-1}[I]$ is an ideal of R.

  Proof: Already know $\phi^{-1}[I]$ is an additive subgroup of R. We know $\phi^{-1}[I] = \{r \in R : \phi(r) \in I\}$. Need to check our multiplicative property: Let $r \in R$, $x \in \phi^{-1}[I]$. Check $rx, xr \in \phi^{-1}[I]$, i.e. $\phi(rx), \phi(xr) \in I$. $\phi(rx) = \phi(r)\phi(x) \in I$ since $\phi(x) \in I$. So $ax \in \phi^{-1}[I]$. Therefore $\phi^{-1}[I]$ is an ideal in R.

- **Containment Lemma:** Suppose $\phi : R \to S$ is onto. If A and B are ideals in S with $A \subset B$, then their preimages will have the same strict containment, i.e. $\phi^{-1}[A] \subset \phi^{-1}[B]$. Reason: $\phi^{-1}(s)$ is a coset of the kernel. If $s \neq t$, then $\phi^{-1}(t)$ is a different coset. If you have more things in B, then its preimage will have more cosets of the kernel.

- **Definition:** In a ring R, an ideal $M \neq R$ is called maximal if there is no other ideal I such that $M \subset I \subset R$.

  Practically, you often show M is maximal by assuming there exists an ideal I with $M \subseteq I \subseteq R$ and show either $M = I$ or $I = R$.

- **Theorem:** Let R by a commutative ring. Then M is a maximum ideal of R if and only if R/M is a field.

  Proof:

  (⇒) Suppose M is maximal. Then $M \neq R$, so R/M is not trivial. So there exists at least one coset other than $0 + M$ in R/M. WTS R/M is a field:

  ∗ We are given that R/M is a commutative ring and $1+M$ is the multiplicative identity coset.

  ∗ Suppose we have a nonzero coset $x + M$ that doesn't have an inverse. Consider the ideal $I = \langle x + M\rangle = \{(r + M)(x + M) : r \in R\}$. Notice I is not trivial: $x + M \neq 0 + M \in I$ and $1 + M \notin I$ since $(x + M)$ has no inverse so there is no $r \in R$ such that $(r + M)(x + M) = (1 + M)$. We now have that $\{0 + M\} \subset I \subset R/M$. Consider the homomorphism $\phi : R \to R/M$ where $r \mapsto r + M$. Taking the preimages of the above ideals of R/I, by the containment lemma, we have that $\phi^{-1}(0 + M) = M \subset \phi^{-1}[I]$. Since the preimage of an ideal is an ideal, we have that M is not maximal. This is a contradiction, so everything in R/M must have an inverse.

  Therefore R/M is a field.

(⇐) Suppose R/M is a field. We want to show that M is maximal. Suppose for some ideal $I \subseteq R$, $M \subseteq I \subseteq R$. Let's use $\phi : R \to R/M$, $r \mapsto r + M$. $\phi[M] \subseteq \phi[I] \subseteq \phi[R] \Rightarrow \{0 + M\} \subseteq \phi[I] \subseteq R/M$. Since R/M is a field, it has no ideals except $\{0 + M\}$ and itself, so either $\phi[I] = \phi[M] \Rightarrow I = M$ or $\phi[I] = \phi[R] \Rightarrow I = R$.

Prime ideals

- **Definition:** Let R be a commutative ring. Then a proper ideal P is called a **prime ideal** if the following property holds:

  $$ab \in P \implies (a \in P \vee b \in P)$$

  Classic example is $p\mathbb{Z}$ in $\mathbb{Z}$ for some prime p.

- **Theorem:** Let R be a commutative ring and let P be a proper ideal. Then P is prime if and only if R/P is an integral domain.

  Proof: Already know R/P is a commutative ring. So it's an integral domain if and only if it has no zero divisors. It has no zero divisors if and only $(a + P)(b + P) = 0 + P \implies (a + P = 0 + P \vee b + P = 0 + P)$ which happens if and only if $ab \in P$ implies one of $a, b \in P$, that is if P is a prime ideal.

- **Corollary:** In a commutative ring, every maximal ideal is prime. (Important: **prime ideals are not always maximal**)

  Proof: M being maximal implies R/M is a field while implies R/M is an integral domain which implies M is prime.

Principal ideals

- **Definition:** An ideal of the form $\langle a \rangle = \{ar : r \in R\}$ for some fixed $a \in R$ is called a **principal ideal**.

- **Theorem:** In $F[x]$, every ideal is principle.

  Proof: If $I = \{0\} = \langle 0 \rangle$, done. If $I \neq \{0\}$:

  - If I contains a unit u of $F[x]$, $u^{-1}u = 1 \in I$, so $I = F[x] = \langle 1 \rangle$.
  - If I doesn't contain a unit, then let $g(x) \in I$ be an element of smallest degree possible. So $\deg(g(x)) = n \geq 1$. WTS $\forall f(x) \in I$, $f(x)$ is a polynomial multiple of $g(x)$.
    $f(x) = g(x)q(x) + r(x)$. Either $r(x) = 0$ or $\deg r < \deg g$.
    $f(x) \in I$ and $g(x)q(x) \in I$ since $g(x) \in I$. So $f(x) - g(x)q(x) = r(x) \in I$. So either $r(x) = 0$ or $\deg r < \deg g$. But the latter is impossible because we chose

$g(x)$ to have the smallest degree possible in I. So $r(x) = 0$ and so $f(x)$ is a polynomial multiple of $g(x)$. Therefore $I \subseteq \langle g(x) \rangle$. We already know $\langle g(x) \rangle \subseteq I$ because $g \in I$, so $\langle g(x) \rangle = I$.

A ring in which all ideals are principal is called a **principal ideal domain**.

- **Theorem:** A nontrivial ideal $\langle p(x) \rangle$ in $F[x]$ is maximal if and only $p(x)$ is irreducible over F.

  Proof:

  (⇒) Suppose $\langle p(x) \rangle$ is nontrivial and maximal. Consider a factorization of $p(x)$. $p(x) = f(x)g(x)$. WTS one of f, g must be a constant so $p(x)$ is irreducible. $\langle p(x) \rangle$ is maximal and therefore prime. We have $f(x)g(x) = p(x) \in \langle p(x) \rangle$ and therefore at least one of $f(x), g(x)$ is in $\langle p(x) \rangle$, i.e. one of them is a polynomial multiple of $p(x)$. WLOG, say $f(x) \in \langle p(x) \rangle$. Then deg $f \geq$ deg p. But $p(x) = f(x)g(x)$, so it must be that deg $f =$ deg p and deg $g = 0$. Since deg $g = 0$, $g(x)$ is constant and therefore $p(x)$ is irreducible over F.

  (⇐) Suppose $p(x)$ is irreducible over F and I is an ideal with $\langle p(x) \rangle \subseteq I \subseteq F[x]$. WTS either $I = \langle p(x) \rangle$ or $I = F[x]$. Since $F[x]$ is a principal ideal domain, I must be principal, i.e. for some $f(x) \in F[x]$, $I = \langle f(x) \rangle$. We now have $\langle p(x) \rangle \subseteq \langle f(x) \rangle \subseteq F[x]$. $\langle p(x) \rangle \subseteq \langle f(x) \rangle$ means that every multiple of $p(x)$ is also a multiple of $f(x)$. In particular, $p(x) \in \langle f(x) \rangle$. So $p(x) = f(x)q(x)$ for some $q(x) \in F[x]$. Since $p(x)$ is irreducible, one of $f(x)$ or $q(x)$ is constant. If $f(x)$ is constant, it is a unit, so $\langle f(x) \rangle = F[x]$. If $q(x)$ is constant, then $f(x)$ is a multiple of $p(x)$, so $\langle f(x) \rangle \subseteq \langle p(x) \rangle$ and therefore $f(x) = p(x)$.

4/28/2015

Field Extensions

- **Simple extension:** $\mathbb{Q}(\sqrt[13]{127}), \mathbb{Q}(\pi^2)$
- **Algebraic extension:** All $\alpha \in E$ are algebraic over F, i.e. every $\alpha \in E$ is the root of a polynomial in $F[x]$. E.g. $\mathbb{Q}(\sqrt[13]{127}, \sqrt{5}), \mathbb{C}$.
- **Finite extension:** E is a finite-dimensional vector space over F.
- Nonexamples: $\mathbb{R}$ over $\mathbb{Q}$ is not simple, algebraic or finite. $\mathbb{Q}(\pi)$ over $\mathbb{Q}$ is a simple finite non-algebraic extension.
- **Def:** If E over F is a finite extension, then the **degree of E over F** is the size of a basis for E as an F-vector space. Note: when $E = F(\alpha)$, the degree of the extension is $\deg(\alpha, F) = \deg \operatorname{irr}(\alpha, F)$
- **Theorem ("Chain rule for field extensions"):** Say we have a string of field extensions $F \leq E_1 \leq E_2$. Then E_2 is an extension of F and $[E_2 : F] = [E_2 : E_1][E_1 : F]$.

  "Proof" by example: Idea: use bases for the two small extensions to build a basis for the big extension. $\mathbb{Q}(\sqrt[3]{5})(\sqrt{11}) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{11}) \geq \mathbb{Q}(\sqrt[3]{5}) \geq \mathbb{Q}$. $[\mathbb{Q}(\sqrt[3]{5} : \mathbb{Q}] = 3$, and the basis for the extension from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt[3]{5})$ is $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$. $[\mathbb{Q}(\sqrt[3]{5}, \sqrt{11}) : \mathbb{Q}(\sqrt[3]{5})] = 2$ and the obvious basis is $\{1, \sqrt{11}\}$. So the degree of our overall extension should be 6. The resulting basis is $\beta = \{1, \sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{11}, \sqrt{11}\sqrt[3]{5}, \sqrt{11}(\sqrt[3]{5})^2\}$.
- **Def:** A field F is called **algebraically closed** if every polynomial in $F[x]$ has a root in F.

  Example: $\mathbb{C}$.

  The fact that $\mathbb{C}$ is algebraically closed is called the Fundamental Theorem of Algebra. Proving it is very hard and we won't do it here.
- **Def:** The **algebraic closure** E of a field of F is the smallest extension field of F that is algebraically closed. Notated as $E = \overline{F}$.

  E.g. $\overline{\mathbb{C}} = \mathbb{C}$, $\overline{\mathbb{R}} = \mathbb{C}$, $\overline{\mathbb{Q}} = \{\text{the set of algebraic numbers}\}$, $\overline{\mathbb{Z}_p}$ is something really weird.
- **Theorem:** Every field has an algebraic closure. This is also hard to prove and we won't do it.
- **Theorem:** A field F is algebraically closed if and only if every polynomial in $F[x]$ factors into linear factors.

  Proof:

($\Leftarrow$) Assume all polynomials in $F[x]$ factor into linear factors. WTS F is algebraically closed, i.e. every nonconstant polynomial has a root in F. Let $f(x) \in F[x]$. By assumption, it can be factored into linear factors. Let $(ax - b)$ be one of the linear factors. Then b/a is a zero in F.

($\Rightarrow$) Assume every nonconstant polynomial in $F[x]$ has a root in F. Let $f(x) \in F[x]$ have degree n. By assumption, we know it has at least one root, r_1. So we can factor $(x - r_1)$ out of $f(x)$. So $f(x) = f_1(x)(x - r_1)$ for some degree-$(n - 1)$ polynomial $f_1(x)$. Simple induction argument from here.