MATH 369 Fall 2025 - Class Notes

11/17/2025

Scribe: Brooke McConnell

Summary: This class we talked about a few definitions and proved a few theorems. Mostly involving integral domains.

Definition. A ring D is a **domain** if it has no zero divisors and $0 \neq 1$.

Definition. An **integral domain** is a commutative ring that is a domain.

Definition. A **division ring** (or sometimes a **skew field**) is a domain in which every nonzero element is a unit (multiplication isn't necessarily commutative).

Example. Hamiltonians:
$\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}$
$1, i, j, k$ are as in the Quaternion Group.
$i^2 = j^2 = k^2 = -1$
$(2 + 3i)(1 - 2j)$ in $\mathbb{H}$
$= 2 - 4j + 3i - 6(ij)$
$= 2 - 4j + 3i - 6k$
(1-2j)(2+3i)
$= 2 - 4j + 3i - 6(ji)$
$= 2 - 4j + 3i + 6k$
This is not commutative.
$\mathbb{H}$ is a division ring that is not a field.
$\mathbb{H}[x]$ (polynomials over $\mathbb{H}$) form a domain that is not an integral domain.

Theorem. Any subring of a field is an integral domain.

Proof. Suppose F is a field and $D \subseteq F$ is a subring of F. Then D is a ring. $0 \neq 1$ in D since $0 \neq 1$ in F and by the definition of a subring the 0 and 1 of D are the same as in F. Suppose that $a, b \in D, ab, \neq 0$ then $a, b \in F$ has no zero divisors so $a, b \neq 0$ in D as well. Thus D is an integral domain. □

Example. $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$- Gaussian integers form an integral domain since they are a subring of $\mathbb{C}$.

Theorem. D is an integral domain iff D[x] is an integral domain.

Proof. Backwards direction: Suppose D[x] is an integral domain, then $1 \neq 0$ pick $a, b \in Da, b \neq 0$ then $a, b \in$ D[x] (constant polynomials) then $ab \neq 0$ in D[x] (since it is an integral domain) ab is a constant so it is in D so $ab \neq 0$ in D.

Forwards direction: Suppose D is an integral domain then $0 \neq 1$ in D so $0 \neq 1$ in D[x] as well. Now suppose $g(x), h(x) \in$ D[x] both nonzero then $g(x) = a_n x^n + ..., h(x) = b_m x^m + ...$ where $a_n \neq 0$ and $b_m \neq 0$. Then $g(x)h(x) = a_n b_m x^{n+m} + ...$ where $a_n b_m \neq 0$ since both aren't zero and are elements of D. So $g(x)h(x) \neq 0$ as well. □

$\mathbb{Z}$ is an integral domain, $\mathbb{Z}[x]$ is an integral domain. $(\mathbb{Z}[x])[y]$ is an integral domain polynomials in y whose coefficients are in $\mathbb{Z}[x]$.
Note: $\mathbb{Z}_n$ is <u>not</u> an integral domain if n is composite since if $n = cd$ then $[c]_n[d]_n = [0]_n$. $\mathbb{Z}_n$ is only an integral domain if n is prime in which case $\mathbb{Z}_n$ is a field.

Theorem. Every finite integral domain is a field.

Proof. Suppose D is an integral domain that is finite. To prove that D is a field we just have ti show every nonzero element has an inverse. Let $b \in D, b \neq 0$. Let $D^* \subseteq D$ be the set of nonzero elements in D. Define $f : D^* \to D^*$ by $f(x) = b(x)$. Note the image is in D^* since D has no zero divisors. Claim: $f(x)$ is one-to-one. Suppose $f(x) = f(y), bx = by$. Even without inverses we have the cancellation property for multiplication in Rings. So $x = y$. So $f(x)$ is one-to-one. Since $f(x)$ is one-to-one on $D^* \to D^*$ it is also onto, $f(x)$ is a bijection so there exists a $c \in D^*$ such that $f(c) = 1$. Then $bc = 1$ then $c = b^{-1}$ so b is a unit in D. So every nonzero $b \in D$ has an inverse and D is a field. □

Theorem. (Wedderburn) Every finite division ring is a field.

Definition. Suppose R and S are commutative rings then $\phi : R \to S$ is a <u>ring homomorphism</u>
If: for every $a, b \in R$
1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$
3. $\phi(1_R) = 1_S$
D is an isomorphism if it is also bijective and it is an automorphism if its and isomorphism from R to R.

Example. $\phi : \mathbb{Z} \to \mathbb{Z}_n, \phi(a) = [a]_n$.
1. Homomorphism of groups under addition
2. $\phi(ab) = [ab]_n = [a]_n[b]_n = \phi(a)\phi(b) = \phi(1) = [1]_n$.
Is a homomorphism of rings.

Proposition. If ϕ is a homomorphism $\phi : R \to S$
a) $\phi(0_R) = 0_S$ (preserves additive identity)
b) $\phi(-a) = -\phi(a)$ (preserves additive inverses)
c) $Im\phi \subseteq S$ is a subring of S

Proof. (a) and (b) follow from the fact that ϕ is a homomorphism of additive groups. (c) $Im\phi$ is a subgroup of S under addition since ϕ is a homomorphism of groups.

$Im\phi$ is closed under multiplication. Suppose $a, b \in Im\phi$. Goal: Show $ab \in Im\phi \exists r, s \in R$ such that $\phi(r) = a, \phi(s) = b$ then $\phi(rs) = \phi(r)\phi(s) = ab$ and $\phi(rs) \in Im(\phi)$ so closed under multiplication. Finally $1_S \in Im\phi$ since $\phi(1_R) = 1_S \in Im\phi$ so $Im\phi$ is a subring of S. $\square$

Example. Evaluation homomorphism
Define $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{R}$ by $\phi_\alpha(f(x)) = f(\alpha)$. This is a homomorphism since $\phi(f+g) = (f+g)(\alpha) = \phi(f) + \phi(g)$ and $\phi(fg) = (fg)(\alpha) = \phi(f)\phi(g)$ and $\phi(1) = 1$
More concrete example:
$\alpha = \sqrt{2}, \phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}, f(x) \to f(\sqrt{2})$ is a homomorphism. So $Im\phi_{\sqrt{2}} \subseteq \mathbb{R}$ is a subring of $\mathbb{R}$, what is this image?
$f(x) = a_n x^n + a_{n-1}x^{n-1} ... a_0$
$f(\sqrt{2}) = a_n 2^{n/2} + a_{n-1}\frac{n-1}{2} + ... a_n = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. So $Im\phi_{\sqrt{2}} = \mathbb{Q}(\sqrt{2})$.

What are the $f(x) \in \mathbb{Q}[x]$ where $\phi_{\sqrt{2}}(f) = 0$? Then $\sqrt{2}$ is a root of f(x) so $(x - \sqrt{2})$ is a factor of f(x) $(x - \sqrt{2})$ is not in $\mathbb{Q}[x]$. Every such polynomial in $\mathbb{Q}[x]$ is a multiple of $x^2 - 2$. (Note the set of multiples of $x^2 - 2$ are the kernel of $\phi_{\sqrt{2}}$.

Example. Let $c \in \mathbb{Z}$ then $\phi_c : \mathbb{Z}[x] \to \mathbb{Z}[x]$ given by $\phi_c(f) = f(x+c)$ is an isomorphism of rings. The inverse of this isomorphism os $\phi_c^{-1} = f(x) \to f(x-c)$.