Commutative Algebra MATH 502

Thanic Nur Samin

Class 1: 01/08

Algebraic Geometry	Commutative Rings
k^n	$k[x_1, \ldots, x_n]$
point $(p_1, \ldots, p_n)$	maximal ideal $(x_1 - p_1, \cdots, x_n - p_n)$
varities	ideals in $k[x_1, \ldots, x_n]$
Some shape defined by $F = 0$	$k[x_1, \ldots, x_n]/(F)$

Table 1: Relationship between Algebraic Geometry and Commutative Rings

ED $\implies$ PID $\implies$ UFD

Theorem 1. Gauss Lemma: A UFD $\implies$ $A[X]$ UFD

Definition 1. Ring is a five-tuple $(A, +, \cdot, 0, 1)$

- A is a set.
- $0, 1 \in A$
- $+ : A \times A \to A : (x, y) \mapsto (x + y)$
- $\cdot : A \times A \to A : (x, y) \mapsto xy$
- $(A, +, 0)$ abelian group
- $(xy)z = x(yz)$ associativity
- $(x + y)z = xz + yz$ distributivity
- $x(y + z) = xy + xz$ distributivity
- $x1 = 1x = x$

A is commutative if $xy = yx$, in this course all rings are commutative.

Example 1 (Commutative Rings)**.** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_{p^r}, A[x], A/I, \text{Frac}(A)$

Definition 2. A homomorphism is a function $f : A \to B$ so that,

$$\begin{aligned} f(x + y) &= f(x) + f(y) \\ f(xy) &= f(x)f(y) \end{aligned}$$

Definition 3. A subring R of a ring A is a subset so that $(R, \cdot, +, 0_A, 1_A)$ is a ring.
$x, y \in R \implies x + y, xy \in R$ which means R is 'closed' under the operations.
$\mathbb{Z}$ is an initial ring. This means, for all ring A, there exists a unique ring homomorphism $\mathbb{Z} \to A$ that sends $1_Z \to 1_A$

Definition 4. An ideal I of A is a subset so that $(I, 0, +)$ is an abelian group and $AI \subseteq I$.
So we have, $0 \in I, x \in A, y \in I \implies xy \in I, x, y \in I \implies x + y \in I$

Example 2. Are all subrings ideals? NO
Are all ideals subrings? NO

$I \triangleleft A$ means I is an ideal. This gives an equivalence relation on A.
$a \sim a' \iff a + I = a' + I \iff a - a' \in I$
$[a] = a + I$ equivalence classes.
$\{a' | a' \sim a\}$

Definition 5. Quotient ring A/I is defined by $[x] + [y] \coloneqq [x + y], [xy] \coloneqq [x][y]$

$A \to A/I$ is a ring homomorphism with $\ker = I$
$f : A \to B$ is a ring homomorphism. This implies:

- $f(A)$ is a subring of$B$
- $\ker f \triangleleft A$
- $A/\ker f$ is isomorphic to A/I

Definition 6. For a ring A, an element $x \in A$ is an unit of there exist y so that $xy = 1$.
$A^\times$ is the group of units.
For example, $\mathbb{Z}^\times$ is the cyclic group of order 2.

Definition 7. $x \in A$ is a zero divisor if there exists nonzero y so that $xy = 0$.

We have units, zero divisors and other elements.

Ring	Zero divisors	units	nonzerodivisors
$\mathbb{Z}/6\mathbb{Z}$	[0],[2],[3],[4]	[1],[5]	
$\mathbb{Z}$	[0]	[1],[-1]	[2],[-2],...

Table 2: Units and Zero divisors

Definition 8. A is a domain if the only zero divisor is zero. For example, fields, subrings of domain, $\mathbb{Z}[\sqrt{5}]$ etc.

If A is a domain then there exists $\mathrm{Frac}(A)$, the field of fractions.
Now, suppose A is a subring of B. let $\beta \in B$.

Definition 9. $A[\beta]$ = smallest subring of B containing A and β
$= \{f(\beta) | f(x) \in A[x]\}$
We have $ev : A[x] \to A[\beta]$ given by $x \mapsto \beta$

Class 2: 01/10
Let A be a domain. This means $xy = 0 \implies x = 0$ or $y = 0$
Key property: Domain implies cancellation
$xy = xz, x \neq 0 \implies y = z$ as $xy = xz \implies xy - xz = 0 \implies x(y - z) = 0 \implies y - z = 0 \implies y = z$

Definition 10. ED, Euclidean Domain is a domain with extra condition: a function $f : A - \{0\} \to \mathbb{Z}_{>0}$ so that for all $a \in A - 0, b \in A$ we have $b = aq + r$ with either $r = 0$ or $f(r) < f(a)$.
Alternative formulation (Dummit and Forte) we can have $f(0) = 0$. Also in some formulation $f(0) = -\infty$.

Example 3. if A is a field then f can be anything since $r = 0$ always. We take const.
For $\mathbb{Z}$ we have $f(x) = |x|$.
In $k[x]$ we have $f(p(x)) = \deg p(x)$
Note that $\mathbb{Z}[x]$ is not an ED.
$\mathbb{Z}[i]$ is an ED. $f(a + ib) = a^2 + b^2$
Lorentz polynomials $k[x, x^{-1}]$ is an ED.
$f(ax^m + \cdots + bx^{-n}) = m + n$

Definition 11. $I \triangleleft A$ is principal if there exists $a \in A$ so that $I = (a) \coloneqq Aa$

A domain A is a PID (Principal Ideal Domain) if all ideals are principal.

Theorem 2. $ED \implies PID$

Proof. Suppose $0 \neq I \triangleleft A$ and (A, f) is ED.
Choose $a \in I$ so that $f(a) = \min f(I - 0)$
for all $b \in I$ we have $b = aq + r$ where $r \in I$. We must have $f(r) \geq f(a)$ which means $r = 0$ and thus $b \in (a)$.

□

Note that $\mathbb{Z}[x], \mathbb{C}[x, y]$ are not PID and thus they are not EDs.

Theorem 3. By Gauss. Every $n \in \mathbb{Z} - 0$ factors into $n = \pm p_1 \cdots p_n$ primes unique upto reordering.

We generalize this.

Definition 12. $x \in A$ is irreducible if $x \neq 0, \notin A^\times$ and $x = ab \implies a \in A^\times$ or $b \in A^\times$.
$x \in A$ is prime if $x \neq 0, \notin A^\times, x \mid ab \implies x \mid a$ or $x \mid b$
$x, y \in A$ are associates if $x = yu$ where $u \in A^\times$.

Definition 13. A domain A is a UFD (unique factorization domain) if for any nonzero nonunit $x \in A$ then:
1. $x = p_1 \cdots p_r$ where p_j are irreducibles
2. Decomposition is unique upto reordering and associates.
This means if $p_1 \cdots p_n = q_1 \cdots q_m$ then $m = n$ and there is a permutation σ of indices and units $u_i \in A^\times$ so that $p_i = q_{\sigma(i)} u_i$

Theorem 4. All PIDs are UFDs.

Proof. Assume A is a PID. Let $x \in A - 0, x \notin A^\times$
First we prove existence (1).
If x is irreducible then we're done. If it is not, then since it is reducible we have $x = x_1 x_2$. If x_1, x_2 are both irreducible then we're done. Otherwise x_1 or x_2 is reducible. WLOG x_1 is reducible. Then $x = x_{11} x_{12} x_2$. We continue. After reordering we have an infinite chain of ideals $(x) \subsetneq (x_1) \subsetneq (x_{11}) \subsetneq (x_{111} \subsetneq)$.
We claim that this terminates. Suppose otherwise.
Then there exists an ∞ number of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$
Take $I = \bigcup_{i=1}^{\infty} I_i$. This is an ideal, but $I = (x)$. $x \in I_n$ for some n which means $I_n = I_{n+1} = \cdots$ so there can't be any infinite ascending chain and thus we're done with te existence.
[Take the tree. If it's unbounded by AOC we have an infinite chain. If x is not a finite product of irreducibles then we have an infinite chain.]
Reread Dummit and Forte.
Lemma: in a domain prime $\implies$ irreducible, and in a PID prime $\iff$ irreducible.
We use this.
$p_1 \cdots p_n = q_1 \cdots q_m$
$p_1 | q_1 \cdots q_m$ implies $p_1 | q_i$ for some i. Reorder so that $p_1 | q_1$. Then $q_1 = p_1 u$. Since q_1 is irreducible u is a unit.
Now we have $p_2 \cdots p_n = u q_2 \cdots q_m$. We keep going for the proof.

□

Class 3: 01/12
Today we prove A UFD $\implies A[x]$ UFD
Monday MLK day, Wednesday explicit Galois Theory $\mathrm{Ga}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ and $\mathrm{Ga}(\mathbb{Q}(\xi_n)/\mathbb{Q})$.
Recall that A is a UFD (Unique Factorization Domain) if A is a domain and every $x \in A - (0 \cup A^\times)$ is a product of irreducibles and this factorization is unique upto reordering and multiplication by units.
Notation: $x \overset{\bullet}{=}$ means x, y are associates, aka $x = yu$ where $u \in A^\times$
Two nice properties of UFD:

- prime $\iff$ irreducible

- gcd and lcm exists

Proposition 1. If A is a UFD, $x \in A$ is non-unit and non-zero, then x prime $\iff$ x is irreducible.

Proof. $\implies$
Suppose x is a prime. Assume x is not irreducible. If $x = ab$ we have, $x|ab$ which implies $x|a$ or $x|b$.
WLOG, $x|a$. Then we have $a = xy$.
So, $x = ab = xyb \implies yb = 1 \implies b \in A^\times$
So x is indeed irreducible.
[Note that this is true for arbitrary domains]
$\impliedby$
Assume x is irreducible. If $x|ab$, we have $ab = xy$
The uniqueness of factorization implies x is a factor of a and b. So x is a prime.
[We need uniqueness for this]

□

Definition 14. GCD. First, d is a common divisor of a and b if $d|a$ and $d|b$. Equivalently, $(a), (b) \subset (d)$. To contain is to divide.
d is a gcd of a and b if d is a common divisor and for any other common divisor d', we have $d'|d$ ir $(d) \subset (d')$. In other words, (d) is the unique minimal principal ideal so that $(a), (b) \subset (d)$

In a general ring, it may or may not exist. But in a UFD, gcd's exist and unique upto multiplication by units.
$\forall a, b \in A$, if d, d' are $\gcd(a, b)$ then $d \overset{\bullet}{=} d'$.
So, $2, -2 = \gcd(4, 6)$
Formula for gcd:
$a = up_1^{e_1} \cdots p_r^{e_r}$
$b = vp_1^{f_1} \cdots p_r^{f_r}$
Where $u, v \in A^\times$, p_j are distinct primes and $e_i, f_i \geq 0$
Thus, $\gcd(a, b) = p_1^{\min(e_i, f_i)} \cdots p_r^{\min(e_r, f_r)}$
Now, we prove that,

Theorem 5. A is a UFD $\implies$ $A[x]$ is a UFD

Note that, if A is a domain, then $A[x]$ is a domain.
Proof is an exercise. Just work through the coefficients.
For the rest of the class, assume A is a UFD. Our canonical example is $A = \mathbb{Z}$. Note that $\mathbb{Z}[x]$ is not a PID.

Definition 15. A polynomial $f(x) = \sum_{j=0}^{n} a_{n-j}x^{n-j} \in A[x]$ is primitive
if $\gcd(a_n, \cdots, a_1, a_0) = 1$.

Theorem 6. Gauss' Lemma: Suppose $f, g \in A[x]$ are primitive. Then fg is primitive.

Proof. Note that, $h \in A[x]$ is primitive $\iff$ $\forall$ prime p of A, $\overline{h} \neq 0 \in A[x]/(p) = (A/p)[x]$ $\iff$ $\forall$ prime $p, p \nmid \gcd(a_n, \ldots, a_0)$
Now, since f, g are primitive, $\overline{f}, \overline{g} \neq 0 \in (A/p)[x]$. Note that $(A/p)[x]$ is a domain.
Now, $\overline{f}\overline{g} = \overline{fg} \neq 0 \in (A/p)[x]$ and thus fg is primitive.

□

Definition 16. Suppose $f \in A[x]$ Then, the content $c(f)$ is the gcd of the coefficients $\gcd(a_n, \cdots, a_0)$.

Note that $\frac{1}{c(f)}f$ is primitive.
Also, $\forall f, c$ we have $\frac{f}{c} \in A[x]$ is primitive $\iff$ $c \overset{\bullet}{=} c(f)$
Note that division doesn't always make sense in a ring. $\frac{x}{y}$ means if $x = yq$ then $q = \frac{x}{y}$
A corollary of Gauss' Lemma: Applying Gauss' Lemma to non-primitive polynomial gives us $c(fg) \overset{\bullet}{=} c(f)c(g)$

Proof. $\frac{1}{c(f)}f, \frac{1}{c(g)}g$ are primitive, which means $\frac{1}{c(f)c(g)}fg$ is primitive. This implies $c(f)c(g) \overset{\bullet}{=} c(fg)$ □

Suppose A is a domain. Let $k = \text{Frac}(A)$. EG $\mathbb{Q} = \text{Frac}(\mathbb{Z})$
(i.e. $A \subset k$ field, $\forall x \in k^\times, x = \frac{a_1}{a_2}$ where $a_1, a_2 \in A$)
For $f \in k[X]$ we define $c(f) \in k^\times$ by $\frac{f}{c(f)} \in A[x]$ is primitive.
Corollary of Gauss Lemma: $\forall f, g \in k[x]$ we have $c(fg) = c(f)c(g)u$ where $u \in A^\times$
Finally we prove our theorem.

Proof. "Existence": Suppose $0 \neq h \in A[x]$.
We can write $h = c(h)f$ where f is primitive.
Factor $c(h) = p_1 \cdots p_k$ as product of primes in A.
Factor $f = f_1 \cdots f_r$ as a product of irreducible in $k[x]$ since $k[x]$ is an Euclidean Domain.
We say that $h = p_1 \cdots p_k \frac{f_1}{c(f_1)} \cdots \frac{f_r}{c(f_r)}$
Since f_j is irreducible in $k[x] \implies \frac{f_j}{c(f_j)}$ is irreducible in $A[x]$

□

Addendum from me: Suppose primitive $f \in A[x]$ such that $f = g'h'$ in the field of fractions. Then, $f = \frac{g}{u}\frac{h}{v} \implies fuv = gh$. So, $c(g)c(h) = c(gh) = c(fuv) \overset{\bullet}{=} uv$. So $f = \frac{g}{c(g)}\frac{h}{c(h)}$

Class 04: 01/17
We have A UFD $\implies$ A[x] UFD
We use Gauss lemma and k[x] UFD.
Since we have $A[x][y] = A[x, y]$ by induction we have A UFD implies $A[x_1, \ldots, x_n]$ is a UFD.
We give a geometric definition.

Definition 17. A variety $V \subset k^n$ is the zero set of $\{f_\alpha\} \subset k[x_1, \ldots, x_n]$

For example, if $f = x_1x_2$ then the variety is the axes in euclidean space [insert pictures]
We actually have a correspondence between varieties in k^n and ideals I of $k[x_1, \ldots, x_n]$
$V \mapsto I(V) = \{f \in k[x_1, \ldots, x_n] | f(V) = 0\}$
On the other hand $V(I) = \{\underline{x} \in k^n | \forall f \in I, f(\underline{x}) = 0\}$
Is it a bijection? No, $V(x) = V(x^2)$ but $(x) \neq (x^2)$
Is $I(v)$ finitely generated? Yes, by a theorem of Hilbert
If so is it by $\leq n$ polynomials? by $\leq n$ irreducible polynomials?
Is $V =$ union of irreducible varieties uniquely?
There are a lot of connections between algebraic geometry and ring theory.

Explicit Galois Theory

eg. $\mathbb{F}_{p^r}/\mathbb{F}_p \simeq \mathbb{Z}/r$ with correspondence between $x \mapsto x^p$ and 1
eg, $\mathbb{Q}(\xi_n)/\mathbb{Q} \simeq \mathbb{Z}/n$ with correspondence between $\xi_n \mapsto \xi_n^k$ and k

Field Extensions

Suppose $0 \neq f \in k[x]$
1. $\exists K$ such that f has a root in K
2. $f(\alpha) = 0$ for some $\alpha \in K$ then the ring $k[\alpha]$ is a field
3. $f(x)$ has at most $\deg f$ roots in k
For proof of 1: Let f_1 be irreducible factor of f.
Then, $K = \frac{k[x]}{(f_1(x))}$, so $x + (f_1(x))$ is a root of f_1 and thus f.
2. Let $\beta \neq 0$ be an element of $k[\alpha]$
Then, $\cdot\beta : k[\alpha] \to k[\alpha]$
It is injective since $k[\alpha]$ is a domain

$\dim_h k[\alpha] \leq \deg f$
So it must be surjective and thus 1 is in the image.
3. α is a root iff $x - \alpha | f$ then induct.

Definition 18. Splitting Fields (Definition 13.4): K/k is a splitting field for nonzero $f \in k[x]$ if $f(x) = a\prod(x - \alpha_i) \in K[x]$
K—-E—-k $\implies$ does not split in E
For example, $\mathbb{Q}[\sqrt{2}]$ is splitting field for $x^2 - 2$ but $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field for x^{3-2}. We need $\mathbb{Q}(\sqrt[3]{2}, \xi_3)$.

We define $\xi_n = e^{2\pi i/n}$ as the primitive root of 1

Theorem 7. $f(x) \in k[x]$.
1. There exists splitting field K/k for $f(x)$
2. If K/k and L/k are splitting fields for f then there exists $\phi : K \to L$ such that $\phi|_k = Id_k$

Proof uses observation and induction on $\deg f$
Application 1:
Algebraic Closure:

Definition 19. A algebraic closure $\overline{k}$ over a field k is $\overline{k}/k$ such that $\alpha \in \overline{k}$ is algebraic over k which means $\exists f(x) \in k[x]$ that is nonzero and $f(\alpha) = 0$ and also every nonzero $f \in k[x]$ has a root $\alpha \in \overline{k}$

Theorem 8. Suppose k is a field. Then,
1: There exists an algebraic closure $\overline{k}/k$
2: If there are two algebraic closures of k then there is an isomorphism which restricted to k is the identity.

Proof: Zorn's lemma
k is algebraically closed if $\overline{k} = k$
Which means every polynomial has a root.
$\overline{k}$ is algebraically closed which means $\overline{\overline{k}} = \overline{k}$
$\mathbb{C}$ is algebraically closed by Gauss Fundamental theorem of Arithmetic.
We have $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$
$\overline{Q}$ is countable and algebraically closed.
$\overline{\mathbb{F}_p} = \cup\mathbb{F}_{p^r}$
Application 2 of splitting field is to finite fields.
Let p be a positive prime number.
$\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$
It is a field.
Suppose F is a finite field.
So, we have, $|F| > 1$ from the definition $1 \neq 0$
There exists a unique prime p so that $p1_F = 0_F$
Proof: Consider the map $\mathbb{Z} \to F$ that sends $1 \to 1_F$. The kernel is $n\mathbb{Z}$. So, the domain $\mathbb{Z}/n\mathbb{Z}$ has an injective homomorphism to F which means n is a prime
$\text{char}(F) = p$ means in F field, $p1_F = 0_f$
Now, $\mathbb{F}_p$ has injective homomorphism to F (sends $1 \to 1$) So we have F is a vector space over $\mathbb{F}_p$ so we have $\dim_{\mathbb{F}_p} = r$

Class 05: 01/19

Finite Fields and Galois Theory

Suppose F is a field and $\text{char}(F) = p \implies p1 = 0$.

Definition 20. Frobenius Endomorphism: $\sigma : F \to F$ given by $\sigma(x) = x^p$

Proposition 2. σ is a field morphism.

Proof. $\sigma(1) = 1, \sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$
$\sigma(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} x^k = x^p + y^p$ since $\binom{p}{k}$ is divisible by p for $1 \leq k \leq p-1$ and hence 0 in F since $\text{char}(F) = p$
Also, $\ker \sigma \triangleleft F$ but F is a field which means σ is $1-1$ aka injective
Also $|F| < \infty \implies \sigma(F) \simeq F$

□

Consider the field of fractions $\mathbb{F}_p(t) = \text{Frac}(\mathbb{F}_p[t])$ then we have $\sigma(t) = t^p$, then σ is not onto as $t \notin \text{im}\, \sigma$
Let F be a finite field. Last time we showed $\text{char}\, F = p$ and $|F : \mathbb{F}_p| = \dim_{\mathbb{F}_p} F = r$

Proposition 3. Let $q = p^r$. Then,

- $\exists$ field of order q
- $|F| = q \implies F$ is splitting field of $x^q - x$
- If $|F| = q = |K|$ then $F \simeq K$

Proof. For 1: Let E be a field where $x^q - x$ splits. Let $f(x) = x^q - x$. We claim that f has distinct roots. One way to look at it is $\gcd(f, f')$. Then, $\gcd(x^q - x, qx^{q-1} - 1) = \gcd(x^q - 1, -1) = 1$ since we are working modulo p and thus $q = 0$. This implies f has q distinct roots in E.
Let $F = E^{\sigma^q} = \{x \in E : \sigma^r(x) = x\} = \{x \in E : f(x) = 0\}$
Then $|F| = q$
We claim that F is a field. We have multiplication and inverse easily. If $\alpha, \beta \in F$ then $(\alpha + \beta)^q = \alpha^q + \beta^q$ [Freshmen's dream] so we have addition too so we have proved that F is a field.
For 2: If F is a field of order q then for $x \in F^\times$ since $|F^\times| = q - 1$ we have $x^{q-1} = 1 \implies x^q - x = 0$, and this is also true for $x = 0$. So, $x^q - x = \prod_{\alpha \in F}(x - \alpha)$ and thus F must be a splitting field.
For 3: Splitting fields are unique.

□

Note that $\mathbb{F}_{p^r}$ means any field of order p^r. All such fields are isomorphic, but there isn't any canonical 'god given' construction of $\mathbb{F}_{p^r}$
Warning: $\mathbb{F}_{p^r} \not\simeq \mathbb{Z}/p^r$
There's another basic fact.

Proposition 4. $\mathbb{F}_p^\times$ is cyclic.

In Dummit and Foote there's a more general fact: $\forall$ field F , any finite subgroup A of $F^\times$ is cyclic. This lemma directly implies the above proposition.

Proof. This uses the third observation from last time. Let $n = |A|$ and let $d = \exp A = \max\{\text{ord}\, a | a \in A\}$. This must divide n.
Then, $x^d - 1$ has n roots [namely the elements of A] which means $d \geq n$ but also $d|n$ so $d = n$ which means A is cyclic.

□

Corollary: $\mathbb{F}_{p^r}/\mathbb{F}_p$ is primitive, i.e. $\mathbb{F}_{p^r} = \mathbb{F}_p[\theta]$ for some θ and $\langle\theta\rangle = \mathbb{F}_q^\times$
Corollary: $\forall r \geq 1, \exists$ irreducible polynomial $h(x)$ of degree r
For this, $h(x)$ is just the minimal polynomial of θ
So $\mathbb{F}_{p^r} \simeq \frac{\mathbb{F}_p[x]}{(h(x))}$
Review of Galois Theory:
Suppose L/K is a finite extension of field.
Then $\text{Aut}(L/K) = \{\sigma : L \to L$ isomorphisms so that $\sigma|_K = Id_K\}$

Definition 21. L/K is Galois if $|\,\text{Aut}(L/K) = |L : K||$

For example, $\mathbb{Q}(\sqrt{2})/Q$ is Galois but for $\sqrt[3]{2}$ it's not.

Definition 22. If L/K is Galois, define,
$\mathrm{Gal}(L/K) \coloneqq \mathrm{Aut}(L/K)$

Theorem 9. Fundamental Theorem of Galois Theory: Suppose L/K is Galois. Then the map of subgroups of $\mathrm{Gal}(L/K)$ to fields E such that $L-E-K$ given by $H \mapsto L^H$ is a bijection.

Back to finite fields: $\sigma(x) = x^p$
Then $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^r}/\mathbb{F}_p)$
Since $\mathbb{F}_q^\times$ is cyclic, $\mathrm{ord}\,\sigma = r$
So, $\sigma^r = Id$
This means $r = |\mathbb{F}_{p^r} : \mathbb{F}_p| \geq \mathrm{Aut}(\mathbb{F}_{p^r}/\mathbb{F}_p) \geq r$
So, $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) = \langle\sigma\rangle \simeq \mathbb{Z}/r$
Corollary: For $d|r, \exists!$ **su** ield F of $\mathbb{F}_q$ of order p^d
For assignment, we were supposed to analyze the lattice.
Given $\mathbb{F}_{p^{n_1}}, \mathbb{F}_{p^{n_2}}$ we can embed in $\mathbb{F}_{p^{n_1 n_2}}$
Note:
$\mathrm{Gal}(\mathbb{F}_{p^n})/\mathbb{F}_p \cong \mathbb{Z}_N$ and the geneeratoris the frobnius map $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $\sigma(a) = a^p$
This is true because $a^{p^n} = a$

Class 06: 01/22
We start on Atiyah MacDonald on wednesday.
Finite Field Definition: 13.5+14.3
Cyclotomic FIeld Definition: 13.6+14.5

Finite Fields	Cyclotomic
$\mathbb{F}_{p^n}$	$\mathbb{Q}(\zeta_n)$
Splitting Field of $x^{p^n} - x$	Minimal Polynomial Φ_n
$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n$ with $a \mapsto a^{p^k}$	$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n^\times$ with $\zeta_n \mapsto \zeta_n^k$

Table 3: Finite vs Cyclotomic Fields

Let $\zeta_n = e^{2\pi i/n}$
Let $\mu_n = \{\zeta \in \mathbb{C}^\times : \zeta^n = 1\} < \mathbb{C}^\times$
Then $\mu_n = \langle\zeta_n\rangle$ and is cyclic of order n

Definition 23. n th cyclotomic polynomial:

$$\Phi_n(x) = \prod_{\text{primitive } \zeta \in \mu_n} (x - \zeta) = \prod_{0<a<n,(a,n)=1} (x - \zeta_n^a)$$

Note: $\deg \Phi_n = \phi(n)$ by definition.

Also: $X^n - 1 = \prod_{d|n} \Phi_d(X)$

This gives us a recursive formula for cyclotomic polynomials:

$$\Phi_n(x) = \frac{x^{n-1}}{\prod_{d|n, d\neq n} \Phi_d(x)}$$

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$

Table 4: Cyclotomic Polynomials

Corollary: $\Phi_n(x) \in \mathbb{Q}[x]$
Corollary of Gauss' Lemma:
Suppose R is a UFD. Let $k = \text{Frac}(R)$. Then $f(x) = g(x)h(x)$ in $k[x]$ with f, g, h monic and $f(x) \in R[x]$ then $g, h \in R[x]$
We can use this to show that all the Φ_n are monic.

Proof. Since g, h are monic, we can find $d, e \in R$ so that $dg(x), eh(x) \in R[x]$ and they are primitive [d, e are lcm of numerators.]
Then, $def(x) = [dg(x)][dh(x)]$, but $def(x)$ and $f(x)$ are both primitive which can only happen if de is a unit aka d, e are both units. So $g(x), h(x)$ are both primitive in $R(x)$

□

This proves that all the Φ_n are integer polynomials.
Lemma: $\Phi_n(x)$ are irreducible in $\mathbb{Q}[x]$
This actually implies $|\mathbb{Q}(\zeta_n) : \mathbb{Q}| = \phi(n)$

Proof. Due to Dedekind.
Suppose $\Phi_n(x) = f(x)g(x)$ with f, g both monic.
With f irreducible, $\deg f > 0$
Now, by corroloary of Gauss Lemma, $f, g \in \mathbb{Z}[x]$
Claim: Suppose p is a prime, $p \nmid n$ and ζ is a primitive n th root of unity and $f(\zeta) = 0$.
Then, $f(\zeta^p)$
Proof of Claim by contradiction:
Note that, $\Phi_n(\zeta^p) = 0$. Suppose $g(\zeta^p) = 0$
Since f is irreducible it is the minimal polynomial of ζ so we have $f(x) \mid g(x^p)$. Then, $g(x^p) = f(x)h(x)$
Consider $\pmod p$ which gives us $\overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$
Now, $\overline{g}(x)^p = \overline{g}(x^p) \mid \overline{f}(x) \mid x^n - 1$
But $x^n - 1$ has no multiple factor in $\mathbb{F}_p(x)$ [formal derivative trick.]

□

Class 07: 01/24
Recall:

Finite Fields	Cyclotomic
$\mathbb{F}_{p^n}$	$\mathbb{Q}(\zeta_n)$
Splitting Field of $x^{p^n} - x$	Minimal Polynomial Φ_n
$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n$, $k \mapsto (a \mapsto a^{p^k})$	$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n^\times$, $k \mapsto (\zeta_n \mapsto \zeta_n^k)$

Table 5: Finite vs Cyclotomic Fields

Yesterday:

$$\Phi_n(x) = \prod_{\text{primitive } \zeta \in \mu_n} (x - \zeta) = \prod_{(a,n)=1, 0 \le a < n} (x - \zeta_n^a)$$

That gave us:
$\deg \Phi_n(x) = \phi(n)$
$x^n - 1 = \prod_{d|n} \Phi_d(x)$
$\Phi_n(x) = \dfrac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)} \in \mathbb{Q}[x]$
Gauss Lemma:
$f \in \mathbb{Z}[x], f = gh \in \mathbb{Q}[x], g, h$ monic implies $g, h \in \mathbb{Z}[x]$
Thus $\Phi_d(x) \in \mathbb{Z}[x]$
Then we have the hard theorem we were in the middle of.
$\Phi_n(x)$ is irreducible.

Proof. $\Phi_n(x) = fg \in \mathbb{Q}[x]$
ζ_n must be a root of either f or g. WLOG $f(\zeta_n) = 0$ and f is irreducible. We want to show that $g = 1$
We had a tricky argument by Dedekind. The stuff on last class wasn't quite right.
Claim:
Suppose we have a primitive $\zeta, f(\zeta) = 0$. If $p \nmid n$ then $f(\zeta^p) = 0$
Proof by contradiction: Assume $f(\zeta^p) \neq 0$. We know that $\Phi_n(\zeta^p) = 0 = f(\zeta^p)g(\zeta^p)$
f is irreducible so f is the minimal polynomial for ζ. But $g(x^p)$ is a polynomial with ζ as a 0. So, $f(x) \mid g(x^p)$. Hence, $g(x^p) = f(x)g(x)$
Reducing mod p we see,
$(\overline{g}(x))^p = \overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$
So, $\overline{f} \mid \overline{g}^p$
So, $\gcd(\overline{f}, \overline{g}) \neq 1$
$(\gcd(\overline{f}, \overline{g}))^2 \mid \overline{f}\overline{g} = \overline{\Phi_n(x)} \mid \overline{x^n - 1}$
But $\gcd(\overline{x^n - 1}, \frac{\mathrm{d}}{\mathrm{d}x}\overline{x^n - 1}) = \gcd(\overline{x^n - 1}, \overline{nx^{n-1}}) = 1$ so we have no multiple factors which is a contradiction.
So, $f(\zeta^p) = 0$
Claim 2: $(a, n) = 1$ implies $f(\zeta_n^a) = 0$
Proof: a is product of primes not dividing n, induct.
So, f has $\phi(n)$ roots ζ_n^a, Φ_n also has $\phi(n)$ roots.

□

Corollary: $|\mathbb{Q}(\zeta_n) : \mathbb{Q}| = \deg \Phi_n(x) = \phi(n)$
Also, $\mathbb{Q}[\zeta_n] = \frac{\mathbb{Q}[x]}{(\Phi_n(x))}$
ALso, $K(\alpha)$ is the smallest field and $K[\alpha]$ is the smallest ring containing α but it's the same if the degree of extension is finite. Not same for π tho.
Claim: Suppose L/K finite. Then,
$|\operatorname{Aut}(L/K)| \leq |L : K|$

Definition 24. L/K is Galois if $|\operatorname{Aut}(L/K)| = |L : K|$ and we call $\operatorname{Gal}(L/K) \coloneqq \operatorname{Aut}(L/K)$

Theorem 10. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois and

$$(\mathbb{Z}/n)^\times \simeq \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

Where k gets mapped to the map $(\zeta_n \mapsto \zeta_n^k)$

Proof. Φ_n is minimal polynomial. For ζ_n and ζ_n^k we have the following diagram [draw commutative digram] □

Definition 25. An extension L/K is Abelian if it is Galois and it's Galois Group $G = \operatorname{Gal}(L/K)$ is abelian.

Definition 26. An extension L/K is simple if $L = K[\alpha]$ for $\alpha \in L$. Then, α is called a primitive element.

We review the Fundamental Theorem of Galois Theory:

Theorem 11 (Fundamental Theorem of Galois Theory)**.** Let K/F be Galois. Then there exists a bijection:
Intermediate extension $K/E/F \leftrightarrow$ subgroups $I - H - G$
Given by:
Subgroup $H \mapsto$ Extension $K^H = \{k : h(k) = h \forall h \in H\}$
Extension $E \mapsto$ Subgroup $G_E = \{g \in G : \forall e \in E, g(e) = e\}$

We have a Corollary: K/E is also Galois and $G_E = \operatorname{Gal}(K/E)$
This is useful in HW P3.
Another Corollary: If $\operatorname{Gal}(K/E)$ is normal in $\operatorname{Gal}(K/F)$ then E/F is Galois and we have $\operatorname{Gal}(E/F) = \frac{\operatorname{Gal}(K/F)}{\operatorname{Gal}(K/E)}$
This is useful in HW P5.
Another Corollary: If L/K is Galois and simple [$L = K[\alpha]$]

Then the minimal polynomial of α is given by: $\prod_{g \in \mathrm{Gal}(L/K)} (x - g(\alpha))$

Done.

Class 08: 01/26

Read Chapter 1 of Atiyah MacDonald (AM)

Chapter 1: Rings and Ideals

Definition 27. Ring [Commutative Ring]
Subring
Ideal $I \triangleleft A$, $(I, +)$ group, $AI = I$
Quotient ring $A \to A/I$
Homomorphism $f : A \to B$
$\ker f \triangleleft A$
$\overline{f} : A/\ker f \xrightarrow{\simeq} f(A)$
zero divisor $\exists y \neq 0$ such that $xy = 0$
domain
PID
units
$A^\times$

Proposition 5 (AM 1.1)**.** If $I \triangleleft A$ then there exists a bijection

$$\{J \triangleleft A | I \subset J\} \leftrightarrow \{\overline{J} \triangleleft A/I\}$$

Map is $J \mapsto q(J)$ the quotient map, and $q^{-1}(J)$ in the other direction.
Proof is in AM.
Look at $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}$ has ideals $(2), (3), (6), (1)$ that contain (6)
$\mathbb{Z}/6\mathbb{Z}$ has ideals $(\overline{3}), (\overline{2}), (\overline{0} = \overline{6}), (\overline{1})$

Definition 28. Field is a ring such that $1 \neq 0$ and $A^\times = A \setminus \{0\}$

Proposition 6 (AM 1.2)**.** The Following Are Equivalent (TFAE):

1. A is a field
2. $I \triangleleft A \implies I = 0$ or A
3. $f : A \to B \neq 0$ implies f is injective

Proof. $1 \implies 2$: We use contradiction. Suppose $0 \neq I \triangleleft A$ and let $0 \neq x \in I$.
So, $A = (1) = (x) \subset I \subset A$ meaning $I = A$
$2 \implies 3$: $f(1) = 1 \neq 0$ so $1 \neq \ker f$ thus $\ker f \neq A \implies \ker f = 0$ so A is injective.
$3 \implies 1$: Suppose $x \in A - A^\times$ then the quotient map $q : A \to A/(x)$ is injective which implies $x = 0$
Note that $A/(x) = 0 \iff A = (x) \iff x \in A^\times$

□

Prime and Maximal Ideals

Atiyah MacDonald Subsection

Definition 29. $I \triangleleft A$ is a prime ideal if $P \neq A$ and if $xy \in P$ then $x \in P$ or $y \in P$

A principal ideal $I = (a)$ is prime means $xy \in I \implies a \mid xy \implies a \mid x$ or $a \mid y$ [Euclid's Lemma] which means a is prime.

Definition 30. $I \triangleleft A$ is proper if $I \neq A$

Definition 31 (Maximal Ideal)**.** $I \triangleleft A$ is maximal if it is a maximal proper ideal, i.e $I \neq A$, if $I \subset J$ and J is a proper ideal of A then $I = J$
For example, $(2), (3)$ are both maximal ideals of $\mathbb{Z}$

Very Useful Trivialities:

$$I \text{ prime} \iff A/I \text{ domain}$$

$$I \text{ maximal} \iff A/I \text{ field}$$

Since all domains are fields, maximal ideal implies prime ideal.
But not the other way around. In $\mathbb{R}[x,y]$ we have $(x-1)$ is prime but $(x-1,y-1)$ is maximal.
A is a domain $\iff$ $0 \triangleleft A$ is a prime

Theorem 12 (AM 1.3)**.** Every $A \neq 0$ has a maximal ideal. [Uses special ase of Zorn's Lemma]

Suppose Σ is the collection of subsets of the set X
Then Zorn's Lemma says that:
If every chain in Σ has an upper bound in Σ then Σ has a maximal element.
Note: $\mathcal{C} \subset \Sigma$ is a chain if $A, B \in \mathcal{C} \implies A \subset B$ or $B \subset A$
$\mathcal{C} \subset \Sigma$ has an upper bound if $\exists B \in \Sigma$ such that $A \in \mathcal{C} \implies A \subset B$
$M \in \Sigma$ is maximal if $M \subset N \in \Sigma \implies M = N$

Proof. Let Σ be the set of proper ideals of A. Consider chain $\mathcal{C} \subset \Sigma$ then the ideal $I = \bigcup_{J \in \mathcal{C}} J$ is a proper ideal of A
Note that unions of proper ideals is not always proper (or even ideal) but if we have a chain it is true.
It is proper because $1 \notin I$
Thus, there always exists an upper bound and therefore by Zorn's Lemma we have a maximal ideal

□

Corollary: if $A \neq 0$ ring then there exists a surjection $A \hookrightarrow$ field.

Proof. $A \mapsto A/M$ □

Corollary 1.4: Any proper ideal is contained in a maximal ideal.

Proof. We have quotient $A \to A/I$ then consider the maximal ideal $\overline{M}$ and then just take $M = q^{-1}(\overline{M})$
Or Zorn's lemma: Let $\Sigma_I = \{J \text{ proper ideal of } A \mid I \subset J\}$

□

Definition 32. A is a local ring if there exists a unique maximal ideal.

It has 'something' to do with local in the sense of topology.
A field as unique maximal ideal (0)
$\mathbb{Z}/p^2\mathbb{Z}$ has local ideal (p)
For prime p we have the local ring $\mathbb{Z}$ localized at p given by
$\mathbb{Z}_{(p)} = \{\frac{r}{s} \in \mathbb{Q} : r, s \in \mathbb{Z}, p \nmid s\} \subset \mathbb{Q}$
The unique maximal ideal is $M = \mathbb{Z}_{(p)}p$
In fact $\mathbb{Z}_{(p)}p/(p) \simeq \mathbb{F}_p$
If A is a local ring then A/M is the residue field.

Class 09: 01/29

Definition 33. A is a local ring if it has a unique maximal ideal.

Another example: you can localize a polynomial ring at a point: $\mathbb{C}[x_1, \ldots, x_n]_{(p)} = \left\{\frac{f}{g} : f, g \in \mathbb{C}[x_1, \ldots, x_n], g(p) \neq 0\right\}$ where $p = (p_1, \ldots, p_n)$ a point.

Proposition 7. Suppose $M \triangleleft A$ and proper and $A - M \subset A^\times$ then A is local and M is maximal.

Proof. We want to show that M is the unique maximal ideal. Let I be a maximal ideal. We want to show that $I = M$
By hypothesis, $A - M \subset A^\times \subset A - I$
Note that $A^\times \subset A - I$ is true for any proper ideal I
This implies $I \subset M$ which implies $I = M$

□

$\mathbb{Z}/p^k\mathbb{Z}$ is maximal with (p) as the maximal ideal by the above proposition [p prime].

Proposition 8. maximal $M \triangleleft A$ such that $1 + M \subset A^\times$ then A is local.

Proof. Let $x \in A - M$, we will show x is a unit.
Then $(x, M) = A$
$\implies ax + m = 1$ for some $a \in A, m \in M$
$\implies ax = 1 - m \in 1 + M \subset A^\times \implies x \in A^\times$
Therefore, $A - M \subset A^\times$ and thus by previous proposition A is local.

□

Exercise: A local ring $\iff A - A^\times \triangleleft A$

Definition 34. If A is a local ring with maximal ideal M then we have an associated canoncial field A/M called the residue field.

Nilradical and Jacobson Radical

Definition 35. Let A be a ring, $x \in A$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$

Examples: $\overline{p} \in \mathbb{Z}/p^k\mathbb{Z}, \overline{x} \in \mathbb{R}[x]/(x^3)$, $\begin{pmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix}$
Note that the last one is not commutative.
Trick: x is nilpotent $\implies 1 \pm x \in A^\times$
This is because $\frac{1}{1-x} = 1 + x + x^2 + \cdots$
Which is a finite sum if x is nilpotent. Similar for $\frac{1}{1+x}$

Definition 36. The nilradical of a ring A, $\operatorname{Nil} A = \mathfrak{N}(A) = \{x \in A : x \text{ is nilpotent}\}$

This looks like a set [because it is] but it is actually an ideal!

Proposition 9. If A is a ring then $\mathfrak{N}(A) \triangleleft A$ and $\mathfrak{N}(A/\mathfrak{N}(A)) = 0$

Proof. $x^n = 0 \implies (ax)^n = 0$
$x^m = 0, y^n = 0$
$$\implies (x+y)^{m+n} = \sum_{j=0}^{m+n} \binom{m+n}{j} x^j y^{m+n-j} = 0$$
Thus $\mathfrak{N}(A)$ is an ideal.
Now, suppose $\overline{X} \in A/\mathfrak{N}(A)$. We prove that it is multipotent by contradiction.
Suppose $\overline{x}^n = 0$
Then $x^n \in \mathfrak{N}(A)$
Thus $(x^n)^k = 0$ for some k
Thus $x^{nk} = 0$
Thus x is nilpotent. So we have a contradiction.

□

Definition 37. Ring A is reduced $\iff \mathfrak{N}(A) = 0$

We can reduce any ring by quotienting out the nilradical.
Motivation: In Algebraic Geometry, if V is a variety, then $k[x_1, \ldots, x_n]/I(V)$ is always reduced. Having nilpotents is problematic if we want to do algebraic geometry.

Proposition 10 (1.8)**.** $\mathfrak{N}(A) = \bigcap_{\text{prime ideal } P \triangleleft A} P$

Useful in homework.

Proof. We want to show that the sets contain each other.
Suppose $x \in \mathfrak{N}(A) \implies x^n = 0$
Let $P \triangleleft A$ be prime.
Thus $0 \in P \implies x^n \in P \implies x \in P$
For other direction, we do contrapositive.
Suppose $x \notin \mathfrak{N}(A)$
Zorn's Lemma time! We construct a prime ideal x is not inside of.
Let $\Sigma = \{I \triangleleft A : \overline{x} \notin \mathfrak{N}(A/I)\} = \{I \triangleleft A : x^n \notin I \forall n\}$
Note: $(0) \in \Sigma$
Any chain in Σ has an upper bound in Σ and thus there exists a maximal element $P \in \Sigma$
Claim: $x \notin P$ and P is prime.
$x \notin P$ since $P \in \Sigma$
To prove P is prime, we prove $a, b \notin P \implies ab \notin P$
Assume $a, b \notin P$
Then $P + (a), P + (b) \notin \Sigma$
$\implies x^m \in P + (a), x^n \in P + (b)$
$\implies x^{m+n} \in P + (ab)$
$\implies P + (ab) \notin \Sigma$ and $P \in \Sigma$
$\implies ab \notin P$

□

Definition 38 (Jacobson Radical)**.** Since nilradical is the intersection of prime ideals, Jacobson Radical is the intersection of maximal ideals.

$$\mathfrak{J}(A) = \bigcap_{M \text{ maximal ideal of } A} M$$

Note that $\mathfrak{N}(A) \subset \mathfrak{J}(A)$ since maximal ideals are prime.
Example where nilradical and jacobson radical are different:
Let $\mathbb{Z}_{(2)} = \frac{p}{q}$ where q odd.
Then $\mathfrak{N}(\mathbb{Z}_{(2)}) = 0$ but $\mathfrak{J}(\mathbb{Z}_{(2)}) = 2(\mathbb{Z})$

Class 10: 01/31

Proposition 11 (AM 1.9)**.** The Jacobson Radical $\mathfrak{J}(A) = \{x \in A : 1 - xA \subset A^\times\}$

Proof. We show it by the two sided inclusion, and we show that by the contrapositive.
Suppose $1 - xa \notin A^\times$
Then there exists maximal ideal M so that $1 - xa \in M$
$\implies 1 \in xa + M$
$\implies xa \notin M$
$\implies x \notin M$
$\implies x \notin \mathfrak{J}(A)$
Now suppose $x \notin \mathfrak{J}(A)$
$\implies x \notin M$ for some maximal ideal M
$\implies (x, M) = A$
$\implies 1 = xa + m$ for some $a \in A, m \in M$
$\implies 1 - xa \in M$
Since M is a proper ideal, $1 - xa \notin A^\times$

□

Operations on Ideals

Suppose we have ideals I, J in A
Then $IJ \subset I \cap J \subset I + J = (I, J)$ are all ideals but $I \cup J$ is not an ideal.
$I + J = \{i + j : i \in I, j \in J\}$ it is an abelian group, and absorbs multiplication so it is an ideal. It is (I, J) so it is an ideal.
Note that $IJ \neq \{ij : i \in I, j \in J\}$
Instead, $IJ = \{\sum_{k=1}^{n} i_k j_k : i_k j_k : i_k \in I, j_k \in J\}$ [finite sum]
Canonical Example: Suppose $A = \mathbb{Z}$
Then $(a)(b) = (ab)$
But $(a) \cap (b) = (\text{lcm}(a, b))$
And $(a) + (b) = (\gcd(a, b))$
This is true for PIDs, potentially UFDs?

Direct Product of Rings

If we have rings $A_1, A_2, \cdots, A_n$ then we can define $A_1 \times A_2 \times \cdots \times A_n = \prod A_i$
Given two rings A_1 and A_2 we can define a ring structure on their cartesian product $A_1 \times A_2 = \{(a_1, a_2) : a_1 \in A_1, a_2 \in A_2\}$ where sum and product are done componentwise. Then $A_1 \times 0$ and $0 \times A_2$ are zero divisors and $1_{A_1 \times A_2} = (1, 1)$.
An element $e \in A$ is an idempotent if $e^2 = e$. Examples: $0, 1$ are trivial idempotents.
$A \cong A_1 \times A_2$ with $A_j \neq 0 \iff$ there exists a non-trivial idempotent in A.
Suppose e is a non-trivial idempotent. We want $e = (1, 0)$ then $1 = e + (1 - e)$ so we have $A_1 = Ae$ and $A_2 = A(1 - e)$.
$A_1 \times A_2$ is product of A_1 and A_2 in the category Ring and CRing
[insert R to $A_1 \times A_2$, A_1 and A_2 category picture]
(maps into products are easy)

Definition 39. Ideals I, J are co-prime if $I + J = A$ i.e. $1 = i + j$ for some $i \in I$ and $j \in J$

Proposition 12 (AM 1.10)**.** Let $I_1, \ldots, I_n$ be ideals of A and let $\phi : A \to \prod_{i=1}^{n}(A/I_i)$ then $\phi(a) = (a + I_1, \cdots, a + I_n)$

1. If $\{I_j\}$ are pairwise co-prime then $\prod I_j = \cap I_j$
2. ϕ is surjective if and only if the ideals are pairwise co-prime
3. ϕ is injective if and only if $\cap_j I_j = 0$

We only prove for $n = 2$, induction is automatic.

Proof. 1: $I_1 I_2 \subset I_1 \cap I_2$ always true
Conversely, if $1 = i_1 + i_2$, for $a \in I_1 \cap I_2$ we see that $a = a \cdot 1 = a \cdot i_1 + a \cdot i_2 \in I_1 I_2$
2: $\implies$ suppose ϕ is surjective. Then, there exists x such that $\phi(x) = (1, 0)$ and thus $1 = 1 - x + x$ where $1 - x \in I_1, x \in I_2$, since $[x] = 0$ in A/I_2 and $[x] = 1$ in A/I_1 implies $[1 - x] = 0$ in A/I_1 so I_1, I_2 are co-prime
$\impliedby$ Since co-prime we can find $1 = i_1 + i_2$ so $\phi(1 - i_1) = (1, 0), \phi(1 - i_2) = (0, 1)$ so we have that ϕ is onto.
3. Suppose ϕ is injective. Then $\ker \phi = 0$. But for any I_1, I_2 we have $\ker \phi = I_1 \cap I_2$. So injectivity is equivalent to $I_1 \cap I_2 = 0$

□

Proposition 13 (AM 1.11)**.** Let $P_1, \ldots, P_n$ be prime ideals and let $I \subset \cup P_j$ then $I \subset P_j$ for some j.
If prime ideal $P \supset \cap P_j$ then $P \supset I_j$ for some j

Proof. We just do the $n = 2$ case. We do contrapositive.
Suppose $I \not\subset P_1, P_2$. We want to prove that $I \not\subset P_1 \cup P_2$
Now, P_1 and P_2 are prime.
Then $\exists x_1, x_2 \in I$ so that $x_1 \notin P_2, x_2 \notin P_1$.

Case 1: $x_1 \notin P_1$ or $x_2 \notin P_2$ in this case we're done since either $x_1 \notin P_1 \cup P_2$ or $x_2 \notin P_1 \cup P_2$
Case 2: $x_1 \in P_1, x_2 \in P_2$. In this case, $x_1 + x_2 \in I$ but $x_1 + x_2 \notin P_1 \cup P_2$ which provides a contradiction.
Thus we're done with part 1.

□

Class 11: 02/02
Ideal P is prime $\iff$ compelement is multiplicatively closed
P is prime $\iff$ $(ab \in P \implies a \in P$ or $b \in P) \iff (a \notin P, b \notin P \implies ab \notin P)$

Proposition 14 (AM 1.11:)**.** 1. Suppose we have prime ideals $P_1, \ldots, P_n$ and an ideal I. Then, $I \subset \cup P_i \implies I \subset P_i$ for some i
2. Suppose we have ideals $I_1, \ldots, I_n$ and prime ideal P.
2a. If $\cap I_j \subset P$ then $I_j \subset P$ for some j
2b. If $\cap I_j = P$ then $I_j = P$ for some j

Proof. 1: We prove the contrapositive.
$I \not\subset P_i$ for all $i \implies I \not\subset \cup P_i$
We induct. For $n = 1$ it's trivial.
Assume true for $n - 1$
Then we have $x_i \in I, x_i \notin \cup_{j \neq i} P_j$
Suppose we have some i so that $x_i \notin P_i$
Then $x_i \notin \cup P_i$ so $I \not\subset \cup P_i$
For the other case, for all i we have $x_i \in P_i$
Then, product of x_j without i is in P_j for all $j \neq i$ and it's not in P_i since P_i is prime.
Let y be the sum of these. Then y is not in any of the P_i so we're done.
2a: Contrapositive.
$\forall i$, $I_i \not\subset P \implies \cup I_i \not\subset P$
$\forall i, \exists x_i \in I_i - P$
$y = \prod x_i \in \prod I_i \subset \cap I_i$
$y \notin P$ since P is prime.
2b. $P = \cap I_i$
So there exists i so that $I_i \subset P \subset \cap I_i \subset I_i$

□

Radicals of Ideals

If $I \triangleleft A$ we define radical $\sqrt{I} = \{x : x^n \in I\} \triangleleft A$
In integers, $\sqrt{(p_1^{e_1} \ldots P_r^{e_r})} = (p_1 \ldots p_r)$
And of course $I \subset \sqrt{I}$
So the nilradical $\mathfrak{N}(A) = \sqrt{0}$
So, $\sqrt{I} = q^{-1}(\mathfrak{N}(A)/I)$ whee $q : A \to A/I$

Proposition 15 (AM 1.14)**.** $\sqrt{I} = \cap_{I \subset P \text{ prime}} P$

Proof. $\sqrt{I} = q^{-1}(\mathfrak{N}(A)/I) = q^{-1}(\cap_{\text{prime} \overline{P} \triangleleft A/I}) = \cap q^{-1}\overline{P} = \cap_{I \subset P} P$ □

Exercise 1.15:

1. $I \subset \sqrt{I}$
2. $\sqrt{\sqrt{I}} = \sqrt{I}$
3. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
4. $\sqrt{I} = A \iff I = A$
5. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$
6. $\sqrt{P^n} = P$ when P is prime.

An ideal I is radical if $\sqrt{I} = I$
So $\sqrt{\cdot}$: ideals $\to$ radical ideals
$\sqrt{I}$ is the smallest radical ideal containing I
The motivation for studying radicals come from algebraic geometry.
Recall the correspondence between varieties in k^n and ideals in $k[x_1, \ldots, x_n]$.
So we have $V(J) = V(\sqrt{J})$
Because $x^2 = 0 \iff x = 0$
Another motivation is the Nullstellensatz.
Suppose k is algebraically closed. If we take an ideal J and take its variety $V(J)$ then $I(V(J)) = \sqrt{J}$ where I is the map from varities to ideals.
Ideal Quotient
Suppose we have ideals $I, J \lhd A$
Then $(I : J)$ is supposed to be like I/J
$(I : J) = \{x \in A : xJ \subset I\}$ This is an ideal because it is closed under addition and multiplication by members of A
From wikipedia: $KJ \subset I \iff K \subset (I : J)$
Also from wikipedia: $I(V - W) = (I(V) : I(W))$ when varities $V, W \subset k^n$
$(0 : J) = \text{Ann}(J)$ is the annihilatoz of J
$\text{Ann}(\mathbb{R} \times 0) = (0 \times \mathbb{R})$
In AM, $\{\text{zero divisors}\} = \cup_{x \neq 0} \text{Ann}(x)$
Useful in HW.
For a set $E \subset A$ we can talk about its radical $\sqrt{E} = P\{x : x^n \in E\}$ for some n
Then $\sqrt{\cup E_\alpha} = \cup \sqrt{E_\alpha}$

Proposition 16 (AM 1.15)**.** $\{\text{zero divisors}\} = \cap_{x \neq 0} \sqrt{\text{Ann}(x)}$
$\{\text{zero divisors}\} = \sqrt{\{\text{ zero divisor }\}} = \cup_{x \neq 0} \sqrt{\text{Ann}(x)}$

Proposition 17 (AM 1.16)**.** If $\sqrt{I} + \sqrt{J} = A$ then $I + J = A$
[radicals co-prime means ideals co-prime]
We use 1.15(v).
$\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{A} = A$
1.15(iv) tells us $I + J = A$
Next, extension and contraction.
Let $f : A \to B$
If $J \lhd B, J^c f^{-1} J \lhd A$ contraction
If $I \lhd A, I^e = (f(I))$ extension

Class 12: 02/05

Extension and Contraction

Consider a ring homomorphism $f : A \to B$
Then, ideals $I \lhd A$ and ideals $J \lhd B$ has a correspondence:
$I \xrightarrow{e} J$
$J \xrightarrow{c} I$
These are extension and contraction.
$C = \text{image } c = \{J^c : J \lhd B\}$, $E = \text{image } e$
$J^c = f^{-1}(J)$
$I^e = (f(I)) = Bf(I) = \{\sum_i b_i f(a_i) | a_i \in I\}$
J prime implies J^c prime
Thus we have $\text{Spec}(f) : \text{Spec}(B) \to \text{Spec}(A)$
Note that $I^e \neq f(I)$ in general.
Consider $f : \mathbb{Z} \curvearrowleft \mathbb{Q}$
Then $(2\mathbb{Z})^e = \mathbb{Q}\mathbb{Z} = \mathbb{Q}$ which is not $f(2\mathbb{Z})$
If f is onto / surjective,
$I^e = f(I)$
[insert category theory image of $A \xrightarrow{f} B$ and $f(A)$ here]

Extension and Contraction are also called going up and going down.
Consider $f : \mathbb{Z} \to \mathbb{Z}[i]$
Consider odd prime $p \in \mathbb{Z}$
Then $\frac{\mathbb{Z}[i]}{(p)} = \frac{\mathbb{Z}[x]}{(p,x^2+1)} = \frac{\mathbb{F}_p[x]}{(x^2+1)} = \begin{cases} \mathbb{F}_{p^2}, & \text{if } p \equiv 3 \pmod 4; \\ \mathbb{F}_p \times \mathbb{F}_p, & \text{if } p \equiv 1 \pmod 4; \end{cases}$
$(2)^e = ((1+i)^2)$ in this case it is called ramified
$p \equiv 3 : (p)^e$ is prime and in this case it is called inert
$p \equiv 1 : (p)^e = Q_1 Q_2$ product of distinct primes, here it is called split
There are about 15 properties of extension and contraction.

Proposition 18 (AM 1.17)**.** 1. $I \subset I^{ec}, J^{ce} \subset J$

2. $I^e = I^{ece}, J^{cec} = J^c$

3. $C \overset{e,c}{\longleftrightarrow} E$ is a bijection, $C = \{I : I = I^{ec}\}, E = \{J : J = J^{ce}\}$

Proof. Exercise. Use map of sets: $g : C \to D$. If Y is a subset, $g(g^{-1}(Y)) \subset Y$ with equality iff $Y \subset g(C)$ but $X \subset g^{-1}(g(X))$. Also, $I^e = Bf(I)$ and $J^c = f^{-1}(J)$ □

Proposition 19 (AM 1.18)**.** 1. $(I_1 + I_2)^e = I_1^e + I_2^e, (I_1 I_2)^e = I_1^e I_2^e$

2. $(J_1 + J_2)^c \supset J_1^c + J_2^c, (J_1 J_2)^c \supset J_1^c J_2^c$

3. $(I_1 \cap I_2)^e \subset I_1^e \cap I_2^e$

4. $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$

5. $(\sqrt{I})^e \subset \sqrt{I_e^e}$

6. $(\sqrt{J})^c = \sqrt{J^c}$

7. $(I_1 : I_2)^e \subset (I_1^e : I_2^e)$

8. $(J_1 : J_2)^c \subset (J_1^c : J_2^c)$

9. e is closed under sum and product, and c is closed under the other three operations (??? not sure what this means)

We're Moving on to Chapter 2 of Atiyah MacDonald!!!

Modules

[The M word]

Definition 40. Let A be a ring. Then a A-module is a abelian group M and a function $A \times M \to M$ given by $(a, m) \mapsto am$ such that $a(x+y) = ax+ay, (a+a')x = ax + a'x, (aa')x = a(a'x), 1x = x$ for all $a, a' \in A, x, y \in M$

The concept of modules generalize both vector spaces and ideals.
Atiyah Macdonald makes an observation that is obvious but not really:
M is a A-Module if and only if M is a representation of A

Proof. We need a ring homomorphism $A \to End(M)$ where $End(M) = Hom(M, M)$, the endomorphism ring of M
Here we have addition, multiplication(composition) and multiplication by a is a homomorphism of M

□

Examples:
$I \triangleleft A$ is an A-module
$\mathbb{Z}-$module is an abelian group
k-module $\iff$ vector space over k
$k[x]$-module $\iff$ vector space over k with $T : V \to V$
Here $M = V, xv \coloneqq T(v)$

$k[x, x^{-1}]$-module $\iff$ vector space over k, $T : V \xrightarrow{\approx} V$
kG-module $\iff$ $k-$represetation of G
Modules form a Category.
There is a Category. $ModA$ is the category of modules of A. The objects are A-modules. The morphisms [the ones we care about] is an A-module map, or an A-map $f : M \to N$ is an A-module map if it respects the structure: $f(x + y) = f(x) + f(y), f(ax) = af(x)$
We need a bit more for categories: composition $(f \circ g)$ and identity Id_M
Compositions of A-module maps are A-module maps.
Mod A is a category enriched in Mod A [wtf???]
$Hom_A(M, N)$ [often just called $Hom(M, N)$] is the set of maps from M to N
This is the set of morphisms $\mathrm{Mor}_{\mathrm{MOd}(A)}(M, N)$
If $f, g : M \to N$ then $f + g : M \to N$ and $(af)(m) = af(m)$
So $Hom(M, N)$ is an A-module.
$Hom(M, N) \times Hom(N, P) \to Hom(M, P)$ is A-bilinear, given by $(f, g) \mapsto g \circ f$
Related fact: Given $f : M \to M'$ We can define an A-module map $Hom(f, Id) : Hom(M', N) \to Hom(M, N)$ given by $h \mapsto h \circ f$
Similarly, given $N \to N'$ we have a map $Hom(M, N) \to Hom(M, N')$ given by $h \to g \circ h$
We have $Hom(A, M) = M$ given by $\phi \mapsto \phi(1)$
$Hom(M, A) = M^\star$ the dual of M

Class 13: 02/07

Submodules and Quotient Modules

Definition 41 (Submodule)**.** A submodule M' of an A-module M if it is a subgroup of M such that $am' \in M'$ for all $a \in A, m' \in M'$

We'll use notation $M' \triangleleft M$

Definition 42 (Quotient Module)**.** If M' is a submodule of M quotient module is the module of cosets/equivalence classes $m + M' = [m]$ where $m \sim \hat{m}$ if $m - \hat{m} \in M'$

We have the quotient map $q : M \to M/M'$
Now we talk about Kernels and Cokernels.
Let $f : M \to N$ be a module map.
Then $\ker f \triangleleft M$
$\mathrm{im}\, f \triangleleft N$
$\mathrm{cok}\, f = N/\mathrm{im}\, f \leftarrow N$
$\ker f = 0 \iff f$ 1-1 or injective
$\mathrm{cok}\, f = 0 \iff f$ onto or surjective

Theorem 13 (1st Isomorphism Theorem)**.** If $f : M \to N$ onto, then $\overline{f} : M/\ker f \xrightarrow{\approx} N$ is a well-defined isomorphism.
$\overline{f}([m]) = f(m), \overline{f}(m + \ker f) = f(m)$

[draw commutative diagram of first isomorphism theorem]

Operations On Submodules

Submodules are generalizations of ideals.
Suppose we have a module M and submodules $\{M_i\}_{i \in I}$
Then $\sum_i M_i \triangleleft M$
$\bigcap_i M_i \triangleleft M$

Proposition 20 (AM 2.1)**.** Out of order

1. (third isomorphism theorem) $N \triangleleft M \triangleleft L$, A-modules imply $(L/N)/(M/N) \cong L/M$

2. (second isomorphism theorem) If $M_1, M_2 \triangleleft M$ then $M_2/(M_1 \cap M_2) \cong (M_1 + M_2)/M_1$

1. Consider $\theta : L/N \to L/M$ given by $\theta(l+N) = l+M$. Since θ is onto and kernel is M/N we have the theorem.
[2]
$M_2 \to \frac{M_1+M_2}{M_1}$ is onto, kernel is $M_1 \cap M_2$ so we have the theorem. □

Definition 43. Let ideal $I \triangleleft A$ and subset $\Sigma \subset M$ where M is a module.
Define $I\Sigma = \{\sum_i^n a_i\sigma_i : a_i \in I, \sigma_i \in \Sigma\} \triangleleft M$

Definition 44. Let $\Sigma \subset M$ where M is an A-module.
Then $(\Sigma) = A\Sigma$ which is the submodule of M generated by Σ
Think of span.
If $M = (\Sigma)$ then M is generated by Σ
A module M is finitely generated if we can write $M = (\Sigma)$ for some finite subset Σ

Definition 45 (module quotient)**.** Let $N, P \triangleleft M$.
Then module quotient: $(N : P) = \{a \in A : aP \subset N\} \triangleleft A$

Definition 46 (Annihilator)**.** $Ann(M) = (0 : M) = \{a \in A : aM = 0\}$ is the Annihilator of M.

Example: Let $A = \mathbb{Z}$ then $Ann(\mathbb{Z}/15 \times \mathbb{Z}/6) = \mathbb{Z}30$
M is an $A/Ann(M)$-module
Exercise 2.2: $Ann(M_1 + M_2) = Ann(M_1) \cap Ann(M_2)$ and $(N : P) = Ann\left(\frac{N+P}{N}\right)$

Category Theory!!!!

Definition 47. A category $\mathcal{C}$ is:

1. A collection of objects $Ob\mathcal{C}$
2. $\forall x, y \in Ob\mathcal{C}$, a collection of morphisms, $\mathcal{C}(x, y)$ [Alternatie: $Mpr_{\mathcal{C}}(x, y)$]
3. $\forall x, y, z \in Ob\mathcal{C}$ we have a map $\mathcal{C}(x, y) \times \mathcal{C}(y, z) \to \mathcal{C}(x, z)$ given by $(g, f) \mapsto f \circ g$ [composition law]
4. $\forall x \in Obx$ we have $Id_X \in \mathcal{C}(x, x)$

So that $(f \circ g) \circ h = f \circ (g \circ h)$
And $Id_y \circ f = f = f \circ Id_X$

We often write $f : X \to Y$ or $X \xrightarrow{f} Y$ for $f \in C(X, Y)$ and it might not be a function because everything is abstract.
We write $X \in \mathcal{C}$ for $X \in Ob\mathcal{C}$

Definition 48 (isomorphism)**.** $f : X \to Y$ is an isomorphism if $\exists g : Y \to X$ so that $f \circ g = Id_Y$ and $g \circ f = Id_X$ and say X and Y are isomorphic, written $X \cong Y$

Example: Set, CRing (in 502, Ring), Rng [Rings possibly without identity], Top
If we have a group G we have a category BG so that $ObBG = \{*\}$ and $BG(*, *) = G$ so morphisms need not be maps.

Class 15: 02/09

Direct Sums and Products

$\{M_i\}_{i\in I}$ is a family of A-modules.
We can define the direct product and direct sum.

Definition 49 (Direct Produt)**.** $\prod_{i\in I} M_i$ is direct product, elements are i-tuples $(x_i)_{i\in I}$, and operations are done componentwise.

Definition 50 (Direct Sum)**.** The direct sum is a submodule of direct product. $bigoplus_{i\in I} \subset \prod_{i\in I} M_i$ containing $(X_i)_{i\in I}$ which vanish a.e.
$\#\{i|X_i \neq 0\}$ is finite.

$\prod_{i\in I} M_i, p_i : \prod M_i \to M_i$ is a product in the category of A-modules.
$\forall(M, \{\phi_i : M \to M_i\}_{i\in I})$ there exists a unique map $\phi : M \to \prod M_i$ so that $p_i \circ \phi = \phi_i$
[Insert category theory picture of $M, \prod M_i$ and M_i]
Maps into products are easy. We can write $\phi = \prod \phi_i$ and we can call it 'universal property'.
Direct sum is a co-product and we reverse all the arrows in this case.
Suppose we have $(\bigoplus_{j\in I} M_j, i_j \to \bigoplus M_j)$ is a coproduct in the category of A-modules.
$\forall(M, \{\phi : M_j \to M\}_{j\in I})$ there exists a unique map $\phi : \bigoplus M_j \to N$ so that $\phi \circ i_j = \phi_i$
[insert reverse commutative diagram here]
Notation: $\phi = \bigoplus \phi_j$
There is a map $\bigoplus M_j \to \prod M_j$. It is an isomorphism if $|J| < \infty$
Remark: $A \cong I_i \oplus I_2$ if and only if $A \cong A_1 \times A_2$

Finitely Generated Modules

Definition 51 (Finitely Generated Modules)**.** A is a ring and M is a A-module. If there is a finite subset $\Sigma \subset M$ so that $M = A\Sigma$ then M is finitely generated.

Definition 52. $B \subset M$ is a basis for M if any $m \in M$ can be expressed uniquely as a linear combination of elements of B: $m = a_1b_1 + \cdots + a_nb_n$

Lemma:
M has a basis $iff M \cong \bigoplus_{i\in I} A$

Proof. Exercise □

Definition 53. M is free if either side of previous lemma holds.

Example: $\prod_\infty \mathbb{R}$ is a free $\mathbb{R}$-module, but $\prod_\infty \mathbb{Z}$ is not a free $\mathbb{Z}$-module

Proposition 21 (AM 2.3)**.** M is finitely generated $\iff \exists A^n \to M$

Proof. Atiyah Macdonald □

Proposition 22 (Nakayama's Lemma)**.** Suppose M is finitely generated.
Then $J(R)M = M \iff M = 0$
textbook version: Let M be finitely generated and $I \triangleleft J(R)$ then $IM = M \implies M = 0$

Applications:
Assume Nakayama's Lemma.
Corollary AM 2.7:
Suppose M is a finitely generated A-module and N is a submodule ($N \triangleleft M$).
$M = J(A)M + N$ implies $M = N$

Proof. We apply Nakayama's lemma to the quotient.
$J(A)(M/N) = (J(A)M + N)/N = M/N \implies M/N = 0 \implies M = N$ □

Proposition 23 (AM 2.8)**.** Let A be a local ring. Let J be the uniuqe maximal ideal of A. Let $k = A/J$. Suppose M is a finitely generated A-module. Let $\{x_1, \ldots, x_n\} \subset M$ so that $\overline{x}_1, \ldots, \overline{x}_n$ is a k-basis for M/JM [which is a A/J module or a k-module]. [In other words, $\overline{x}_1, \cdots, \overline{x}_n$ generate M/JM as A-module]

Proof. Let $N = A\{x_1, \ldots, x_n\} \triangleleft M$
Then $N \hookleftarrow M \to M/JM$ [hooked arrow means onto] composition is into.
Thus $N + JM = M \overset{27}{\implies} M = N$

□

Proposition 24 (AM 2.4)**.** Suppose $M = A\{x_1, \ldots, x_n\}$ is a finitely generated module. Let $\phi : M \to M$ be an endomorphism and $I \triangleleft A$ and $\phi(M) \subset IM$.
Then $\phi^n + a_1\phi^{n-1} + \cdots + a_0 = 0$ with $a_i \in I$. [Cayley Hamilton].

Recall that, for square matrix P, there is adjugate matrix $adj(P)$ so that $P \cdot adj(P) = (\det P)I$ which is the transpose of matrix of cofactors.
This generalizes to commutative rings.
We want to come up with matrices $\phi(x_i) = \sum a_{ij}x_i, a_{ij} \in I$
Then $\sum_j (\delta_{ij}\phi - a_{ij})X_j = 0$. Let P be the matrix $(\delta_{ij}\phi - a_{ij})X_j = 0$
Then, $P\underline{x} = 0 \implies (\det P)\underline{x} = adj(P)P(\underline{x}) = 0$
This means, for all X_i we have $(\det P)(x_i) = 0$ so $\det P$ letting it be an endomorphism on M must be 0.
Let $P \in M_n A[t]$. Consier $\det P$ and plug in $t = \phi$.

Class 15: 02/12

Proposition 25 (AM 2.4)**.** Suppose M is a finitely generated A-module generated by $u_1, \ldots, u_n$ [we write it $M = A\{u_1, \ldots, u_n\}$]. Suppose $I \triangleleft A$, there is $\phi : M \to M$ so that $\phi(M) \subset IM$. Then $\exists a_1, \ldots, a_n \in I$ sp that there exists equation $\phi^n + a_1\phi^{n-1} + \cdots + a_{0I=0}$.

Remark: If $I = A = k$ [a field] then this is Cayley-Hamilton Theorem. We let $p(x) = \det(xI - \phi)$. Then $p(\phi) = 0$.

Proposition 26 (AM Corollary 2.5)**.** If M is a finitely generated A-module and $IM = M$,

1. Then $\exists x \equiv I \pmod{I}$ so that $x \in Ann(M)$
2. $\exists i \in I$ so that $\forall m \in M, im = m$.

Proof. 1: use 2.4. Let $\phi = Id$ and let $x = 1 + a_1 + \cdots + a_n$. Then, $xm = (Id^n + a_1 Id^{n-1} + \cdots + a_0)m = 0m = m$.
2: Let $i = x + 1$, then $im = xm + m = m$ □

Recall the Jacobson Radical:

$$J(A) = \bigcap_{\text{maximal ideal}} I \overset{AM1.9}{=} \{j \in A : 1 + jA \subset A^\times\}$$

We also have Nakayama's Lemma:

Proposition 27 (Nakayama's Lemma)**.** Let M be finitely generated A-module. Then,

$$J(A)M = M \implies M = 0$$

Atiyah Macdonald gives two proofs, second proof is cooler. - Davis
First Proof:
$J(A)M = M$, by AM2.5 we have $\exists x \equiv 1 \pmod{J(A)}$ such that $xM = 0$. Using 1.9, $x \in A^\times, xM = 0 \implies M = 0$.
Second Proof:
Let $M = A\{u_1, \ldots, u_n\}$, n is minimal, $J(A)M = M$, and $M \neq 0$. We try to find a contradiction.
$u_n \in M = J(A)M$
Thus, $u_n = j_1u_1 + \cdots + j_nu_n$ where $j_i \in J(A)$.
Thus, $(1 - j_n)u_n = j_1u_1 + \cdots + j_{n-1}u_{n-1}$
$1 - j_n$ is a unit by 1.9, which means u_n can be written in terms of $u_1, \ldots, u_{n-1}$. This contradicts minimality of n.

Exact Sequences

Definition 54. Let M, M', M'' be A-modules.

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$$

is exact at M if $im\alpha = \ker\beta$

Note that $\operatorname{im}\alpha \subset \ker\beta \iff \beta \circ \alpha = 0$

Definition 55. Sequence of homomorphisms

$$M_n \to M_{n-1} \to \cdots \to M_0$$

is exact if it is exact at $M_{n-1}, \ldots, M_2, M_1$

Note, $0 \to M \xrightarrow{\alpha} N$ is exact if and only if α is injective. This is equivalent to saying $\ker\alpha = 0 \iff \alpha$ is 1-1 or injective.
$M \xrightarrow{\beta} N \to 0$ is exact if and only if $\operatorname{im}\beta = N \iff \beta$ is onto.
If $M \hookrightarrow N$ then $0 \to M \to N \to N/M \to 0$ is exact.
Memorize these.
Most important special case:

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

is called a short exact seuqence.
This means α is injective, β is surjective.
We have $\overline{\beta} : M/\operatorname{im} M' \xrightarrow{\cong} M''$.
So, $M' \cong \alpha(M'), M \cong M, M'' \cong M/\alpha(M')$
[insert commutative diagram about this here]
Example of short exact sequence:

$$0 \to M' \to M' \oplus M'' \to M'' \to 0$$

Question: are all short exact sequences created this way?
Answer: No! example:

$$0 \to \mathbb{Z}/2 \xrightarrow{\cdot 2} \mathbb{Z}/4 \xrightarrow{q} \mathbb{Z}/2 \to 0$$

Multiplication by 2 sends $[m]$ to $[2m]$.
When is it created this way? If we have pseudo-inverse: If there exists $M \xleftarrow{s} M''$ such that $\beta \circ s = Id_M$.

Proposition 28. Suppose $A = k$, a field. Then,

$$0 \to U \to V \to W \to 0$$

implies $\dim V = \dim U + \dim W$.

Theorem 14 (Consequence of Third Isomorphism Theorem:)**.** If we have $L \triangleleft M \triangleleft N$ then,
$0 \to M/L \to N/L \to N/M \to 0$ is a short exact sequence.

Hom

$Hom(-,-)$ A-module $\times A$-module $\to$ A-module
This is a bifunctior, and contravariant in the first variable. It is also left exact.
Suppose we have a short exact sequence $0 \to M' \to M \to M'' \to 0$. Then, for all N,

$$0 \to Hom(N, M') \to Hom(N, M) \to Hom(N, M'')$$

is exact,

$$0 \to Hom(M'', N) \to Hom(M, N) \to Hom(M', N)$$

Atiyah Macdonald has a fancier way to show this.

Proposition 29 (AM 2.9:)**.** 1. $M' \to M \to M'' \to 0$ is exact if and only if $\forall N$, we have $0 \to Hom(M'', N) \to Hom(M, N) \to Hom(M', N)$ is exact.

Sample proof: i: $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ is exact.

We want to show $0 \to Hom(M'', N) \xrightarrow{v^\star} Hom(M, N) \xrightarrow{u^\star} Hom(M', N)$
Id $v^\star$ injective? $0 = v^\star(\phi) = \phi \circ v$, moreover $\phi(M'') = \phi(b, V)$
$\phi(M'') = \phi(u(M)) = 0$ so $\phi = 0$
[insert commutative diagram here].
Since $u^\star\phi = 0, \phi = (\overline{\phi} \circ \overline{v}^{-1}) \circ v \in \operatorname{im} v^\star$

Class 16: 02/14
Question: Are all short exact sequences same?
Answer: Yes and No.
Yes: all are $0 \to M' \hookrightarrow M \to M'/M \to 0$
No: Not all are $0 \to M \xrightarrow{i} M \oplus M' \xrightarrow{p} M' \to 0$

Proposition 30 (AM 2.10, Snake Lemma)**.** If white stuff is in short exact, then yellow is exact [picture]
[just see Ivan notes]
$\partial m'' = \left[(v')^{-1} f u^{-1} m''\right] \in cok f'$

'Euler Characteristic'

Let $\mathcal{C}$ = a collection of A-modules
G = abelian group
Then $\lambda : \mathcal{C} \to G$ is <u>additive</u> if every short exct sequence

$$0 \to M' \to M \to M'' \to 0$$

with modules in $\mathcal{C}$ has $\lambda(M) = \lambda(M') + \lambda(M'')$
eg $A = \mathbb{Q}$ and $\mathcal{C}$ = finite dimensional vector spaces over $\mathbb{Q}$ and $\lambda(M) = \dim_{\mathbb{Q}}(M)$
If $\mathcal{C}$ = finitely generated abelian groups, $A = \mathbb{Z}$ and $\lambda(M) = rank(M)$ [rank is the dimension of the free part. In other words, it is $\max n : \exists \mathbb{Z}^n \hookrightarrow M$. For all abelian groups, rank is a non-negative integer or infinity. for example, $rank\mathbb{Q} = 1$]. $\mathcal{C}'$ = all abelian groups of finite rank.
Suppose $\mathcal{C}$ is the collection of finite (abelian) groups and $G = \mathbb{Q}^\times$ and $\lambda(M) = |M|$.
This works, but $+$ is actually the group operation of $\mathbb{Z}$

Proposition 31 (AM 2.11)**.** If we have an exact sequence

$$0 \to M_n \to M_{n-1} \to \cdots \to M_1 \to M_0 \to 0$$

With $M_i \in \mathcal{C}$ and $K_i = \ker(M_i \to M_{i-1}) \in \mathcal{C}$
And λ additive,
Then $\sum_{i=1}^{n} (-1)^i \lambda(M_i) = 0$

Consequene: Consider finite abelian groups F_j. Suppose:

$$0 \to F_n \to \cdots \to F_1 \to F_0 \to 0$$

Then, $\displaystyle\prod_{i=0}^{n} |F_i|^{(-1)^i} = 1$ or $\displaystyle\prod_{i \text{ even}} |F_i| = \prod_{i \text{odd}} |F_i|$

Proof. For all homomorphism $f : M \to N$ we have a short exact sequence $0 \to \ker f \to M \to imf \to 0$
Thus, $0 \to K_i \to M_i \to K_{i-1} \to 0$ Thus,

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = \sum (-1)^i \lambda(K_i) + \sum (-1)^i \lambda(K_{i-1})$$

□

We're not actually going to talk about Euler Characteristics.

Tensor Products

It is a functor:
$- \otimes_A - : A - mod \times A - mod \to A - mod$
First we want some notation for free module.
If we have a ring A and a set S then we have:
$A[x]$ (or $A^{(s)}$): the free module with basis S.
Then $a_1 s_1 + \cdots + a_n s_n \in A[S]$ where s_i distrinct.
If S is finite we have no problem, if S is infinite just consider it to be the formual sum.
$A[S] \cong \bigoplus_S A$
This is the set of (set-theoretic) functions $S \to A$ that vanish almost everywhere.

$$A[S] \cong \{f : S \to A : f(s) = 0 \, a.e.\}$$

If M, N, P are A-modules and we have bilinear $f : M \times N \to P$ so that $f(-, n) : M \to P$ and $f(m, -) : N \to P$ are both linear for all m, n,
We sometimes write $(P, f : M \times N \to P)$ as (P, f)
Goal: Associate bilienar maps $f : M \to N \to P$ with a linear map $f' : M \otimes_A N \to P$

Proposition 32 (AM 2.12)**.** Suppose we have A-modules M and N.
i: Existence: $\exists (T, g : M \times N \to T)$ a bilinear map which is 'initial/universal' in the following sense: Any bilinear map factors through this. That is, for any bilienar map $f : M \times N \to P$, there exists a unique map $f' : T \to P$ so that $f' \circ g = f$ [insert commutative diagram here].
ii: Uniqueness: Given $(T, g), (T', G')$ there exists a unique $j : T \to T'$ such that it is an isomorphism and $g' \circ j = g$

We're going to construct g and show that it has this property.

Proof. Existence $\implies$ Uniqueness
Suppose $M \times n \xrightarrow{g} T$ and $M \times N \xrightarrow{g'} T'$ [insert commutative diagram]. We want to say T and T' are the same. By i there exists unique j such that $T \xrightarrow{j} T'$ and we also have a unique $j' : T' \xrightarrow{j'} T$.
Now we have $M \times N \xrightarrow{g} M \times N$ and $M \times N \xrightarrow{g} T$ so there is unique $T \xrightarrow{Id} T$
So we have $j' \circ j = Id$
Proof of Existence:
Let $T \coloneqq \frac{A[M \times N]}{R}$ ['generators $M \times N$ relations']
Where R is the submodule generated by $(m + m', n) - (m, n) - (m', n)$ and $(m, n + n') - (m, n) - (m, n')$ and $(am, n) - a(m, n)$ and $(m, an) - a(m, n)$.
We call $M \otimes_A N \coloneqq T$ and call $m \otimes n \coloneqq [(m, n)]$
We have $g : M \times N \to M \otimes_A N$ so that $g(m, n) \to [(m, n)]$. This is bilinear by definition, and given $f : M \times N \to P$, we have $F : A[M \times N] \to P$ [by exercise 3 in next assignment], thus, since F is bilinear, we have $f' : \frac{A[M \times N]}{R} \to P$
This is true since $R \subset \ker F$.

□

Class 17: 02/16
Recall: Tensor Products are given by $M \otimes_A N = \frac{A[M \times N]}{R}$. We write $\otimes_A = \otimes$
We have universal property: any bilinear map factors through the tensor product [insert commutative diagram here]
We have a map $M \times N \xrightarrow{g} M \otimes N$
Let $m \otimes n \coloneqq g(m, n)$
Then $m_1 \otimes n_1 + \cdots + m_k \otimes n_k \in M \otimes N$
Due to the relations we modded out, we have these relationships:

- $(m + m') \otimes n = m \otimes n + m' \otimes n$

- $m \otimes (n + n') = m \otimes n + m \otimes n'$
- $(am) \otimes n = m \otimes (an) = a(m \otimes n)$

Note, $0_M p \times n = 0_A(0_M \otimes n) = 0_{M \otimes N}$
Basically $0 \times n = 0$

Proposition 33 (AM 2.14)**.** We have the following:
i. $M \otimes N \cong N \otimes M$ with isomorphism $m \otimes n \leftrightarrow n \otimes m$
ii. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$ with isomorphism $(m \otimes n) \otimes p \leftrightarrow m \otimes (n \otimes p)$
iii. $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$ with isomorphism $(m, n) \otimes p \leftrightarrow (m \otimes p, n \otimes p)$
iv. $A \otimes M \cong M$ with $a \otimes m \mapsto am, 1 \otimes m \leftarrow\!\shortmid m$

Proof. i: Consider maps from $M \times N$ to $M \otimes N, N \otimes M$. By universal property there is an invertible map between them.
iv: Consider the maps from $A \times M$ to M and $A \otimes M$. By universal property, there exists a unique map from $A \otimes M$ to M. $a \otimes m \mapsto am$ gives that to us. □

Note that 2.14 immedialtely givs us that:
$A^m \otimes_A A^n \cong (\bigoplus_m A) \otimes A^n \cong \bigoplus_m (A \otimes A^n) \cong \bigoplus_m (A \otimes \bigoplus_n A) \cong \bigoplus_{m,n} A \otimes_A A \cong \bigoplus_{m,n} A \cong A^{mn}$
A $\mathbb{Z}$-module T is <u>torsion</u> if $\forall t$ there exists non-zero n so that $nt = 0$. Basically, every element has an [additive] order.
Exercise: T is torsion if and only if $T \otimes_{\mathbb{Z}} \mathbb{Q} = 0$
for example $T = \mathbb{Q}/\mathbb{Z}$ is torsion.

Proposition 34 (AM Corollary 2.13)**.** If $\sum_i m_i \otimes n_i - 0 \in M \otimes N$ then $\exists$ finitely generated $M_0 \triangleleft M, N_0 \triangleleft N$ so that:
$m_i \in M_0$
$n_i \in N_0$
And $\sum_i m_i \otimes n_i = 0 \in M_0 \otimes_A n_0$

Proof. This is a corollary of the construction
Use the fact that $M \otimes N = \frac{A[M \times N]}{R}$.
$\sum_i m_i \otimes n_i = 0 \implies \sum_i [m_i, n_i] = \sum_j r_j \in R$
Thus, $r_j = \sum_{jk} a_{jk}(m_{jk}, n_{jk})$
Let $M_0 = (m_i, m_{jk}), N_0 = (n_i, n_{jk})$
That gives us the answer.

□

Now we prove the previous fact.

Proposition 35. Let T be a $\mathbb{Z}$ module. Then $T \otimes \mathbb{Q} = 0 \iff T$ torsion

Proof. $\impliedby$ (easy)
For any $t \in T$ there exists $n \neq 0$ so that $nt = 0$.
Then $t \otimes q = t \otimes \frac{n}{n} q = nt \otimes \frac{q}{n} = 0 \times \frac{q}{n} = 0$
$\implies$ (uses the corollary)
Assume $T \otimes \mathbb{Q} = 0$. We want to prove that T is torsion.
For any $t \in T$ we have $t \otimes 1 = 0$
2.13 says: $t \otimes 1 = 0$ in $T_0 \otimes \mathbb{Q}_0$ where $T_0, \mathbb{Q}_0$ are finitely generated.
Since Q_0 is a finitely generated submodule of $\mathbb{Q}$ it has to be $\frac{1}{q}\mathbb{Z} \cong \mathbb{Z}$
Then $T_0 \otimes \frac{1}{n}\mathbb{Z} \cong T_0$ with map $x \otimes \frac{k}{n} \leftarrow\!\shortmid kx$
$t \otimes 1$ must go to nt, since $t \otimes 1 = 0$ we have $nt = 0$.
[???]

□

Definition 56 (Functor)**.** A functor $F : \mathcal{C} \to \mathcal{D}$ is $F : Ob\mathcal{C} \to Ob\mathcal{D}$ so that if we have a morphism, then $F : \mathcal{C}(x, y) \to \mathcal{D}(F(x), F(y))$ such that $F(f \circ g) = F(f) \circ F(g)$ and $F(1_X) = 1_{F(X)}$. So $X \mapsto F(X)$, $X \xrightarrow{f} Y \mapsto F(X) \xrightarrow{F(f)} F(Y)$

Now, $- \otimes_A -$ is a functor.
If we have $f : M \to M'$ and $g : N \to N'$ we can define the corresponding thing on morphism: we have a map $f \otimes g : M \otimes N \to M' \otimes N'$ given by $f(\otimes g)(m \otimes n) = f(m) \otimes g(n)$
Since tensor product is a functor it respects maps.

Proposition 36 (AM 2.18)**.** Tensor Product is Right Exact

This is useful for computation. See Exercise 7. 7 helps in 8.
Suppose $M' \to M \to M'' \to 0$ is exact.
Then, for all N,

$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

is exact. Even the maps are given by $f \otimes 1$ and $g \otimes 1$.

Proof. $(g \otimes 1) \circ (f \otimes 1) = (g \circ f) \otimes 1 = 0 \otimes 1 = 0$
Define: $\overline{g \otimes 1} : \frac{M \otimes N}{im(f \otimes 1)} \to M'' \otimes N$
Take $[m \otimes n] \in \frac{M \otimes N}{im(f \otimes 1)}$. Then $[m \otimes n] \mapsto g(m) \otimes n$
Take $m'' \otimes n$. Since onto, we can lift it: $[\hat{m}'' \otimes n] \leftarrow\!\shortmid m'' \otimes n$ whee $g(\hat{m}'') = m''$
□

AM adjoint proposition: $Hom(M \otimes N, P) \cong Hom(M, Hom(N, P))$ so that $\varnothing \mapsto (m \mapsto (n \mapsto \phi(m \otimes n)))$

Class 18: 02/19

Flat Modules

$- \otimes_A N$ is right exact, but not exact.
For example, $- \otimes_{\mathbb{Z}} \mathbb{Z}/2$ is not exact. Consider the following exact sequence:

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2 \to 0$$

But from homework, tensoring doesn't make it exact.

Definition 57. N is a flat A-module if $- \otimes_A N$ is an exact functor, i.e. any short exact sequence $0 \to M' \to M \to M''$ we have $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is also short exact sequence.

For example A is flat since $M \otimes_A A = M$
A^n is flat since $M \otimes_A A^n = M^n$
Any free module is flat. Recall free module is given by $\bigoplus_S A = A[S], (\bigoplus_S A) \otimes M = \bigoplus_S M$
Note that $\mathbb{Z}/2$ is not a flat $\mathbb{Z}$-module.
Atiyah Macdonald says: $\mathbb{Q}$ is a flast $\mathbb{Z}$ module.
N is a flat $\mathbb{Z}$-module if and only if N is torsion-free, which means it has no element of finite order.

Proposition 37 (AM 2.19)**.** Let N be an A-module. TFAE:

1. $\forall \cdots \to M_{i+1} \to M_i \to M_{i-1} \to \ldots$ exact $\implies \cdots \to M_{i+1} \otimes N \to M_i \otimes N \to M_{i-1} \otimes N \to \ldots$ is exact
2. $\forall 0 \to M' \to M \to M'' \to$ shot exact sequence implies $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ short exact sequence
3. For any injection $M' \to M$ we have an injection $M' \otimes N \to M \otimes N$
4. For any injection $M' \to M$ so that M', M are finitely generated, we have an injection $M' \otimes N \to M \otimes N$

Proof. $1 \iff 2$:
Suppose we have $\cdots \to C_{i+1} \overset{f_{i+1}}{\to} C_i \overset{f_i}{\to} C_{i-1} \to \dots$
Let $B_i = imf_{i+1}, B_{i-1} = imf_i$
Then $\to C_{i+1} \overset{f_{i+1}}{\to} C_i \overset{f_i}{\to} C_{i-1}$ is exact if and only if:
$0 \to B_i \to C_i \to B_{i-1}$ is exact for all i.
So $1 \iff 2$
$2 \iff 3$ by AM 1.18 [right exactness of $- \otimes_A N$]
$3 \implies 4$ 4 is just a special case of 3.
$4 \implies 3$: We use AM 2.13. Consider an injection $f : M' \to M$. Consider $u \in \ker(f \otimes 1 : M' \otimes N \to M \otimes N)$
Let $u = \sum_i x'_i \otimes y_i$
$0 = (f \otimes 1)i = \sum_i f(x'_i) \otimes y_i$ Let $M'_0 = A(x'_i) \lhd M'$
2.13 implies there exists finitely generated $M_0 \lhd M, N_0 \lhd N$ so that $\sum_i f(x'_i \otimes y_i) = 0 \in M_0 \otimes N_0$
WLOG $\overline{M_0} \supset f(M'_0)$. Let $\overline{M_0} = (M_0, f(x'_i))$
Thus $u \in \ker(f \otimes 1)[M'_0 \otimes N \to \overline{M_0} \otimes N]$. By 4, we have $u = 0$ so we're done.
Corollary: $\mathbb{Q}$ is a flat $\mathbb{Z}$ module.
Idea: M finitely generated means $M =$ torsion $\oplus$ free.

□

Restriction and Extension of Sclalars

Extension of Scalars is also called induction.
Suppose we have a homomorphism $f : A \to B$.
Then we have the module homomorphisms:
$f^* : B - mod \to A - mod$
$f_* : A - mod \to B - mod$
Restriction: f^*N is N as an abelian group like $a \cdot n \coloneqq f(a)n$.
AM writes N instead of f^*N
Induction / Extension of Scalars:
$f_*M = B \otimes_A M$ [or $f^*B \otimes_A M$]
Note that B is A-module with $a \cdot b = f(a)b$
f_*M is a B-module by $b'(b \otimes m) = b'b \otimes m$

Proposition 38 (AM 2.16)**.** If N is finitely generated and B is finitely generated as A-module,
f^*N is finitely generated as A-module.

Proposition 39 (AM 2.17)**.** If M is finitely generated A-module then f_* is finitely generated B-module.

$M = A(x_i), f_*M = B(1 \otimes x_i)$
Observaton:
f^* preserves exactness.
f_* preserves freeness.
If $N' \to N \to N''$ is exact then $f^*N' \to f^*N \to f^*N''$ is exact.
$f_*A = B \otimes_A A = B$
$f_*A^n = B^n$

Algebra

:

Definition 58 (Algebra)**.** Consider rings A, B.
If we have a homomorphism $f : A \to B$ we call B an A-algebra

homomorphism of A-algebra: a ring map $B \xrightarrow{h} C$ so that $h \circ f = g$ where $A \xrightarrow{f} B$ and $A \xrightarrow{g} C$
Category: A-algebra $= A \downarrow$ Ring
So, $\mathbb{Z}$-algebra = Ring
Suppose k is a field. If we have $f : k \to B$ then f is injective. So, k-algebra is the same thing as a ring B so that $k \subset B$.
Note that f need not be injective so this is not necessarily true.
If B is an A-algebra $\implies$ B is an A-module with $a \cdot b = f(a)b$.
Consider the following 'competing' definition:

Definition 59. B is a finite A-algebra if B is a finitely generated A-module

Definition 60. B is a finitely generated A-algebra if $\exists b_1, \cdots, b_n$ such that $B = f(A)[b_1, \cdots b_n]$ polynomials with b_i coefficients in $f(A)$

Note that finite $\implies$ finitely generated.
B is a finitely generated A-algebra $\iff$ $\exists A[t_1, \cdots, t_n] \to B$ where $a \mapsto f(a), t_i \mapsto b_i$
eg $\mathbb{C}$ is a finite $\mathbb{R}$-algebra:
$\mathbb{R}[\overline{x}, \overline{y}] = \frac{\mathbb{R}[x,y]}{(y-x^2)}$ is a finitely generated $\mathbb{R}$-algebra but it is not finite.

Class 19:02/21

Proposition 40. If B, C are A-algebras then $B \otimes_A C$ is also an A-algebra

Proof. To give a map out of tensor product, we need to check what it does on pure tensors and then check if it is bilinear. We check the multiplication map:

$$(b_1 \otimes c_1) \cdot (b_2 \otimes c_2) \coloneqq (b_1 b_2) \otimes (c_1 c_2)$$

We want to check if it is well defined. For that, we need to check bilinear. That is trivial.

□

We have Universal Property: An algebra map out of $B \otimes_A C$ is the same thing as giving algebra maps out of B and C.
In other words, if we have algebra maps:

$$f : B \to D$$

$$g : C \to D$$

Then there exists a unique algebra map

$$f \otimes g : B \otimes_A C \to D$$

Such that $f \otimes g(b \otimes 1) = f(b)$ and $f \otimes g(1 \otimes c) = g(c)$
Warning: This is a class on commutative algebra, so we can assume everything is commutative, but in this case commutativity is essential. $(b \otimes 1)$ and $(1 \otimes c)$ commute! This is NOT fine in non-commutativity case. We need a map such that the images of B and D commute.

Rings and Modules of Fractions

If D is a domain [example: $\mathbb{Z}$] we can construct a field of fractions Frac(D) [example: $\mathbb{Q}$] which is constructed as $D \times D_{\neq 0}/\equiv$ an equivalence class so that $(a, s) \equiv (b, t) \iff at - bs = 0$ which we write a/s. We can give it a ring structure by $(a/s) \cdot (b/t) = (ab/st)$ and $(a/s) + (b/t) = (at + bs)/st$.
This is a ring, and $D \hookrightarrow$ Frac(D) by $x \mapsto x/1$. Moreover, Frac(D) is a field with $(a/s) \cdot (s/a) = 1$. So we have a multiplicative inverse as long as $a \neq 0$ but $a = 0$ implies $a/s = 0$ so all non-zero elements have inverses.
We can generalize this construction in two different ways.

First way: General Commutative Rings [not just domains]
Second way: Only inverst some elements [instead of all nonzero elements]
Note that if we make generalization one then we must make generalization two, but not the other way around. This is because we can't invert all elements of general rings.
Example: Dyadic Rationals: Fractions whose denominator is a power of 2. This is a ring.
Another example: fractions with odd denominator. Multiplication of odd denominators is odd, and lcm of odd numbers is odd so this is also rings.
Questions: What kind of subsets of A should we be allowed to invert?
If two things are allowed to be a denominator then their product must also be allowed to be a denominator.
We want 1 to be an allowed denominator since we wand $a \mapsto a/1$ to be a valid map.

Definition 61. $S \subset A$ is a multiplicatively closed subset [not subring or ideal] if $1 \in S$ and S is closed under multiplication.

Definition 62. $S^{-1}A$ is defined as $A \times S/\equiv$ so that $(a,s) \equiv (b,t)$ if $(at-bs)\cdot u = 0$ for some $u \in S$ [we can't use the previous one because in order for it to be an equivalence relationship, we need transitivity which we don't have. So zero divisors play the role of zero].
We still have addition and multiplication like before.

Lemma: $\equiv$ is an equivalence relationa and $S^{-1}A$ is a ring.
Warning: There is always a map $A \to S^{-1}A$ with $x \mapsto x/1$. This will be a ring homomorphism, but if might not be injective anymore.
Example: if $0 \in S$ then $S^{-1}A$ is isomorphic to the zero ring, since everything will be equivalent.
Example: if $S = \{1,2,4\}$ in $\mathbb{Z}/6$ then $S^{-1}\mathbb{Z}/6 \cong \mathbb{Z}/3$
So, if we try to invert a zero divisor, it only kills the things that it multiplies with to make zero. If we try to invert zero then that kills everything so we can only have the zero ring.
Univeral Property If $g : A \to B$ is a ring homomorphism such that $g(s)$ is invertible in B for all $s \in S$, then there exists a unique map $h : S^{-1}A \to B$
[draw commutative diagram of $A, B, S^{-1}A$]
Example, we have a map from $\mathbb{Z}/6$ to $\mathbb{Z}/3$ so it must factor through some $S^{-1}A$ where $S = \{1,2,4\}$

Proof. Uniqueness: $h(a/s)$ must be equal to $h(a/1)\cdot h((s/1)^{-1}) = g(a)\cdot g(s)^{-1}$ so the only possible way to define this map is $h(a/s) = g(a)\cdot g(s)^{-1}$
Existence: Define $h(a/s) \coloneqq g(a)\cdot g(s)^{-1}$ and check that it is well-defined [does it respect equivalence?]
Suppose $(a,s) \equiv (a',s')$. Then $(as'-a's)t = 0$ for some $t \in S$.
Then $(g(a)g(s') - g(a')g(s))g(t) = 0$. Since $g(t)$ is invertible, we can cancel it.
$\implies g(a)g(s') = g(a')g(s) \implies g(a)g(s)^{-1} = g(a')g(s')^{-1}$
So the map indeed exists.

□

Corollary: If $g : A \to B$ is a ring homomorphism such that:

1. $s \in S \implies g(s)$ is invertible
2. $g(a) = 0 \implies as = 0$ for some $s \in S$
3. Every element of B is of the form $g(a)g(s)^{-1}$

Then $\exists! h : S^{-1}A \to B$ that is an isomorphism such that $g = h \circ f$
1 tells us that a map exists, 2 tells us that the map is injective [kernel is 0] and 3 gives us surjectivity.
Example:

In the map $\mathbb{Z}/6 \to \mathbb{Z}/3$ and we have $1 \mapsto 1, 2 \mapsto 2, 4 \mapsto 1$ all of whom are invertible, and $3, 6$ gets mapped to 0 for whom $2 \cdot 3, 1 \cdot 6 = 0$.
Example: If $f \in A$, we can set $S = \{f^n\}_{n \in \mathbb{Z}_{>0}}$. Then we can look at $A_f \coloneqq S^{-1}A$ for this particular S.
This includes the dyadic rationals, $\mathbb{Z}_2$.
Other example: Consider ideal $\mathfrak{p}$. Then $A - \mathfrak{p}$ is multiplicatively closed if and only if $\mathfrak{p}$ is a prime ideal. Then we can take $S = A - \mathfrak{p}$.
$A_{\mathfrak{p}} \coloneqq S^{-1}A$ for this A. We can consider the fractions with odd denominators $\mathbb{Z}_{(2)}$.

Class 20: 02/23
We finish with one more example.
Take $\mathbb{C}[x]$, and localize at the ideal generated by x.
The fraction field of $\mathbb{C}[x]$ are rational functions
$\mathbb{C}[x]_{(x)}$ then are the rational functions defined at 0.
$\mathbb{C}[x]_{(x-a)}$ are the rational functions defined at a

Definition 63. If S is a multiplicatively closed subset of A and M is an A-module then we define $S^{-1}M$ is defined to be $M \times S/\equiv$ so that $(m, s) \equiv (m', s') \iff \exists t \in S, t$ so that $t(sm' - s'm) = 0$

We need to check:
1. $\equiv$ is a equivalence relation
2. $S^{-1}M$ is an $S^{-1}A$-module
Again, we write M_f where f is an element and $M_{\mathfrak{p}}$ where $\mathfrak{p}$ is a prime ideal of A.
Category theory: "S^{-1} is functorial". That is to say, not only does it make sense to apply S^{-1} to a module, but it also makes sense to apply S^{-1} to maps.
If $f : M \to N$ is a map then we have the map $S^{-1}f : S^{-1}M \to S^{-1}N$ that is defined by: $\frac{m}{s} \mapsto \frac{f(m)}{s}$.
Check that it is a module.
We also need: $S^{-1}(id_M) = id_{S^{-1}M}$
$S^{-1}(f \circ g) = S^{-1}f \circ S^{-1}g$

Proposition 41. S^{-1} is exact.

What does this mean?
If we have $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact, then:

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

Is exact.
Corollary: If f is injective then $S^{-1}f$ is injective.
If f is surjective then $S^{-1}f$ is surjective.
Proof is by putting 0 in the exact sequence.

Proof. We want to show that:
$\ker(S^{-1}g) = \operatorname{im}(S^{-1}f)$.
We are going to show inclusion in both direction.
$\ker(S^{-1}g) \supseteq \operatorname{im}(S^{-1}f)$ by functoriality.
For $\subseteq$:
Suppose $\frac{m}{s} \in S^{-1}g$.
Then, $S^{-1}g(\frac{m}{s}) = 0$
$S^{-1}g(\frac{m}{s}) = \frac{g(m)}{s}$
Thus, there exists $t \in S$ such that $t \cdot g(m) = 0 \implies g(tm) = 0 \implies tm \in \ker g = \operatorname{im} f$
So, $f(x) = tm \implies S^{-1}f(\frac{x}{ts}) = \frac{mt}{ts} = \frac{m}{s}$
□

Corollary:
If N, P are submodules of M,

1. $S^{-1}(N + P) = S^{-1}N + S^{-1}P$

2. $S^{-1}(N \cap P) = S^{-1}M \cap S^{-1}P$

3. $S^{-1}(M)/S^{-1}(N) \xrightarrow{\sim} S^{-1}(M/N)$

Proof. 1. We use the definition and how we add fraction.
2. $S^{-1}(N \cap P) \subseteq S^{-1}M \cap S^{-1}P$ is easy.
For $\supseteq$, suppose $\frac{y}{s} = \frac{z}{t}$ where $y \in N, z \in P$.
So, there exits $u \in S$ so that $u(ty - sz) = 0 \implies \exists w = uty = usz$.
Thus, $w \in N \cap P$.
Finally, $\frac{y}{s} = \frac{w}{uts}$
3. [this is actually the corollary].
Take the exact sequence:

$$0 \to N \to M \to M/N \to 0$$

Then,

$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$$

Thus, first map is injective, last map is surjective, kernel is image.
Thus $S^{-1}(M/N) \cong S^{-1}(M)/S^{-1}(N)$

□

Proposition 42. $S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$

Proof. We prove it works on pure tensors and check it's bilinear.

$$\frac{a}{s} \otimes m \mapsto \frac{am}{s}$$

This is a map of $S^{-1}A$-modules. It exists by the universal property of tensor products since it is bilinear.
It is also an $S^{-1}A$ module map.
It is also surjective: everything of $S^{-1}M$ is of the form $\frac{m}{s}$. We have: $\frac{1}{s} \otimes m \mapsto \frac{m}{s}$
For injectivity:
Lemma: Every element of $S^{-1}A \otimes M$ is of the form $\frac{1}{s} \otimes m$.
Note that usually tensor products are usually huge sum. The way we write it as one sum is: common denominators!

$$\sum_{i=1}^{n} \frac{a_i}{s_i} \otimes m_i = \frac{1}{\prod s_i} \sum_i \left(\prod_{j \neq i} s_j \right) a_i \otimes m_i = \sum_i \frac{1}{s} t_i a_i \otimes m_i$$

$$= \sum_i \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \sum_i a_i t_i m_i = \frac{1}{s} \otimes m$$

Thus we have proved the lemma.
Suppose $0 = f(\frac{1}{s} \otimes m) = \frac{m}{s}$, then $\exists t \in S$ so that $mt = 0$ thus $\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0$.
So, the kernel is 0 and thus it is injective.

□

Class 21: 02/26
Localization review.
Suppose we have a ring A and a multiplicatively closed set S.

Definition 64. $S \subset A$ is multiplicatively closed [mc] if S is a submonoid of $(A, \times)$.
By monoid, we mean $1 \in S, a, b \in S \implies ab \in S$.

In this situation, we can localize, or invert in S.
If M is an A-module, we define an equivalence relation on $M \times S$ so that $(m, s) \sim (m', s')$ if there exists $s'' \in A$ such that $(ms' - m's)s'' = 0$
We write $\frac{m}{s} = [(m, s)]$ the equivalence class.
We write $S^{-1}M = M \times S/\sim$.
$S^{-1}M$ is an abelian group.
$\left(\frac{m}{s} + \frac{m'}{s'}\right) = \frac{ms'+sm'}{ss'}$
If $M = A$ then $S^{-1}A$ is a ring, $\left(\frac{a}{s}\right)\left(\frac{a'}{s'}\right) = \frac{aa'}{ss'}$
We have a map $f : A \to S^{-1}A$ given by $a \mapsto a/1$.
f is S-inverting ($f(S) \subset (S^{-1}A)^\times$) and initial.
Universal Property (3.1):
If $g : A \to B$ is S-inverting, that is, $g(S) \subset B^\times$ then g factors through the map $f : A \to S^{-1}A$ so we have a unique map h so that $h \circ f = g$.
Examples: If $0 \in S$, that's bad because we shouldn't be able to invert S. Then $S^{-1}A = 0$.
If A is a domain and $S = A - 0$, then $S^{-1}A = Frac(A)$.
An ideal I of A is prime if and only if $A - I$ is multiplicatively closed. This is just the contrapositive of the definition of the prime ideal.
If we have a prime ideal P in A then $A - P$ is multiplicatively closed, then A_P is defined to be $(A - P)^{-1}A$, and it is called the localization of A at P.
A_P is a local ring with maximal ideal PA_P.
We have a correspondence: Ideals of $A_p \leftrightarrow \{I \lhd A | I \subset P\}$
Note that $A \to S^{-1}A$ is injective if and only if $S \subset$ non-zero divisors.
If we have $f \in A$ then we can look at the multiplicatively closed subset $\{1, f, f^2, \cdots\}$ and then we can look at $\{1, f, f^2, \cdots\}^{-1}A$. AM notation for this is A_f, better notation is $A[\frac{1}{f}]$.
Example: $\mathbb{Z}_{(2)}$, where we invert everything outide (2) so it is $\{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, 2 \not| b\}$. This contains $\mathbb{Z}$.
Also, $\mathbb{Z}_2 = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^k} \in \mathbb{Q}\}$
In 3.3, we proved $S^{-1} : A - mod \to S^{-1}A - mod$ is flat.
A functor F is flat if it takes exact sequences to exact sequences, and $- \otimes_A M$ is flat then we say the module M is flat.
In 3.5, we proved $S^{-1}A \otimes_A M \xrightarrow{\approx} S^{-1}M$.
3.3 and 3.5 implies corollary 3.6:
$S^{-1}A$ is a flat A-module, since $S^{-1}A \otimes -$ is flat.
For example, $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.
Also, 3.5 and chapter 2 implies Proposition 3.7, which says $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \xrightarrow{\approx} S^{-1}(M \otimes_A N)$

Local Properties

Proposition 43 (AM 3.8)**.** "Being zero is a local property".
Let M be an A-module. Then TFAE:

1. $M = 0$
2. $M_P = 0 \forall$ prime $P \lhd A$
3. $M_I = 0 \forall$ maximal ideal $I \lhd A$

Proof. 1 implies 2 is obvious, 2 implies 3 since all maximal ideals are prime.
Instead of 3 implies 1 we prove the contrapositive.
$M \neq 0 \implies \exists x \neq 0 \in M$.
Thus, $Ann(x)$ is a proper ideal of A since it doesn't contain 1.
By Zorn's lemma, $Ann(x)$ is contained in a maximal ideal I.
For all $s \in A - I, s \notin Ann(x)$ thus $sx \neq 0$.
$\frac{x}{1} \neq M_i$ is nonzero if and only if $\forall s \in A - I, sx \neq 0$, which we proved before.

Thus, $M_I \neq 0$.

□

Proposition 44 (AM 3.9)**.** Let $\phi : M \to N$ be a module map. Then TFAE:

1. Φ is 1-1.
2. Φ_P is 1-1 for all prime P.
3. Φ_I is 1-1 for all maximal I.

Same hold for onto.

Proof. 1 implies 2 is true since localization is exact [3.3]. Think of the morphism $\Phi_P : M_P \to N_P$
2 implies 3 since maximal are prime.
3 implies 1 since if $\phi : M \to N$ and let M' be the kernel of Φ then we have the exact sequence $0 \to M' \to M \to N$ is exact, and by 3.3 we have $0 \to M'_I \to M_I \to N_i$ is exact, and by the hypothesis we must have $M'_I = 0$ for all I , and by 3.8 we have $M' = 0$ therefore Φ is injective.
For the onto part, reverse the arrows. □

Proposition 45 (AM 3.10)**.** 'Flatness is a local property'.
A module is flat if and only if its localization and prime ideals are flat [or maximal].

Class 22: 02/28

Proposition 46 (AM 3.10)**.** "Flatness is a Local Property"
Let M be an A-module. Then the following are equivalent:

1. M is flat, that is tensor with M is an exact functor
2. For all prime $P \triangleleft A$, M_P is flat A_P module
3. For all maximal $I \triangleleft A$, M_I is flat A_I module.

Proof. $i \implies ii$:
Note, flatness means it takes injective maps to injective maps.
Suppose M is flat, and we have a injective map $N \to Q$ of A_P modules.
Then $M \otimes_A N \to M \otimes_A Q$ is injective since M is flat
Then $A_P \otimes_A M \otimes_A N \to A_P \otimes_A M \otimes_A Q$ is injective since $S^{-1}A$ is a flat A-module
Note that $A_P \otimes_A M \otimes_A N = M_P \otimes_{A_P} N$ and $A_P \otimes_A M \otimes_A Q = M_P \otimes_{A_P} Q$
So, $M_P \otimes_{A_P} N \to M_P \otimes_{A_P} Q$ is injective
Thus M_P is flat A_P module.
$ii \implies iii$ follows from the fact that maximal ideals are prime.
$iii \implies i$:
Suppose $N \to Q$ is injective A-module map. Since injectivity is a local property [3.9] we have for all maximal I, $N_I \to Q_I$ is injective.
Therefore, for all I, $M_I \otimes N_I \to M_I \otimes Q_I$ is injective [since M_I is flat by hypothesis]
Note that $M_I \otimes N_I = (M \otimes N)_I$ and $M_I \otimes Q_I = (M \otimes Q)_I$ by 3.7
Therefore, $M \otimes N \to M \otimes Q$ is injective by 3.9, injectivity is local property.

□

Extension, Contraction, Localization

Preview: Corollary 3.13:
We can look at ideals in A_P where P is prime, which is equal to $(A - P)^{-1}A$ by definition.
We want to show that ideals in A_P are in a bijective correspondence with ideals $I \subset P \triangleleft A$.
$I \subset P \triangleleft A, I \cap S = \varnothing \overset{c,\approx}{\longleftarrow}$ ideals in A_P
So, we have $f^{-1}J \longleftarrow J$ where $f : A \to S^{-1}A$.

Example: consider $\mathbb{Z}_{(2)}$. This has ideals $\frac{a}{odd} \in \mathbb{Z}_{(2)}$.
Then contraction gives us ideals $\mathbb{Z}2^k$ of $\mathbb{Z}$
In general, if we have $f : A \to B$, we have a correspondence between $I \lhd A$ and $J \lhd B$ by extension and contraction: $J^c = f^{-1}(I)$ and $I^e = Bf(I)$
If $C = \operatorname{im} c$ and $E = \operatorname{im} e$ then we have a bijection from C to E.
Now we are going to apply this to $A \to S^{-1}A$.
$I^e = S^{-1}I = \{\frac{f(i)}{s} | s \in S, i \in I\}$

Proposition 47 (AM 3.11)**.** i: Every ideal in $S^{-1}A$ is extended
ii: $I \lhd A \implies I^{ec} = \bigcup_{s\in S}(I : s)$
ii': $I^e = (1) \iff I \cap S \neq \varnothing$
iii: $I \in C \iff$ no element of S is zero divisor in A/I
iv:

Proof. i: Suppose $J \lhd S^{-1}A$. We have $J \supset J^{ce}$ by 1.17
Consider $\frac{x}{s} \in J$ this implies $\frac{x}{1} \in J$ this implies $x \in J^c$ this implies $\frac{x}{s} \in J^{ce}$
So $J \subset J^{ce}$. Therefore $J = J^{ce}$ so J must be an extended ideal
ii:
Recall $(I : s) = (I : (s)) = \{x | xs \in I\}$ 'ideal quotient'
$x \in I^{ec} = (S^{-1}I)^c$
$\iff \frac{x}{1} = \frac{i}{s} \in S^{-1}A$ for $i \in I, s \in S$
$\iff (xs - i)s' = 0 \in A$ where $i \in I, s, s' \in S$
$\iff xss' \in I$
$\iff xs'' \in I$
$\iff x \in (I : s'')$
iii: $I \in C \iff I^{ec} = I$
$\iff (sx \in I \implies x \in I)$
$\iff \overline{s}$ is not zero divisor in A/I

□

Class 23: 03/01

$$\{\text{ideals } (2^k) \lhd \mathbb{Z}\} \longleftrightarrow \{\text{ideals of } \mathbb{Z}_{(2)}\}$$

$$\mathbb{Z}/2^k\mathbb{Z} \cong \mathbb{Z}_{(2)}/2^k\mathbb{Z}_{(2)}$$

Proposition 48 (AM 3.11)**.** Consider $A \mapsto S^{-1}A$.

i Every ideal in $S^{-1}A$ is extended

ii $I^{ec} = \bigcup_{s\in S}(I : s)$, $(I : s) = \{x \in A | xs \in I\}$

iii I contracted if and only if $\operatorname{im}(S \to A/I) \subset nzd(A/I)$

iv $\{\text{prime } P \lhd A, P \cap S \neq \varnothing\} \overset{\text{bijection}}{\longleftrightarrow} \{\text{prime ideals in } S^{-1}A\}$

v S^{-1} commutes with finite sums, finite products, finite intersections and radicals.

For v, we use 1.18 and 3.4.

Proof. (iv):
Map from left to right: $P \mapsto P^e$
Map from right to left: $Q \mapsto Q^c$
Pick prime $Q \lhd S^{-1}A$. Note that Q^c is a prime ideal.
[Q^c is prime if and only if A/Q^c is a domain, which embeds $A/Q^c \hookrightarrow S^{-1}A/\mathbb{Q}$ which is a domain].
$Q = Q^{ce}$ by (i). So we get an identity. So contraction has a one sided inverse.
Suppose we have prime $P \lhd A$. Then A/P is a domain. Let $\overline{S}$ be the image of S in A/P. Then $\overline{S}^{-1}(A/P) = S^{-1}A/S^{-1}P$ [which is 3.4].
We have two cases here. Case 1: when this ring is zero, case 2: where it is nonzeo.

Case 1: $\overline{S}^{-1}(A/P) = 0$: This means $0 \in \overline{S}^{-1}$ which means $S \cap P \neq \varnothing$ so it doesn't satisfy the condition.
Case 2: $\overline{S}^{-1}(A/P) \neq 0$. This implies $S \cap P = \varnothing$, thus $\overline{S}^{-1}(A/P) \subset Frac(A/P) \implies S^{-1}A/S^{-1}P$ is a domain, thus $S^{-1}P = P^e$ is prime.
Corollary 3.12: $Nil(S^{-1}A) = S^{-1}Nil(A)$

□

Proof. Follows from 3.11 □

Corollary 3.13 Suppose $P \triangleleft A$ is prime. Then,

$$\{\text{prime ideal of } A \subset P\} \longleftrightarrow \{\text{prime ideals of } A_{\mathbb{P}}\}$$

Proof. Let $S = A - P$ and use 3.11(iv). □

Remark: P, Q prime in A. Then Spec is a contravariant function:

$$Spec(A_p) \hookrightarrow Spec(A)$$

We also have:

$$Spec(A/P) \hookrightarrow Spec(A)$$

Image in $P' \supset P$
Suppose we have $P \subset Q \triangleleft A$ where P, Q are prime. consider:

$$\operatorname{im} SpecA_Q \cap \operatorname{im} Spec(A/P) = \{P \subset sP' \subset\}, A/Q/P \cong A/P_{\overline{Q}}$$

And also $A_Q/S^{-1}P \cong A/P_{\overline{Q}}$
When $P = Q$ $A_P/P = Frac(A/)$
residue field.

Proposition 49 (AM 3.14)**.** Suppose M is a finitely generated A-module. Then,

$$S^{-1}Ann(M) = Ann(S^{-1}M) \triangleleft S^{-1}A$$

Proof. Case 1: M is cyclic

$$0 \to Ann(M) \to A \to M \to 0$$

$$0 \to S^{-1}AnnM \to S^{-1}A \to S^{-1}M \to 0$$

$$S^{-1}M = \frac{S^{-1}A}{S^{-1}AnnM}$$

$$0 \to S^{-1}Ann(M) \to S^{-1}A \xrightarrow{\pi} S^{-1}M \to 0$$

$Ann(S^{-1}M) = \ker \pi = S^{-1}Ann(M)$
Case 2: Assume we have $S^{-1}Ann(M) = Ann(S^{-1}M)$
$S^{-1}Ann(N) = S^{-1}Ann(S^{-1}N)$
Claim: $S^{-1}Ann(M+N) = Ann(S^{-1}(M+N))$
Note tha the claim implies the proposition.
proof of claim:
$S^{-1}Ann(M+N) = S^{-1}(Ann(M) \cap Ann(M))$ [2.2]
$= S^{-1}AnnM \cap S^{-1}AnnN$ [3.11(v)]
$= Ann(S^{-1}M) \cap Ann(S^{-1}N)$ [hypothesis]
$= Ann(S^{-1}M + S^{-1}N)$ [2.2]
$= Ann(S^{-1}(M+N))$ so we're done.

□

Corollary 3.15: Suppose we have $N, P \triangleleft A$, P finitely generated. Maybe P is not prime. Then,

$$S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$$

Proposition 50 (AM 3.16)**.** For a general homomorphism $f : A \to B$ and prime $P \triangleleft A$, $P \in C \iff P = P^{ec}$

Class 24: 03/04

Some Algebraic Geo

Let k be a field, and $I \triangleleft k[x_1, \ldots, x_n]$
$f \in k[x_1, \cdots, x_n]$ gives function $f : k^n \to k$
By the evalutation map $f(a_1, \cdots, f(a_n))$.
Given a polynomial f we can look at its variety, $V(f) = f^{-1}(0) = \{\mathbf{a} \in k^n : f(a_1, \cdots, a_n) = 0\}$
If $f \neq 0$ then $V(f) \subset k^n$ is called a hypersurface.

For example draw $V(x_2^2 - x_1(x_1^2 - 1))$ or $V(x_2^2 - x_1^2(x_1 + 1))$ or $V(x_3^{2-(x_1^2+x_2^2)})$ or $V(x_2^2 - x_1x_2 - x_1^2x_2 + x_1^3)$ which is $V((x_2 - x_1)(x_2 - x_1^2))$. The last case is reducible: a variety is reducible if it is union of two varieties.
Suppose $S \subset k[x_1, \cdots, x_n]$

Definition 65. $\mathcal{V}(S) = \bigcup_{f \in S} \mathcal{V}(f) \subset k^n$

Remark: $V(S) = V(I(S))$ where $I(S)$ is the ideal generated by S.

Definition 66. A variety is a subset of k^n of the form $\mathcal{V}(I)$ for some ideal $I \triangleleft k[x_1, \cdots, x_n]$.

Suppose $X \subset k^n$ ideal of X
$I = \{f \in k[x_1, \cdots, x_n] : f(X) = 0\} \triangleleft [x_1, \cdots, x_n]$
If $X = k^n$ define the coordinate ring of X.
$\Gamma[X] = \frac{k[x_1, \cdots, x_n]}{I(X)}$
Then each $[f] \in \Gamma[X]$ defines $f : X \to k$ by $[f](X) = f(x)$
Lemma:

- $S \subset I(V(S))$ for any $S \subset k[x_1, \cdots, x_n]$
- $X \subset V(I(X))$ for any $X \subset k^n$
- $I(X) = I(V(I(X)))$ for ideal $I \subset k[x_1, \cdots, x_n]$
- $V(S) = V(I(V(S)))$ for any $X \subset k^n$

Now, in 0 characeristics, $V(f) = V(f^n)$.
In a general ring, $\sqrt{I} = \{a \in A : a^n \in I\}$ and $Nil(A) = \sqrt{0}$. A is a reduced ring $NilA = 0$ aka $\sqrt{0} = 0$
Lemma:
$I(X)$ is a radical ideal and $\Gamma(X)$ is a reduced ring.

Definition 67. A variety V is reducible if $V = V_1 \cup V_2$ where V_i are varieties with $V_i \neq V$

eg $V(x_1x_2)$ is reducible.
We also have the following lemama:
The following are equivalent:

- V is irreducible
- $\Gamma(V)$ is a domain

- $I(V)$ is a prime ideal

from definiton we already have 2nd iff 3rd.
In AM: variety, in others algebraic set.
AM: irreducible variety, in others variety
Important theorems: Hilbert Basis ts,heorem and Nullstellensatz.

Theorem 15 (Hilbert Basis Theorem)**.** Any ideal $I \triangleleft k[x_1, \cdots, x_n]$ is finitely generated.
Equivalently, any variety is intersection of finite number of hypersurfaces.

Questin: is a variety the intersection of n hypersurfaces?

Theorem 16 (Nullstellensatz)**.** Explanation: zero place theorem. We need k be algebraically closed.

1. (Weak Nullstellensatz) Let $I \triangleleft k[x_1, \cdots, x_n]$ be a proper idal. Then $V(I)$ is non-empty.
2. (Strong Nullstellensatz) $I(V(I)) = \sqrt{I}$

Exam review recitation
6 question.
We have $ED \implies PID \implies UFD$
PID is nicer than UFDs. If all primes are maximal ideals, then UFD is a PID.
Example: $\mathbb{Z}[x]$ is not a PID, since $\mathbb{Z}[x]/(x) = \mathbb{Z}$ which is not a field but an integral domain, which means (x) is prime but not maximal. $(2, x)$ contains it, for example.
Galois theory:
Cyclotomic polynomial: $\Phi_n(x)$ product of (x - primitive roots)
eg find $\Phi_{10}(x)$
We have $\Phi_{10}(x) | x^{10}-1 = x^{10}-1 = (x^5-1)(x^5+1) = (x^5-1)(x+1)(x^4-x^3+x^2-x+1)$
So we have $x^4 - x^3 + x^2 - x + 1$
order of galois group is also 4. So it is $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$
$Nil(A)$ = intersection of primes
$Jac(A)$ intersection of max
$A \cong A_1 \times A_2$ if and only if there exists nontrivial idempotent
$Spec(A)$ is all prime ideals of A.
$f : A \to B$ gives us $Spec(f) : Spec(B) \to Spec(A)$
This means Spec is a contravariant functor
Nakayama's Lemma.
If M if finitely generated and $I \subset Jac(A)$ and $IM = M$ then $M = 0$
If A is a local ring with max ideal I and M finitely generated and $\frac{A}{I} \otimes_A M = 0$ then $M = 0$
If k is a field and M, N are k algebra then $M \otimes_k N$ is a k algebra, and so $(a \otimes b)(c \otimes d) = ac \otimes bd$
If M, N are finitely generated then M, N are finite dimensional with basis e_i and f_j respectively. $M \otimes_k N$ is also a finite dimensional vector space with basis $\{e_i \otimes f_j\}$

Class 25: 03/08
We skip chapter 4.

Chapter 5: Integrality/Valuations

It's analogous to what we learned from fields.
Suppose we have a field extenstion K over k.

Definition 68. $x \in K$ is algebraic over $k \iff$ it satisfies some polynomial, aka

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

where all $a_i \in k$ not all zero
$\iff |k[x] : k| < \infty$

What about rings? Suppose we have $x \in B$ where B is a ring over A.
Throughout today, A is a subring of B. It does contain the identity. We will also have $x \in B$.

Definition 69. $x \in B$ is integral over A if there exists an equation:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with $a_i \in A$.
Notice that the polynomial is monic.
i.e. x is a root of a monic polynomial in $A[t]$.

We can think of $k \in K$, or we can look at $\mathbb{Z} \subset \mathbb{Q}$, we can think of $\mathbb{Z} \subset \overline{\mathbb{Q}}$ or $\mathbb{Z} \subset \mathbb{Q}[i]$ or $\mathbb{Q}[t] \subset \mathbb{Q}(t^{\frac{1}{2}})$
If we have $k \subset K$ extension of fields, then x integral $/k$ is the same thing as saying x is algebraic $/k$, since we can divide by the leading term.
5.0 claim: $x \in \mathbb{Q}$ integral over $\mathbb{Z} \implies x \in \mathbb{Z}$

Proof. Suppose $x = \frac{r}{s}$ with r, s integers, $(r, s) = 1$. So,

$$(\frac{r}{s})^n + a_1(\frac{r}{s})^{n-1} + \cdots + a_0 = 0$$

$$\implies r^n = -a_1 r^{n-1} s - \cdots - a_0 s^n$$

Thus, $s \mid r^n$ but since $(r, s) = 1$ this implies $s \mid \pm 1$ which means $x \in \mathbb{Z}$

□

Now, consider $\mathbb{Z} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$.
Recall that $\overline{\mathbb{Q}}$ is $\{x \in \mathbb{C} : x \text{ algebraic over } \mathbb{Q}\}$, these are called 'algebraic numbers'
It is due to Gauss that $\mathbb{C}$ is algebraically closed.
Define $\mathbb{A} = \{x \in \mathbb{C} : x \text{ integral over } \mathbb{Z}\}$. These are called 'algebraic integers'. For example, $\sqrt{2} \in \mathbb{A}$
Note that $\frac{1}{5} \notin \mathbb{A}$
Is $\mathbb{A}$ a ring?

Theorem 17 (Proposition 5.1)**.** : we have A a subring of B and $x \in B$. Then TFAE:

1. x integral / A
2. $A[x]$ is a finitely generated A-module
3. There exists subring C such that $A[x] \subset C \subset B$ and C is finitely generated as A-module.
4. $\exists A[x]$ module M which is faithfull ($Ann(M) = 0$) and M is finitely generated.

Proof. We prove $1 \implies 2 \implies 3 \implies 1$ we will not use iv. AM uses 2.4 [the determinant trick]
Assume we have $x^n + a_1 x^{n-1} + \cdots + a + 0 = 0$.
Claim: $A[x] = (1, x, \cdots, x^{n-1}) = I$. If this is true we have $A[x]$ is finitely generated.
Note that, $x^n = -a_1 x^{n-1} - \cdots - \cdots - a_0 \in I$.
Multiplying by x^{n+r} we see that this is also in I by induction. Thus we are done.
$2 \implies 3$ just take $C = A[x]$
$3 \implies 1$: Suppose C is generated by $c_1, \cdots, c_n$. We have, $xC \subset C$. This implies,

$$x \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = [a_{ij}] \begin{bmatrix} c_1 \\ \cdots \\ c_n \end{bmatrix}$$

Since $xc_1 = a_{11}c_1 + \cdots + x_{1n}c_n$
Thus,

$$\implies (xI - (a_{ij})) \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

But we need to prove the last implication. So we multiply by the adjugate on the left. Just see proof of 2.4.
Thus,

$$dI \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

This means $dc_i = 0$ for all i. Since $1 \in C, 1 = \sum_i f_i c_i$ so all can't be 0 Which means $d = 0$ whih gives us a monic polynomial.

□

Now we do a sequence of definitions which we'll use to answer whether the set of algebraic integers is a ring.

Definition 70. B is integral over A if every $x \in B$ is integral. B can also be called an integral extension.

Definition 71. Integral closure of A in B
notation: $IC(A \subset B) = \{x \in B : x \text{ is integral / } A\}$

Definition 72. A is integral closed in B if $A = IC(A \subset B)$. Exxample: $\mathbb{Z}$ is integral closed in $\mathbb{Q}$

Definition 73. A domain A is integrally closed if it is integrally closed in $Frac(A)$ eg $\mathbb{Z}$ is integrally closed.

Two obvious question about integrably closed $IC(A \subset B)$:
One: Is this a ring? we are going to say yes, it's a consequence of the theorem.
Two: Is $IC(A \subset B)$ integrally closed in B?
Corollary 5.2: Let $x_1, \cdots x_n \in B$ be integral / A. Then [this statement is stronger than AM]

1. $A[x_1, \cdots, x_n]$ is finitely generated A-module [this is in AM]
2. $A[x_1, \cdots x_n]$ is intgegral / A

Proof. 1: by induction on n. For $n = 1$ we want to know if $A[x_1]$ is a finitely generated A-module which is implied by 5.1. Assume $A_{n-1} \coloneqq A[x_1, \cdots, x_{n-1}]$ is a finitely generated A-module. Then, $A_{n-1}[x_n]$ is a finitely generated A_{n-1} module, and the previous things imply A_n is finitely generated A-module.
2: Let $x \in A[x_1, \cdots, x_n]$. Then, $A \subset A[x] \subset A[x_1, \cdots, x_n]$. Since 3 implies 1 in 5.1 this implies x is integral over A. □

Thus, x, y integral over A implies $x + y, xy$ integral over A.
Also, corollary: $IC(A \subset B)$ is a ring.
corollary: $\mathbb{A}$ is a ring.

Class 26: 03/18
Subring $A \subset B$
$x \in B$ is integral over A $\exists$ monic $f \in A[t]$ such that $f(x) = 0$
eg $x \in A$ is a root of $t - x$

Definition 74. B is integral over A if $\forall x \in B, x$ is integral over A. For example, $\mathbb{Z}[i]$ is integral over $\mathbb{Z}$ since if $x = a + ib$ then $(t - (a + ib))(t - (a - ib)) \in \mathbb{Z}[t]$

Definition 75. Integral closure of A in B

$$IC(A \subset B) = \{x \in B \mid x \text{ integral over } A\}$$

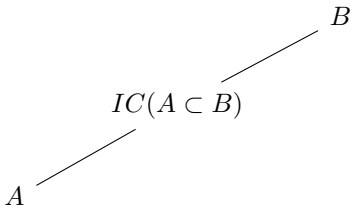
Corollary 5.3: $IC(A \subset B)$ is a ring
Corollary 5.4: 'transitivity'
If we have B is integral over A and C is integral over B then C is integral over A

Proof. If $x \in C$ then there exists:

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

$b_i \in B$. We had $B' = A[b_1, \cdots, b_n]$ a finitely generated A-module.
$B'[x]$ is a finitely generated B'-module, so $B'[x]$ is a finitely generated A-module.
By 5.1(iii) we have x is integral over A. □

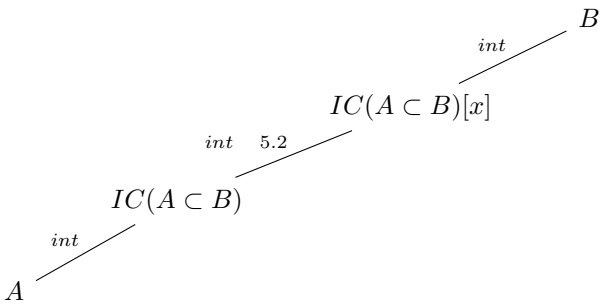
We have



Definition 76. A is integrally closed in B if $A = IC(A \subset B)$

eg $\mathbb{Z} \subset \mathbb{Q}$ is I.C.
eg $\mathbb{Q} \subset \mathbb{R}$ not I.C.
$\sqrt{2} \in IC(\mathbb{Q} \subset \mathbb{R})$, $\sqrt{2} \notin \mathbb{Q}$
$\mathbb{Z} \subset \mathbb{Z}[i]$ not I.C.
Corollary 5.5: $IC(A \subset B)$ is I.C. in B

Proof. Let $x \in B$ be integral over $IC(A \subset B)$. We have:



5.4 implies $IC(A \subset B)[x]$ is integral over A which means x is integral over A □

Proposition 5.6: Suppose B is integral over A. Then,
i: $J \triangleleft B, I = A \cap J$ implies B/J is integral over A/I
ii: If S is multiplicatively closed subset of A then $S^{-1}B$ is integral over $S^{-1}A$.

Proof. $\forall x \in B$ we have the equation *:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for i: reduce * mod J
ii: Let $\frac{x}{s} \in S^{-1}B$ where $x \in B$, then multiply * by s^{-n}

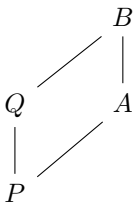
□

Remark/Definition: B is an integral A-algebra if:
We have a ring homomorphism $f : A \to B$ and B is integral over $f(A)$
We can define more generally over subrings.
Note: finite type + integral = finite
finite type means finitely generated as an A-module and finite means finitely generated as A-algebra.
This follows from 5.1 and 5.2.

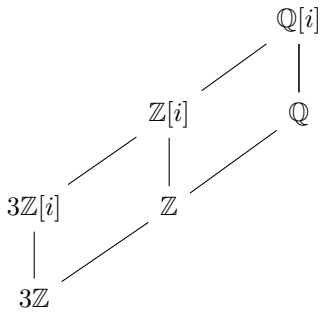
Example: $\mathbb{Z}/6[t]$ is not integral $\mathbb{Z}$-algebra. But $\mathbb{Z}/6$ is integral as $\mathbb{Z}$-algebra.
Recall, if we have a field k then x is algebraic over k if and only if $k[x]$ is a field.

Going Up Theorem

Suppose we have rings $A \subset B$ and prime ideals $P \triangleleft A$ and $Q \triangleleft B$,
If we have $P = Q^c = A \cap Q$ then:



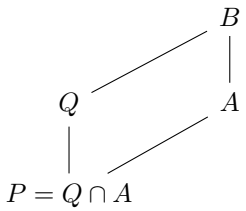
We say Q lies above P
We also say P lies below Q.
We have:



Claim: $3\mathbb{Z}[i]$ is prime in $\mathbb{Z}[i]$
Proof:

$$\frac{\mathbb{Z}[i]}{(3)} = \frac{\mathbb{Z}[t]/(t^2+1)}{(3)} = \frac{\mathbb{Z}[t]}{(3, t^2+1)} = \frac{\mathbb{F}_3[t]}{(t^2+1)} = \mathbb{F}_q$$

Observation: If we have $A \subset B$ and



For all prime $Q \triangleleft B$ there exists prime P lying under Q.
$A/P \hookrightarrow B/Q$ domain.
Proposition 5.7: If $A \subset B$ domains, B is integral over A then A is a field if and only if B is a field.
Proof: $\implies$: $0 \neq y \in B$, choose smallest degree polynomial $y^n + a_1 y^{n-1} + \cdots + a_n = 0$.
Since domain, $a_n \neq 0$ Solve for a_n and factor for y. We have:

$$y\left[\frac{-y^{n-1} - \cdots - a_{n-1}}{a_n}\right] = 1$$

So $y^{-1} \in B$ so we have field.
$\impliedby$: suppose $0 \neq x \in A$. THen $x^{-1} \in B$ which is integral over A so we have polynomial:
$x^{-m} + a_1' x^{-m-1} + \cdots + a_m' = 0$
Solve fore x^{-m} and multiply by x^{m-1}

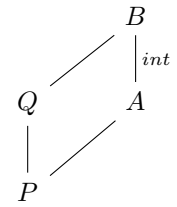
$$x^{-1} = -(a_1' + \cdots + a_m x^{m-1}) \in A$$

So a field.

Class 27: 03/20
Recall

Proposition 51 (AM 5.7)**.** If $A \subset B$ and B is a domain, B is integral over A, then A is a field if and only if B is a field.

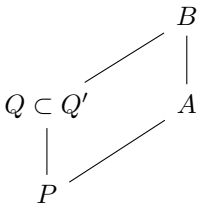
In the same spirit, if x is algebraic over k then $k[x]$ is a field.
Corollary 5.8: If we have



Then Q maximal if and only if P maximal.

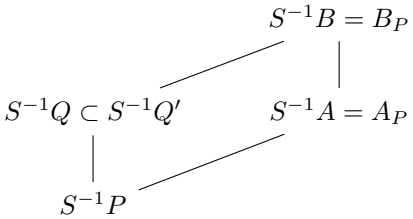
Proof. B/Q is integral over A/P by 5.6.
Q maximal iff B/Q field iff A/P field iff P maximal. □

Corollary 5.9:



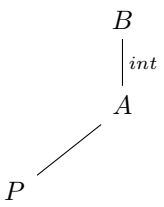
$Q \cap A = P, Q' \cap A = P$
then $Q = Q'$

idea. Replace A by local A_P and use 5.8.
$S = A - P \subset A$. Then,



$S^{-1}P$ is maximal since A_P is local, which gives us $S^{-1}Q \subset S^{-1}Q'$ maximal by 5.8 which tells us $S^{-1}Q = S^{-1}Q'$. Therefore, $(S^{-1}Q)^c = (S^{-1}Q')^c \implies Q = Q'$ □

Theorem 18 (AM 5.10)**.** Suppose B is integral over A and P is a prime ideal of A. Then there exists a prime Q lying over P.
Basically, we can complete the following:



Proof. Consider the following commutative diagram:

$$\begin{array}{ccc} B & \xrightarrow{\beta} & S^{-1}B \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j \text{ (int by 5.9)}} \\ A & \xrightarrow{\alpha} & A_P = S^{-1}A \end{array}$$

Let $N \triangleleft S^{-1}B$ be maximal. Then,

$$\begin{array}{ccc} Q = B^{-1}N & \text{———} & N \\ | & & | \\ Q \cap A & \text{———} & M \coloneqq N \cap A_P \end{array}$$

N exists by Zorn's lemma
By 5.8 M is maximal.
Now, $Q \cap A = i^{-1}\beta^{-1}N = \alpha^{-1}j^{-1}N = \alpha^{-1}M = \alpha^{-1}(PA_P) = P$ since A_P local and PA_P maximal.

□

Remark: Q may not be unique. See:

$$\begin{array}{ccc} (2+i)\mathbb{Z}[i], (2-i)\mathbb{Z}[i] & \text{——} & \mathbb{Z}[i] \\ | & & | \\ 5\mathbb{Z} & \text{———} & \mathbb{Z} \end{array}$$

Note: $5\mathbb{Z}[i] = ((2+i)\mathbb{Z}[i])((2-i)\mathbb{Z}[i])$
Now we have the Going-up theorem.

Theorem 19 (AM 5.11)**.** Suppose we have integral extension B over A and we have chain of prime ideals $P_1 \subset P_2 \subset \cdots P_n$ of A and chain of prime ideals $Q_1 \subset \cdots \subset Q_m$ of B and $\forall i \leq m, Q_i \cap A = P_i$ then we can extend the chain of Q's to $Q_1 \subset \cdots \subset Q_n$ such that for all i, $Q_i \cap A = P_i$.
We basically have,

$$\begin{array}{ccc} Q_1 \subset \cdots \subset Q_n \subset \cdots \subset Q_m & \text{——} & B \\ | & & | \\ P_1 \subset \cdots \subset P_n & \text{———} & A \end{array}$$

Proof. We use 5.10. Base case is 5.10.
We want to define Q_{m+1}. If $n > m > 0$,
Recall: quotient of integral extensions are integral by 5.6. Let $\overline{B} = B/Q_m, \overline{A} = A/P_m$.
So we have by 5.10

$$\begin{array}{ccc} \exists\overline{Q_{m+1}} & \text{——} & \overline{B} = B/Q_m \\ | & & |{\scriptstyle \text{int by 5.6}} \\ \overline{P_{m+1}} & \text{———} & \overline{A} = A/P_m \end{array}$$

Let $Q_{m+1} = \overline{Q_{m+1}}^c$ and we are done.

□

Context:
Krull dim $A = \max\{n | P_0 \subsetneq \cdots \subsetneq P_n \text{ primes in } A\}$
A corollary of 5.11 tells us, if B is integral over A then $\dim B \geq \dim A$.

Going down theorem

Proposition 52 (AM 5.12)**.** Localization respects integral closure.
Suppose B is integral over A and $S \subset A$ is multiplicatively closed. Then, we have $C = IC(A \subset B)$ the integral closure. Then, $S^{-1}C = IC(S^{-1}A \subset S^{-1}B)$

Proof. 5.6 implies $S^{-1}C \subset IC(S^{-1}A \subset S^{-1}B)$. We have one direction. For the other direction,
Let $\frac{b}{s} \in IC(S^{-1}A \subset S^{-1}B)$. So there is some integral dependense relation:

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_1}{s_1}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

Let $t = s_1 \cdots s_n$. Multiply the polynomial by $(st)^n$ so we have

$$(bt)^n + \cdots + (st)^n \frac{a_n}{s_n} = 0$$

Thus, $bt \in C = IC(A \subset B)$
Thus, $\frac{b}{s} = \frac{bt}{st} \in S^{-1}C$
So we're done. □

Class 28: 03/22
Recall the going up theorem.
(krull) $\dim A = \max_n\{\exists P_o \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \lhd A\}$
dim field $= 0$
$\dim \mathbb{Z} = 1$
$\dim k[x_1, \cdots, x_n] = n$
variety $V, \dim V = \dim \frac{k[x_1,\cdots,x_n]}{I(V)}$
Corollary:
If B is integral over A then $\dim A = \dim B$
Another corollary
A domain, $\dim A = 0$ if and only if A field.
Simply:
Let $A \subseteq B$.
Going up:
If B is integral over A
$P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$ in A
$Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ in B
implies $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_n$
Going down:
If B is integral over A and is a domain
$P_1 \supseteq P_2 \supseteq \cdots \supseteq P_n$ in A
$Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_m$ in B
implies $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_n$

Proposition 53 (AM 5.13)**.** Let A be a domain. Integral closure is a local property. Meaning TFAE:

i A is IC

ii $\forall$ prime $P \lhd A, A_P$ is IC

iii $\forall$ maximal $M \lhd A, A_M$ is IC.

Proof. Let $k = Frac(A)$ and let $C = IC(A \subset k)$
Inclusion: $f : A \hookrightarrow C$
$f_P : A_P \hookrightarrow C_p \coloneqq (A - P)^{-1} \overset{5.12}{=} IC(A_P \subset k) \subset k$
$f_M : A_M \hookrightarrow C_M$
Now, $\left\{\begin{matrix} A \\ A_P \\ A_M \end{matrix}\right\}$ ic IC $\iff$ $\left\{\begin{matrix} f \\ f_P \\ f_M \end{matrix}\right\}$ is surjective
3.9 implies surjectivity is a local property so we are done. □

Going up iff $\operatorname{Spec} B \to \operatorname{Spec} A$ is closed map
Going down iff $\operatorname{Spec} B \to \operatorname{Spec} A$ is open map

Definition 77. Suppose $A \subset B$ rings and $I \triangleleft A$ and $x \in B$.
x is integral over I, if there exists equation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

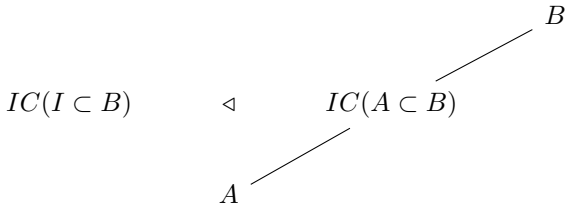
where $a_i \in I$.

eg 2 is integral over $4\mathbb{Z} \triangleleft \mathbb{Z}$ since 2 satisfies $x^2 - 4$

Definition 78. Suppose B is integral over A and $I \triangleleft A$. We can define the integral closure of this ideal.

$$IC(I \subset B) \coloneqq \{x \in B : x \text{ is integral over } I\}$$

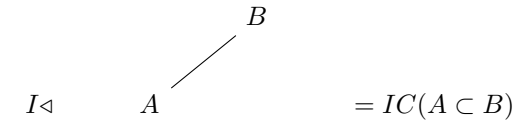
Lemma 5.14: Suppose B is integral over A and $I \triangleleft A$. Then



In fact $IC(I \subset B) = \sqrt{I^e} = \sqrt{IC(A \subset B)I}$

Proof. $C \coloneqq IC(A \subset B)$ ring
$IC(I \subset B) = \sqrt{I^e} \overset{def}{=} \sqrt{CI}$
Want to show $IC(I \subset B) = \sqrt{CI}$
$\subseteq$:
$x \in IC(I \subset B)$
ie $\exists x^{n+a_1 x^{n-1}+\cdots+a_0=0}$ where $a_i \in I$
Thus $x^n \in CI$
So $x \in \sqrt{CI}$
$\supseteq$:
$x \in \sqrt{CI}$
So $x^n = \sum_i a_i c_i$ where $a_i \in I, c_i \in C$
5.2 implies,
$M \coloneqq A[c_1, \cdots, c_p]$ finitely generated A-module.
and $x^n M \subset IM$
by 2.4 x^n integral over I
So x integral over I
So we're done. □

Class 29: 03/25
Special Case of 5.14



Then $IC(A \subset B) = \sqrt{I}$

Proposition 54 (AM 5.15)**.** Suppose B is a domain, B is integral over A and $A = IC(A \subset B)$. Let $I \triangleleft A$
Then $x \in B$ is integral over A.
Suppose $K = \operatorname{Frac}(A)$. Then $\operatorname{Irr}_K(x)(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in K[t]$ [minimal polynomial] satisfies $a_i \in \sqrt{I}$.

Proof. x integral over over I implies x is algebraic over K.
Let L be a splitting field for $\operatorname{Irr}(x)$.
$\operatorname{Irr}(x) = \prod(t - x_i)$
x_i's are the conjugates of x
Claim: x_i are integral over I.
This is becaue they are conjugates of x.
x is integral over I means there exists monic polynomial $g(t) = t^k + b_1 t^{k-1} + \cdots + b_k$ where $b_k \in I, g(x) = 0$ where $\operatorname{Irr}(x) \mid g$
So $g = h \operatorname{Irr}(x)$
So $g(x_i) = h(x_i)(\operatorname{Irr}(x)(x_i)) = 0$ so x_i is integral over I.
Now,
$\prod(t - x_i) = \operatorname{Irr}(x) = t^n + a_1 t^{n-1} + \cdots + a_n$
a_j are polynomials in $x_1, \cdots, x_n \in IC(I \subset B) = \sqrt{I}$
[elementary symmetric polynomials]

□

This will be useful in hw.
Useful even when $I = A$
Note: integral means some monic polynomial with good coefficient exists, this proposition lets us take the minimal polynomial.

Proposition 55 (AM 5.17)**.** Let A be a domain.

$$\begin{array}{ccc} IC(A \subset L) = B & \longrightarrow & L \\ \downarrow & & \downarrow \\ IC(A \subset K) = A & \longrightarrow & K = \operatorname{Frac}(A) \end{array}$$

Where L is a field with characteristic zero.
Suppose $n = |L : K| < \infty$
Then there exists basis $u_1, \cdots u_n$ and $v_1, \cdots, v_n$ of L/K such that:

$$\sum Au_i \subset B \subset \sum Av_i$$

If we have

$$\begin{array}{ccc} K \cap \mathbb{A} = \mathcal{O}_k & \longrightarrow & K \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

5.17 implies $\mathcal{O}_K$ is free abelian of rank n.
$\mathcal{O}_K \cong \mathbb{Z}^n$ as abelian group.
Trace
Suppose $\overline{K}$ is the algebraic closure of K.
Suppose $x \in \overline{K}$ is algebraic over K.
Define $\operatorname{Tr}(x) = \sum_i x_i$
Now, suppose:

$$x \in \begin{array}{c} \overline{K} \\ | \\ L \\ |\text{finite} \\ K \end{array}$$

then $\operatorname{Tr}_{L/K}(x) = |L : K(x)| \operatorname{Tr}(x) \overset{fact}{=} \operatorname{Tr}(L \xrightarrow{\cdot x} L)$
$T = \operatorname{Tr}_{L/K} : L \to K$ is K-linear.
$\operatorname{Tr}(1) = n$, the dimension.
Also,

$$\prod_{i=1}^{d}(t-x_i) = \mathrm{Irr}(x) = t^d + a_1 t^{d-1} + \cdots$$

So $T(x) = \mathrm{Tr}_{L/K}(x) = (\frac{n}{d})(-a_1)$
Corollary of 5.15: [special case where $I = A$]
$\mathrm{Tr}_{L/K}(B) \subset A$.
Claim 1: $\forall v \in L, \exists a \neq 0 \in A$ such that $av \in B$.
Proof: v is algebraic over K so we have some polynomial

$$v^n + \frac{a_1}{b_1}v^{n-1} + \cdots + \frac{a_r}{b_r}0$$

where $a_i \in A$
multiply by $a = (\prod b_i)$
multiply by a^r
$(av)^r + a\frac{a_1}{b_1}(av)^{r-1} + \cdots + (a)^r\frac{a_r}{b_r} = 0$
So $av \in B$
Claim 2:
There exists basis $u_1, \cdots, u_n$ of L/K such that $u_i \in B$

Proof. Let $w_1, \cdots, w_n$ be basis of L/K. By claim 1, choose a_i such that $a_i w_i = B$
Let $u_i = aw_i$ □

Class 30: 03/27
Correcting previous class:
If B is a domain, $I \triangleleft A$ and B is integral over A and $K = \mathrm{Frac}(A)$
A is integrally closed (ie $A = IC(A \subset K)$)
and $x \in B$ is integral over I
Then,
If $\mathrm{Irr}_K(x) = t^n + a_1 t^{n-1} + \cdots + a_n$
Then $a_i \in \sqrt{I}$.
We want to prove 5.17, which is important in algebraic number theory.

Proposition 56 (AM 5.17)**.**

$$\begin{array}{ccc} B & \text{——} & L \\ | & & | \\ A & \text{——} & K \end{array}$$

Where L, K fields, $n = |L : K|$ and $char = 0$ and $K = \mathrm{Frac}(A), B = IC(A \subset L)$
Then $\exists$ bases $\begin{matrix} u_1, \cdots, u_n \\ v_1, \cdots, v_n \end{matrix}$ of L/K such that $\sum Au_i \subset B \subset \sum Av_i$

Lemma 5.14: Suppose $I \triangleleft A$ and B is integral over A. Let $C = IC(A \subset B)$. Then $IC(I \subset B) = \sqrt{CA}$
5.14 implies,
1. $IC(I \subset B)$ is closed under + and ×
2. Special case(A = B):
$IC(I \subset A) = \sqrt{I}$
eg $IC(4\mathbb{Z} \triangleleft \mathbb{Z}) = \sqrt{4\mathbb{Z}}$
2 is root of $t^2 - 4$
Special case of 5.15: $A = I$
If $x \in B$ is integral over $I = A$ then coefficients lie on A.
Similar to HW.

Proof. $\mathrm{Irr}_K(x) = \prod(t - x_i) \in L[t]$
x_i are conjugates.
$\mathrm{Irr}_K(x) = \mathrm{Irr}_K(x_i)$ [we proved in last class].
This implies x_i are integral $/A$
So $x_i \in IC(I \subset B)$

So, 5.14 closed implies $a_i = \sigma_i(x_1, \cdots, x_n) \in IC(I \subset B) \cap A =_{AIC} IC(I \subset A) =_{5.14} \sqrt{I}$

□

trace $T = \mathrm{Tr}_{L/K} : L \to K$
K-linear
$T(1) = n$
$T(B) \subset A$ by 5.15.
Claim: $\exists$ basis u_j for L/K such that $\sum_i Au_j \subset B$

Proof. Clear denominator □

Claim: there exists basis $\{v_i\}$ of L/K such that $T(v_i u_j) = \delta_{ij}$

Proof. Define $\beta : L \times L \to K$ by $\beta(x, y) = T(xy)$. This is a K-bilinear form.
So we have $Ad\beta : L \to L^* = Hom_K(L, K)$ by $x \mapsto (y \mapsto \beta(x, y))$
$Ad\beta$ is $1 - 1$ ie B is non-degenerate:
$x \neq 0$ means $Ad\beta(x)(x^{-1}) = \mathrm{Tr}(xx^{-1}) = \mathrm{Tr}(1) = n \neq 0$ so it is actually non-degenerate.
So, $Ad\beta : L \to L^*$ is actually an isomorphism.
Let $\hat{u}_i$ be the u_i dual basis of L
ie $\hat{u}_i(u_j) = \delta_{ij}$
Let $v_i = (Ad\beta)^{-1}\hat{u}_i$ □

Now we prove $B \subset \sum_i Av_i$

Proof. Consider $x \in B \implies x = \sum_i k_i v_i$, where $k_i \in K$
Note that $xu_j \in B$
5.15 means $A \ni T(xu_j) = T(\sum_i k_i v_i u_j) = k_j$ so we're done. □

Valuation Rings

Let B be a domain and let $K = \mathrm{Frac}(B)$

Definition 79. B is a valuation ring of K if $x \in K^\times \implies x \in B$ or $x^{-1} \in B$

Basically $B \cup (B - 0)^{-1} = K$
eg $\mathbb{Z}_{(p)}$ is a valuation ring.
But $\mathbb{Z}$ not a valuation ring.
Suppose A is a domain and $K = \mathrm{Frac}(K)$
Then $IC(A \subset K) = \cap_{A \subset B \subset K, B \text{ valuation ring}} B$

Proposition 57 (AM 5.18)**.** Let B be a valuation ring (over K). Then,
i: B is a local ring
ii: $B \subset B' \subset K$ implies B' is a valuation ring.
iii: B is integrably closed.

Proof. i: Let $M = B - B^\times$, non-units.
We want to show M is an ideal, then we're done.
$M = \{0\} \cup \{x \in B : x^{-1} \notin B\}$
First: M is closed under multiplication by B.
If $a \in B, m \in M$, for contradiction assume $am \notin M$. Then $(am)^{-1} \in B$ [since valuation ring], so $m^{-1} = a(am)^{-1} \in B$ so we have contradiction.
Second: M is closed under addition.
$x, y \in M - 0$ then $xy^{-1} \in B$ or $x^{-1}y \in B$ since valuation ring.
WLOG $xy^{-1} \in B$
Then $x + y = (1 + xy^{-1})y \in M$
ii is clear
iii: Suppose $x \in K$ is integral over B.
Then $x^n + b_1 x^{n-1} + \cdots + b_n = 0$
If $x \in B$ then we're done.

If $x^{-1} \in B$ then solve for x^n and multiply by x^{1-n} so $x \in B$

□

Class 31: 03/29
One to One Correspondence Between Valuation and Valuation Ring
Ex 30 and 31
A valuation on field is homomorphism $v : K^* \to \Gamma$ where Γ is totally ordered abelian group such that $v(x+y) \geq \min(v(x), v(y))$.
If Γ is discrete it is called a discrete valuation.
Totally Ordered Abelian Group: We have order, and $a \geq b \implies a + c \geq b + c \forall c$.
eg p-adic valuation on $\mathbb{Q}$.
$v_p : \mathbb{Q}^\times \to \mathbb{Z}$ given by:
$v_p(p^k \frac{a}{b}) = k$ where $p \nmid a, b$
Note: if we define for $x \in \mathbb{Q}$, $|x|_p \coloneqq p^{-v_p(x)}$ it is like an absolute value. It is actually a non-archemedian absolute value.
We can define a metric: $d_p(x,y) = |x-y|_p$
Completion of this metric space is the p-adic numbers $\mathbb{Q}_p$
Valuation $\longleftarrow$ valuation ring
$v : K^\times \to \Gamma \mapsto B = \{x \in K : v(x) \geq 0\}$
$\Gamma = K^\times / B^\times \leftarrow B$
$[x] \geq [y] \overset{def}{\iff} xy^{-1} \in B$
$B = v_p^{-1}[0, \infty) = \mathbb{Z}_{(p)}$
Now, let K be a field and Γ be an algebraically closed field.
$\Sigma = \{(A, f) | A \subset K \text{ subring } f : A \to \Gamma \text{ homomorphism}\}$
Poset $(A, f) \leq (A', f') \overset{def}{\iff} A \subset A', f'|_A = f$
Zorn's lemma implies: $\exists \max(B, g) \in \Sigma$
eg suppose $\Omega = \overline{K}$. Then $B = K$.
eg $K = \mathbb{Q}$ implies $\Omega = \overline{\mathbb{F}}_p = \cup \overline{\mathbb{F}}_{p^r}$

Theorem 20 (AM 5.21)**.** Let K be a field and Ω be algebraically closed field. Let (B, g) be maximal element of Σ. Then B is a valuation ring of K.

Lemma 5.19: B is a local ring with maximal ideal $M = \ker g$

Proof. $M = \ker g$
So $B/M \cong g(B) \subset \Omega \implies M$ prime since $g(B)$ is a domain
$g(B - M) \subset \Omega^\times$
$\implies \overline{g}$ such that $(B_M, \overline{g}) \geq (B, g)$ maximal.
So $B_M = B$
M maximal since B_M is local.

□

Lemma 5.20: Let $x \in B^\times$.
Then $M[x] \neq B[x]$ or $M[x^{-1}] \neq B[x^{-1}]$
Note: $M[x] = M\{1, x, x^2, \cdots\} \lhd B[x]$

Proof. Of 5.20
By contradiction.
Suppose $M[x] = B[x]$ and $M[x^{-1}] = B[x^{-1}]$
ie $1 \in M[x], 1 \in M[x^{-1}]$
Then 1: $u_0 + u_1 x + \cdots + u_m x^m = 1$ $[u_i \in M]$
Also 2: $v_0 + v_1 x^{-1} + \cdots + v_n x^{-n}$ $[v_\in M]$
WLOG $m \geq n$ with m, n minimal.
3: $v_1 x^{n-1} + \cdots + v_n = (1 - v_0) x^n$
$1 - v_0 \in B - M$ [since M proper] $\implies (1 - v_0)^\times \in B$ since M maximal.
4: $w_0 + w_1 x + \cdots + w_m x^{m-1} = x^m$
Plug 4 to 1, that contradits minimality.

□

Finally, we prove 5.21.

Proof. $x \in K^\times$
WTS $x \in B$ or $x^{-1} \in B$
$M = \ker g \lhd B$. Maximal.
WMA (5.20) $M' = M[x] \trianglelefteq B[x] =: B'$
$M = M' \cap B$ since M maximal.
B/M is a field.
So we have map $B/M \to \Omega$
If we go to B'/M'
By universal property, $B'/M' = B/M[\overline{x}]$
So $\overline{x}$ algebraic over B/M
$B' \to B'/M' \to \Omega$
$(B, g) \in \Sigma$ maximal implies $B = B' = B[x] \implies x \in B$.

□

Class 32: 04/01
Let K be field and Ω be an algebraically closed field.
Consider the poset $\Sigma = \{(B, g) | B \subset K, g : B \to \Omega\}$
Since the set has an upper bound, every chain has an upper bound.
Using Zorn's Lemma, there must exist a maximal element.
Most interesting case: $K = \mathbb{Q}$ and Ω is the algebraic closure of $\mathbb{F}_p$
Theorem 5.21 states that if (B, g) is a maximal element then B is a valuation ring.
Meaning $x \in K^\times \implies x$ or $x^{-1} \in B$
Corollary 5.22: Let A be a subring of the field K. Then the integral closure of A in K $[IC(A \subset K)]$ is the intersection of valuation ring containing K

$$IC(A \subset K) = \bigcap_{A \subset B \subset K,\ B \text{ valuation ring}} B$$

Example: $IC(\mathbb{Z} \subset \mathbb{Q}) = \bigcap \mathbb{Z}_{(p)}$

Proof. $\subset$: Let B be a valuation ring. 5.18(iii) implies B is IC $\implies IC(A \subset K) \subset B$ so we're done with this direction.
$\supset$: Suppose $x \in IC(A \subset K)$. Note that x integral if and only if $x \in A[x^{-1}] = A'$.
Thus, $x^{-1} \in A'$ but is not a unit.
Thus there exists a maximal ideal containing x^{-1}. So, $x^{-1} \in M'$.
We have a map $A' \to A'/M' = k'$ since M' is a maximal ideal. We can include $k' \hookrightarrow \overline{k'} = \Omega$ the integral closure.
Note that $x^{-1} \mapsto 0$
Extend to maximal (B, g)
$g(x^{-1}) = 0 \implies x^{-1}$ not a unit in $B \implies x \notin B$
B is a valuation ring by theorem 5.21

□

Proposition 58 (AM 5.23)**.** Suppose B is extension of ring A and B is finitely generated over A, meaning $B = A[x_1, \cdots, x_n]$ where x_j are elements of B and B is a domain.
Suppose $0 \neq v \in B$.
Then $\exists u \in A$ such that:
For any homomorphism $f : A \to \Omega$ where Ω is algebraically closed with $f(u) \neq 0$
$\exists g : B \to \Omega$ such that $g|_A = f$ and $g(v) \neq 0$

Proof. By induction. Key case: $n = 1$
Assume $B = A[x]$
Consider $v \in B$ nonzero.
Two cases: x is not algebraic over A.
Let $v = a_0 x^n + \cdots + a_n \in B$
Let $u = a_0$
$\forall f : A \to \Omega$ such that $f(u) \neq 0$ we can define:

$f(a_0)t^n + \cdots + a_0 \in \Omega[t]$
has n roots.
Choose nonroot $\xi \in \Omega$
define $g : B \to A[x] \to \Omega$ by $g(x) = \xi$
Then $g(v) \neq 0$ and we're done.
Case ii: x is algebraic over A
Then $\mathrm{Frac}(A)[x]$ is a field
Then v^{-1} is algebraic over A
x algebraic.
1: $a_0x^m + \cdots + a_m = 0$
v^{-1} algebraic
2: $a_0'v^{-n} + \cdots + a_n'$
Let $u = a_0a_0'$
Let $f : A \to \Omega, f(a_0a_0') \neq 0$
f extends to $f_1 : A[u^{-1}] \to \Omega$ by $f_1(u^{-1}) = f(u)^{-1}$
Now, $(A[u^{-1}], f_1) \leq (C, h)$
Let $g = h|_B$
5.21 $\implies$ C is valuation ring, 5.18 $\implies$ C integrally closed.
1 $\implies$ x integral over $A[u^{-1}]$ $\implies$ $x \in C$ $\implies$ $B \subset C$
2 $\implies$ v^{-1} integral over $A[u^{-1}]$ $\implies$ $v^{-1} \in C$ $\implies$ v is a unit in C $\implies$ $h(v) \neq 0$ $\implies$ $g(v) \neq 0$

□

We have a nice corollary:
Corollary 5.24 [Zariski's Lemma]: Suppose we have a field k and a polynomial ring $B = k[x_1, \cdots, x_n]$ field. Then $|B : k| = \dim_k B < \infty$

Proof. Apply 5.23 with $v = 1, \Omega = \overline{k}, f =$ inclusion.
So, $\exists g : B \to \overline{k}$, injective since B field
$k \subset g(B) \subset \overline{k}$
$g(B) = B$
B/k algebraic and B finitely generated implies $|B : k| < \infty$ □

Corollary: Weak Nullstellensatz (HWK)
Let k be algebraically closed. Let I be a proper ideal of $k[t_1, \cdots, t_n]$
Week: $V(I) \neq \varnothing$
Strong: $I(V(I)) = \sqrt{I}$
'counterexample': $I = (x^2 + 1) \lhd \mathbb{R}[x]$ but then $V(I) = \varnothing$. This is not really a contradiction since $\mathbb{R}$ is not algebraically closed.

Class 33: 04/03

Chapter 6 Chain Conditions

Proposition 59 (AM 6.1)**.** Let $(\Sigma, \leq)$ be a poset.
TFAE:
i: Ascending chain condition (acc): Every $x_1 \leq x_2 \leq x_3 \leq \cdots$ is stationary: $\exists n$ such that for all $i, j \geq n$ we have $x_i = x_j$
ii: Maximal condition: every $\phi \neq T \subset \Sigma$ has a maximal element.

Proof. $\neg ii \implies \neg i$:
$0 \neq T$ no max. $x_1 \in T$. $x_1 < x_2 < x_3 \cdots$
$ii \implies i$: $x_1 \leq x_2 \leq \cdots$ has a maximal x_n □

Definition 80. Module M is Noetherian/Artinian
if (Σ = submodules, $\subseteq$) satisfies acc (iff maximal condition) / dcc (iff minimal condition)

Definition 81. Ring A is Noetherian/Artinian if it is so as an A-module.

Remark: Submodule of $A \iff$ ideal of A. So we are talking about chains of ideals.
eg $A = k$ field, $M = V$ vector space.
If V is finite dimensional, it satisfies this condition.
Call length of chain $l(x_0 < x_1 < \cdots < x_n) = n$. Then length of chain of n-dimensional vector space is n.
So, $\dim V < \infty \iff V$ is N.
$\mathbb{R}^\infty$ satisfies dcc, but not acc. So it is Artinian.
$k = \mathbb{Q}, V = \mathbb{R}$ is not Artinian.
eg $A = \mathbb{Z}$ or any PID. It is Noetherian, but not Artinian.
eg $(6) \subset (2) \subset (1)$ and $(6) \subset (3) \subset (1)$
eg $(2) \supset (4) \supset (8) \supset \cdots$
If $A =$ field, then it is noetherian and artinian ring.
eg $\mathbb{Z}$-modules aka abelian groups.
$\mathbb{Z}$ is noetherian not artinian.
$\mathbb{Q}/\mathbb{Z}$ is artinian not noetherian.
$(1) \subset (\frac{1}{2}) \subset (\frac{1}{4}) \subset \cdots$
$\mathbb{Q}$ is neither artinian nor noetherian [as a $\mathbb{Z}$-module]
eg k-algebras where k is a field.
If one variable $k[t]$ then we are in a PID situation. So noetherian not artinian.
First: $k[t_1, t_2, \cdots]$ infinite not Artinian, not Noetherian.
We have two other possibilities:
$k[\alpha_1, \cdots, \alpha_n]$ finitely generated, and other possibility is finite type, $\dim_k < \infty$
$k[\alpha_1, \cdots, \alpha_n]$ finitely generated is Noetherian.
$k[\alpha_1, \cdots, \alpha_n]$ finite type, $\dim_k < \infty$ is Artinian and Noetherian.

Proposition 60 (AM 6.2)**.** M is Noetherian A-module if and only if every submodule is finitely generated.

Corollary: Ring A is Noetherian if and only if every ideal is finitely generated.

Proof. $\implies : P \subset M$ where M is noetherian.
Let $T = \{$finitely generated submodules of $P\}$
6.1 $\implies \exists$ maximal $P_0 \in \Sigma$
So, $\forall x \in P, (P_0, x) \subset P \implies (P_0, x) = P$.
P_0 maximal means $x \in P$
$\impliedby$ suppose $M_0 \subseteq M_1 \subseteq \cdots \subseteq M$.
Take $\bigcup M_i$. It is finitely generated.
Choose $n \gg 0$ such that M_n contains all generators. □

Proposition 61 (AM 6.3)**.** Consider $SES0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$.
i: M is noetherian if and only if M', M'' are noetherian.
ii: M is artinian if and only if M' and M'' are artinian.

Proof. i: ascending chain in M' (or M'') gives ascending chain in M via α (or β^{-1}). Hence stationary.
$\impliedby$ let $M_0 \subset M_1 \subset \cdots$ ac in M. Then $\alpha^{-1}M_i$ is ac in M' and $\beta(M_i)$ is ac in M''.
So, there exists n such that $\alpha^{-1}M_i$ and $\beta(M_i)$ are stationary at n. Then $\forall j > n$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \alpha^{-1}M_n & \longrightarrow & M_n & \longrightarrow & \beta M_n & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow & & \downarrow{=} & & \\ 0 & \longrightarrow & \alpha^{-1}M_j & \longrightarrow & M_j & \longrightarrow & \beta M_j & \longrightarrow & 0 \end{array}$$

By the five lemma, $M_n = M_j$

□

Corollary 6.4: If $M_1, \cdots, M_n$ are N/A then $\oplus M_i$ is N/A

Proposition 62 (AM 6.5)**.** If A is N/A ring and M is finitely generated, then M is N/A.

Proof. M finitely generated iff we have a surjection $A^n \to M$. 6.4 implies A^n is N/A. 6.3 implies M is N/A. □

Class 34, 35 skipped
Due to Ben:

Proposition 63. $I \triangleleft A$, A is noetherian (resp Atinian) implies A/I is noetherian (resp artinian)

Proof. A/I noetherian A-module implies A/I noetherian A/I module. □

Composition Series:
$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ maximal
i.e. $M_{i-1} \supsetneq M_i$ maximal proper, i.e. M_i/M_{i-1} simple.
eg $\mathbb{Z}/12$ as a $\mathbb{Z}$-module.
$\mathbb{Z}/12 \supset 2\mathbb{Z}/12 \supset 6\mathbb{Z}/12 \supset 0$. Simple factors $\mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/2$
Neg: $12\mathbb{Z}$ has no composition series.

Proposition 64 (Jordan-Holder)**.** Suppose M has a c.s. of length n. Then,
i: Any strict chain in M can be extended to a c.s.
ii: Any two c.s. for M has the same simple factors up to isomorphism, hence the same length.

Proposition 65. $0 \to M' \to M \to M'' \to 0$ SES implies $l(M) = l(M') + l(M'')$

Proposition 66. M has a c.s. $\iff$ M is noetherian and artinian.

Proof. Suppose M has a c.s. Then all strict chains have length $\leq l(M) < \infty$.
Thus, M is noetheian AND artinian.
Suppose M is both noetherian and artinian.
$M_0 = M$ has a maximal proper submodule M, since M is noetherian. Continue $M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$ will be stationary since M is artinian. □

Proposition 67. V is a vector space over k. Then TFAE:
i: $\dim V < \infty$
ii: $l(V) < \infty$ in which $\dim V = l(V)$
iii: V is noetherian.
iv: V is artinian

Proof. i $\implies$ ii clear
ii $\implies$ iii, iv by previous proposion
$\neg$ i $\implies$ $\neg$ iii, $\neg$ iv: If $\dim V = \infty$ then there exists linearly independent $x_1, x_2, x_3, \cdots$.
Let $u_n = span(x_1, \cdots, x_n)$ and $v_n = (x_{n+1}, x_{n+2}, \cdots)$ □

Corollary: Ring A, suppose $\exists$ maximal $M_1, \cdots, M_n$ with $M_1 \cdots M_n = 0$
Then A is noetherian $\iff$ A is artinian.

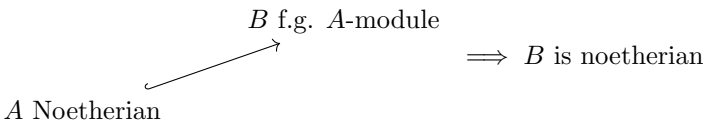
Proof. Consider the chain: $0 = M_1 \cdots M_n \subset M_1 \cdots M_{n-1} \subset \cdots \subset M_1 M_2 \subset M_1 \subset A$.
Each factor $\frac{M_1 \cdots M_i}{M_1 \cdots M_{i+1}}$ is a vector space over $\frac{A}{M_{i+1}}$. Then acc $\iff$ dcc for each factor.
Then acc for A $\iff$ dcc for A □

Chapter 7: Noetherian Rings

Proposition 68. $A \rightarrowtail B$. Then A noetherian $\implies$ B noetherian

Proof. $B \cong A/\ker$ noetherian □

Proposition 69.



Class 35:
Lemma: Ring A noetherian $\implies S^{-1}A$ noetherian.

Proof. $I \triangleleft A \implies I = (x_1, \cdots, x_n) \implies S^{-1}I = (\frac{x_1}{I}, \cdots, \frac{x_n}{I})$ □

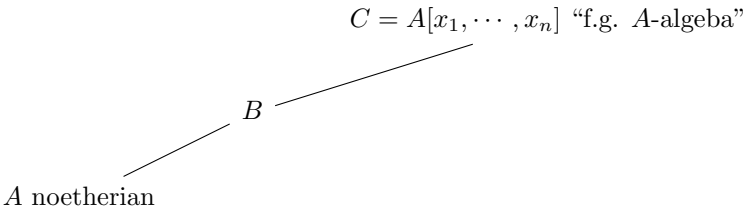
Corollary: P prime, A Noetherian $\implies A_P$ Noetherian.

Theorem 21 (Hilbert Basis Theorem)**.** If A is Noetherian then so is $A[t]$

Corollary: A noetherian implies $A[t_1, \cdots, t_n]$ is noetherian.
Corollary A noetherian implies so is any finitely generated A-algebra.

Proof. (Proof of Hilbert Basis theorem skipped. Look it up) □

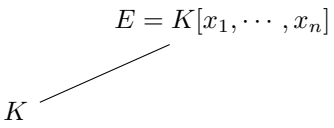
Proposition 70.



Suppose either i: C is f.g. as a B-module or ii: C is integral $/B$. Then B is f.g. as an A-algebra.

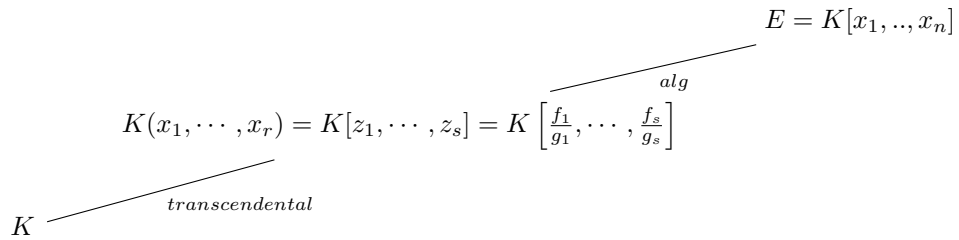
Proof. Note: 5.1 + ii $\implies$ i so we may assume i.
So, $C = \sum_{j=1}^{m} By_j$. Then $x_i = \sum_j x_{ij}y_j.y_iy_j = \sum_k b_{ijk}y_k$. Let $B_0 = A[b_{ij}, b_{ijk}]$.
Let $B_0 = A[b_{ij}, b_{ijk}]$. We know C is f.g. as a B_0 module/
B_0 noetherian $\implies$ B is f.g. as a B_0-module (since (A noetherian $\implies$ B noetherian.)) $\implies$ B_0 is f.g. as an A-algebra.
$\implies$ B f.g. as an A-algebra. □

Proposition 71 (Zariski Lemma)**.**



E field $\implies |E : K| < \infty$ hence E/K alg.

Proof. After reordering $x_1, \cdots, x_n$,



where $f_i, g_i \in K[x_1, \cdots, x_n]$
Choose irreducible $h \in K(x_1, \cdots, x_r)$ such that h is relatively prime to g_1.
Claim: $h^{-1} \notin K[x_1, \cdots, x_r] = K\left[\frac{f_1}{g_1}, \cdots, \frac{f_s}{g_s}\right]$
$\implies h^{-1} = \frac{l}{\prod g_i^{d_i}}, (l, g_i) = 1$
$\implies h^{-1} \in K[x_1, \cdots, x_r]$ contradicting h irreduible.
claim $\implies r = 0$ □

Class 36: 04/12

Primary Decomposition

Chapter 4 and 7

Definition 82. $Q \lhd A$ proper is primary if every zero divisor in A/Q is nilpotent.

eg $p^n\mathbb{Z} \lhd \mathbb{Z}$ is primary.
Zero divisors of $\mathbb{Z}/p^n\mathbb{Z}$ is $p(\mathbb{Z}/p^n\mathbb{Z})$. This is both the set of zero divisors and the set of nilpotents.
Note that nilpotents are automatically zero divisors.
Note: Powers of maximal ideals are primary.

Proposition 72. Contraction of prime ideal is a prime ideal.

If we have $A \xrightarrow{f} B \rhd Q$ then:
$A/f^{-1}Q \rightarrowtail B/Q$

Proposition 73 (AM 4.1)**.** If primary $Q \lhd A$ then: $\sqrt{Q}$ is smallest prime ideal containing Q.
Most interesting thing is: radical of a primary ideal is a prime ideal.

Proof. (Special Case) $Q = 0$. This is primary.
$\sqrt{0} = \text{Nil}(A)$. We want to show that this is prime.
Suppose $xy \in \text{Nil}(A)$. Then $(xy)^n = 0$
So, $x^n y^n = 0$
Thus, either $x^n = 0$ or $y^n = 0$ or x, y are both zero divisors.
Thus, $x \in \sqrt{0}$ or $y \in \sqrt{0}$ or x, y are both zero divisors.
So, $\text{Nil}(A)$ is indeed prime.
Since $\text{Nil}(A) = \cap_{prime} P$
So $\text{Nil}(A)$ is indeed the smallest prime containing 0.
General Case: this implies the special case.
Note: $A/\sqrt{Q} = (A/Q)/\sqrt{0}$ domain
If $Q \lhd A$ is primary, then $0 \lhd A/Q$ is primary.
So, $\sqrt{0}$ is the smallest prime of A/Q
Thus $\sqrt{Q}$ is smallest prime of A containing Q.

□

So, given a primary ideal we get an associated prime by proposition 4.1. We make this into a definition.

Definition 83. If $Q \lhd A$ is primary then $P = \sqrt{Q}$ is prime.
Then say: Q is P-primary.

Now we talk about primary decomposition.

Definition 84. Primary decomposition of $I \lhd A$ is $I = Q_1 \cap \cdots \cap Q_n$ where Q_j are distinct primary ideals.

Contrast it with: $n = p_1^{e_1} \cdots p_r^{e_r}$ and $(n) = (p_1^{e_1}) \cap \cdots \cap (p_r)^{e_r}$ where $A = \mathbb{Z}$
Irreducible components are unique, but we are not going to prove that.

Theorem 22. (AM 7.13)
A is Noetherian $\implies$ every ideal has a primary decomposition.

Proof is not trivial, but uses usual Noetherian tricks.

Definition 85. $I \lhd A$ is irreducible if $I = J \cap K \implies (I = J \text{ or } I = K)$. eg min prime implies irreducible.

Lemma 7.11: A noetherian. Then every $I \lhd A$ is a finite intersection of irreducible ideals.
Lemma 7.12: A noetherian, Q irreducible means Q is primary.
Proof of 7.11: By contradiction.
Let $T =$ set of ideals which are not finite intersection of irreduible.
$\varnothing \neq T \implies \exists$ maximal $M \in T$ since A is noetherian.

$M = J \cap K, J, K \notin T$ by maximality.
So, $M = J \cap K =$ (intersection of irreducible) intersecting (intersection of irreducibles)
Which is a contradcition.
Proof of 7.12: We may replace A by A/Q and assume 0 is irreducible.
We want to show that 0 is a primary ideal of A/Q
So, we want to show x zero divisor implies x is nilpotent.
Suppose x is a zero divisor.
We have $xy = 0, y \neq 0$.
Note that $Ann(x) \subset Ann(x^2) \subset \cdots$ which is stationary from noetherian.
So, $Ann(x^n) = Ann(x^{n+1})$ eventually.
Claim: $(x^n) \cap (y) = 0$.
Claim along with the fact that 0 is irreducible means $(x^n) = 0$ or $(y) = 0$. Thus, $(x^n) = 0 \implies x^n = 0$.
Proof of Claim: Suppose $a \in (y)$. So, $a = cy$. Thus, $ax = cxy = 0$.
Thus, $a \in (x^n) \implies a = bx^n \implies ax = bx^{n+1} \implies ax \in (x^{n+1})$
Now, $ax = 0$. So, $b \in Ann(x^{n+1}) = Ann(x^n)$
So, $bx^n = 0 \implies a = 0$.
Uniqueness of Primary Decomposition
Example: Consider $k[x, y]$. Then $(x) = (x) \cap (x^2)$ [How???]

Definition 86. $I = \bigcap Q_i$ is minimal if:
i: $\sqrt{Q_i}$ distinct
ii: $\forall i$ we have $Q_i \not\supset \cap_{j \neq i} Q_j$

Fact: I has primary decomposition implies I has minimal primary decomposition.
Are minimal primary decomposition unique? NO.
Consider $k[x, y]$ and $(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$

Theorem 23. (AM 4.5, 1st uniqueness theorem)
$I = \bigcap Q_i$ minimal primary decomposition implies $P_i = \sqrt{Q_i}$ are uniquely determined upto reordering by I.

Definition 87. $I = \bigcap Q_i$ minimal primary decomposition. Let $P_i = \sqrt{Q_i}$.
Q_i (or P_i) is isolated if P_i is a minimal element of $\{P_1, \cdots, P_n\}$

eg in the above example (x) is isolated.

Theorem 24. (AM 4.10,4.11, 2nd Uniqueness Theorem)
Let $I = \bigcap Q_i$ be minimal primary decomposition.
i: [corollary] Isolated Q_i are uniquely determined by I.
ii: If $Q_{i_1}, \cdots, Q_{i_m}$ are isolated (primary) then $Q_{i_1} \cap \cdots \cap Q_{i_m}$ is uniquely determined.

Class 37: 04/15

Dedekind Domain

Definition 88. A domain A is a dedekind domain if it satisfies the three following properties.

1. A is Noetherian
2. Nonzero primes are maximal
3. A is integrally closed

Comment on ii: ii is equivalent to saying the krull dimension $\dim A \leq 1$.
A field is a dedekind domain, in that case $\dim A = 0$. This is stupid.
Classical Example: If we have a finite extension K of $\mathbb{Q}$ and look at the ring of integers $\mathcal{O}_K$:

$$\begin{array}{ccc} \mathcal{O}_K & \text{——} & K \\ \Big| & & \Big|\text{finite} \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

So $\mathcal{O}_K = IC(\mathbb{Z} \subset K) = K \cap \mathbb{A}$.

Theorem 25 (AM 9.5)**.** $\mathcal{O}_K$ is a dedekind domain.

Proof. i: $\mathcal{O}_K$ is noetherian by 5.17
Review of proof: let $n = |K : \mathbb{Q}|$.
$\exists u_1, \cdots, u_n \in \mathcal{O}_K$ and linearly independent over K.
Then $\bigoplus \mathbb{Z}u_i \subset \mathcal{O}_K \subset \bigoplus \mathbb{Z}\hat{u}_j$
where $\mathrm{Tr}(u_i\hat{u}_j) = \delta_{ij}$
Thus $\mathcal{O}_K \cong \mathbb{Z}^n$ as $\mathbb{Z}$-module thus $\mathcal{O}_K$ is noetherian.
ii: First proof (AM): Take prime $0 \neq P \lhd \mathcal{O}_K$.
Claim: $P \cap \mathbb{Z} \neq 0$
Proof of claim: if $P \cap \mathbb{Z} = 0$ then $0 \subset P$ both lie above 0 so by 5.8 $0 = P$.
5.9 gives P maximal $\iff$ $P \cap \mathbb{Z}$ maximal.
2nd Proof: Let $0 \neq \alpha \in P$.
norm $N\alpha = \prod$ conjugates of α.
$N\alpha \neq 0$
$N\alpha \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$
$(N\alpha)/\alpha \in K \cap \mathbb{A} = O_{\mathbb{K}}$
So, $N\alpha = \left(\frac{N\alpha}{\alpha}\right)\alpha \in \mathcal{O}_K P = P$
(so $P \cap \mathbb{Z} \neq 0$)
Now, we have
$\mathcal{O}_K/P \hookleftarrow \mathcal{O}_K/\alpha \hookleftarrow \mathcal{O}_K/N_\alpha$
so, $\mathcal{O}_K/P$ is finite domain hence $\mathcal{O}_K/P$ is a field.
Thus, P is maximal.
Also, integrally closed by 5.5

□

Theorem 26. (Main Theorem) Let A be a domain which is not a field. Then TFAE:

1. A is a Dedekind Domain.
2. Every ideal $I \lhd A$ factors uniquely as a product of prime ideals $I = P_1^{e_1} \cdots P_r^{e_r}$
3. Every fractional ideal is invertible
4. If $I \subset J \lhd A, \exists K \lhd A$ such that $I = JK$. 'To contain is to divide'
5. $\forall$ nonzero prime $P \lhd A$, A_P is a DVR
6. Every ideal of A is a projective A-module
7. Every submodule of A^n is projective

Definition 89 (Fractional Ideal)**.** Suppose $K = \mathrm{Frac}(A)$. Let $M = yI \subset K$ where $y \in K^\times, I \lhd A$. Then M is a fractional ideal. M is invertible if there exists N such that $M \cdot N = A$

Lets talk about 2:
Recall "Ideals" is 'ideal numbers'
Numbers factor into product of primes, similarly ideals factor into product of ideals.
Suppose $K = \mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$
Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$
Take $p \in \mathbb{Z}$
How does $p\mathcal{O}_K$ factor?
$2\mathbb{Z}[\sqrt{2}] = (\sqrt{2}\mathbb{Z}[\sqrt{2}])^2 = Q^2$
Suppose p odd, $p \not\equiv 1 \pmod 8$

Then $p\mathbb{Z}[\sqrt{2}] = Q$ prime
If $p \equiv \pm 1 \pmod 8$ then $p\mathbb{Z}[\sqrt{2}] = Q_1Q_2, Q_1 \neq Q_2$
Note: $\mathbb{C}[x,y]$ is not dedekind domain since $\dim \mathbb{C}[x,y] = 2$ or (x) a prime ideal is not maximal.
Fact: suppose A is a Dedekind Domain.
Ten A PID $\iff$ A UFD
Suppose $K = \mathbb{Q}[\sqrt{-5}]$
Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$
Not a UFD since $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$
So, $\mathbb{Z}[\sqrt{-5}]$ is a DD that is not a PID.
Note: $\mathbb{Z}[\sqrt{8}]$ is not Integrally Closed and hence not a Dedekind Domain.
If A is a domain and $K = \text{Frac}(A)$
$M \subset K$ is a fractional ideal if it is a fraction times an ideal: $M = yI$ where $I \triangleleft A, y \in K^\times$
eg $\frac{2}{5}\mathbb{Z} \subset \mathbb{Q}$ is fractional ideal.
AM equivalent definition: M is an A-submodule of K such that $\exists x \in K^\times$ such that $xM \subset A$
Lemma: If M is a finitely generated A submodule of $K = \text{Frac}(A)$ then M is a fractional ideal.
Suppose $M = \sum A\frac{w_i}{z_i}$. If $x = \prod z_i$ then $M = \sum A\frac{y_i}{x}$ so $xM \subset A$
Claim: if A is Noetherian, every fractional ideal is finitely generated: $M = yI$ and I is finitely generated
If $M, N \subset K$ are fractional ideals, then $MN = \{\sum_i m_i n_i\}$ is a fractional ideal.

Definition 90. M is invertible $\exists N$ such that $MN = A$

Here $\left(\frac{2}{5}\mathbb{Z}\right)^{-1} = \frac{5}{2}\mathbb{Z}$
Proof of 4 $\implies$ 3
Let M be a fractional ideal. Then $M = yJ$ for some $J \triangleleft A$
Choose $0 \neq a \in J$, by 3 we have $\exists L$ such that $(aA) = JL$
Then $M^{-1} = y^{-1}a^{-1}L$

Class 38: 04/17

Recall:

Definition 91. Domain A is a dedekind domain if:
i: A is noetherian
ii: nonzero primes are maximal
iii: A is IC

Theorem 27. Let A be a domain. TFAE:
i: A is DD
ii: $\forall$ nonzero ideal I, $I = P_1^{e_1} \cdots P_r^{e_r}$ [uniquely]. The equivalence is true with or without uniqueness.
iii: Every nonzero fractional ideal is invertible.
iv: To contain is to divide: $I \subset J \subset A$ means $\exists L \triangleleft A$ such that $I = JL$
v: $\forall 0 \neq P \triangleleft A$ means A_P is a DVR [ring with unique nonzero prime ideal]
vi: Every ideal of A is a projective module
v: Every submodule of A^n is a projective module

Yesterday we did iii $\iff$ iv which is easy.
ii′: $\forall$ non-zero fractional ideal, $\exists! M = P_1^{e_1} \cdots P_r^{e_r}$
Different from ii in the sense that instead of ideal we have fractional ideal, and we allow negative exponent.
Recall:

Definition 92. A subset $M \subset K = \text{Frac}(A)$ is a fractional ideal if $M = yI$ where $y \in K^\times$ and I is an ideal of A

A f.i. is invertible if $\exists$ f.i M^{-1} such that $MM^{-1} = A$

Definition 93. M is principal f.i if $M = yA$ for some $y \in K$

Definition 94. Ideal class group of dedekind domain A:

$$Cl(A) = \frac{(\text{nonzero frac ideal}, \cdot)}{(\text{nonzero prime f.i.})}$$

We have $Cl(\mathbb{Z}) = 0$
Also $Cl(A) = 0 \iff A$ is PID

Survey of Algebraic Number THeory

Clasically it's about finite extensions.

$$\begin{array}{ccc} K \cap \mathbb{A} = \mathcal{O}_K^{IC} & \text{——} & K \\ \Big| & & \Big|\text{finite} \\ \mathbb{Z} & \text{————} & \mathbb{Q} \end{array}$$

Theorem 28. $Cl(\mathcal{O}_K)$ finite.

$h_K = |Cl(\mathcal{O}_K)|$
Let prime $p \in \mathbb{Z}$
$p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$
$f_i = |\mathcal{O}_K / P_i : \mathbb{F}_P|$
$|K : \mathbb{Q}| = \sum e_i f_i$
Suppose K integral over $\mathbb{Q}$ and galois.
Then for all $\phi : K \hookrightarrow \mathbb{C}$ we have $\phi(K) = K$
In $\mathrm{Gal}(K/\mathbb{Q})$ permute P_i
$e = e_1 = \cdots = e_r$
$f = f_1 = \cdots = f_r$
Then $|K : \mathbb{Q}| = efr$
e is ramification index
Suppose K over $\mathbb{Q}$ galois abelian.
Class field theory implies: $\exists N$ such that factorization of p in $\mathcal{O}_K$ depends on $p \pmod N$
There exists n such that $K \subset \mathbb{Q}(\zeta_n)$
$K/\mathbb{Q}$ abelian
quadratic $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$, d squarefree
If $d \equiv 2, 3 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$
If $d \equiv 1 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$
cyclotomic extension $\mathbb{Q}(\zeta_n)$
What is the ring of integers?
$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$
We have: for odd prime p

$$\begin{array}{ccccc} & & \mathbb{Q}(\zeta_p) & & \\ & \overset{p\equiv 1 \pmod 4}{\swarrow} & & \overset{p\equiv 3 \pmod 4}{\searrow} & \\ \mathbb{Q}[\sqrt{p}] & & & & \mathbb{Q}[\sqrt{-p}] \end{array}$$

$Cl(\mathcal{O}_{\mathbb{Q}[\sqrt{-d}]}) = 0$
$d > 0$ iff $d = 1, 2, 7, 11, 19, 43, 67, 163$
$Cl(\mathbb{Z}[\zeta_p]) = 0$ if and only if $p < 23$
Complex geometry:
Suppose X is compact complex 1-manifold. "Riemann Surface"
Riemann sphere $\mathbb{C} \cup \infty$ is one example.
Let A be a ring of holomorphic functions of X
$X \to \mathbb{C}$
points in $X \leftrightarrow$ nonzero prime ideals A
Explicitly,

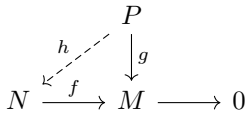
$x_0 \mapsto \{f \in A \mid f(x_0) = 0\} = P_{x_0}$
We can think about local rings:
$A_{P_{x_0}}$ = "germs of holomorphic functions at x_0 "
Claim: only ideals of $A_{P_{x_0}}$ are $(P_{x_0}^n)$
$f \in A_{P_{x_0}}$ then $n = \text{order}_{x_0} f$
Implies $A_{P_{x_0}}$ is a DVR
So A is a Dedekind domain.
Divisor class group
$Cl(A) = \frac{\mathbb{Z}[x]}{\{\sum_{x \in X} \text{order}_x f | f: X \to \mathbb{C} \cup \infty \text{ meromorphic}\}}$
$Cl(S^2) = \mathbb{Z}$
for higher genus, Cl = uncountable.
$Cl(A)$ is useful for characterizing the zeroes and poles of $f : X \to \mathbb{C} \cup \{\infty\}$

Class 39: 04/19
Today we prove:

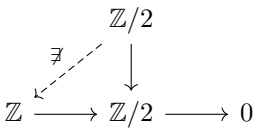
Proposition 74. domain A is DD $\iff$ every ideal is a projective module

What is a projective module?

Definition 95. Module P is projective if $\forall$ epimorphism $f : N \rightarrowtail M, \forall g : P \to M$ there exists lift $h : P \to N$ such that $f \circ h = g$



Nonexample: $\mathbb{Z}/2$ is not projective $\mathbb{Z}$ module



$A = \mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/6\mathbb{Z} \overset{A-\text{modules}}{=} \underbrace{2\mathbb{Z}/6\mathbb{Z}}_{P} \oplus \underbrace{3\mathbb{Z}/3\mathbb{Z}}_{Q}$
P projective not free.
Exercise: module P projective $\iff \exists Q$ such that $P \oplus Q$ free $\iff \forall$ SES $0 \to A \to B \to P \to 0$ splits.
Discrete Valuation Ring (DVR): local version of DD

Definition 96. DVR is a PID with a unique nonzero maximal ideal.

Example: $\mathbb{Z}_{(p)} = \{\frac{a}{b} p^k : (b, p) = 1\} \subset \mathbb{Q}$
$p^k \mathbb{Z}_{(p)}$
$M = p\mathbb{Z}_{(p)}$
eg DVR:
suppose prime $0 \neq P \lhd A$ PID
Then A_P is DVR
iireducible $f \in k[x]$
Then $k[x]_{(f)}$ is DVR

Definition 97. A discrete valuation on a field K:
Homomorphism $\nu : K^\times \rightarrowtail \mathbb{Z}$
$\nu(x + y) \geq \min(\nu(x), \nu(y))$

eg: $\nu_p : \mathbb{Q}^\times \to \mathbb{Z}$
$\nu_p(\frac{a}{b}p^k) = k$, $p \not| a, b$
Extend: $\nu(0) = +\infty$
Lemma: Let A be a domain. TFAE:
a: A DVR
b: [AM definition] $\exists$ DV $\nu : \mathrm{Frac}(A) \to \mathbb{Z}$ such that $A = \nu^{-1}[0, \infty]$

Proof. $\implies$: A PID means A UFD
Let $x \in A$ be 'unique' [upto unit] irreducible in A.
Define $\nu(ux^k) = k$ for $u \in A^\times$
$\impliedby$ Claim: $u \in K$
$u \in A^\times \iff \nu(u) = 0$
IE $A^\times = \nu^{-1}0$
proof: $0 = \nu(1) = \nu(uu^{-1}) = \nu(u) + \nu(u^{-1})$ tells us $\nu(u) = 0$
$\nu(u) = 0 \implies \nu(u^{-1}) = -0 = 0 \implies u, u^{-1} \in A$ // Claim
$b \implies a$
Let $\nu : K \to \mathbb{Z}$ be a DV
Choose $x \in K$ such that $\nu(x) = 1$
x "uniformizing parameter"
Then, $\forall a, a = ux^{\nu(a)}, uin A^\times$ (claim)
$\implies$ A is PID with unique maximal ideal (x)

□

Proposition 75 (AM 9.2)**.** Let A be noetherian local with $\dim A = 1$
TFAE:
i: A is DVR
ii: A IC
iii: The maximal ideal is principal
iv: resudue field $k = A/M$, $\dim_k(M/M^2) = 1$
v: Every nonzero ideal is a power of M
vi: $\exists x \in A$ such that I is nonzero ideal, then $I = (x^k)$

Example of noetherian local domain with $\dim A = 1$ but not DVR
Example:

$$\left(\frac{k[x,y]}{(y^2 - x^3)}\right)_{(x,y)}$$

Lemma [p95]: Let A be local, noetherian, $\dim A = 1$
A: If $0 \neq I \lhd A$ proper, $\exists m$ such that $I \supset M^m$
B: $\forall n, M^n \neq M^{n+1}$
Question: is $\bigcap M^n$ 0 for a local ring?
No, but Yes for DVR.

Proof. B: It is a consequence of Nakayama's Lemma
Recall: Nakayama: For M finitely generated A-module, $I \subset J(A) = \bigcap_{\text{maximal}} M$ then $IM = M \implies M = 0$
We use contradiction.
Assume $M^n = M^{n+1}$
So, $M(M^n) = M^n$
M finitely generated since Noetherian
Nakayama's Lemma means $M^n = 0$
Contradiction since A is a domain

□

Add:
Chapter 4: Definition of Primary along with Proposition 4.1, Definition of Primary Decomposition
??: Uniqueness? Probably not.
Chapter 7: Theorem 7.13, Dedekind domains and DVRs

Class 40: 04/22

Proposition 76 (AM 7.14)**.** Let A be Noetherian and $I \triangleleft A$. Then $\exists m$ such that $(\sqrt{I})^m \subset I$

Proof. Since A is noetherian, $\sqrt{I}$ is finitely generated.
$\sqrt{I} = (x_1, \cdots, x_k)$
$\forall i, \exists n_i$ such that $x_i^{n_i} \in I$
$(x_1, \cdots, x_k)^m$ is finitely generated. It's generators are monomials: $x_1^{r_1} \cdots x_k^{r_k}$ where $\sum_i r_i = m$
Let $m = (\sum_i (n_i - 1)) + 1$
Then $\exists i$ such that $r_i \geq n_i$
So, $x_i^{r_i} \in I$
Thus, $(\sqrt{I})^m \subset I$

□

Corollary 7.13 If A is Noetherian, then the 'ideal of nilpotents is nilpotent'.
$\exists m$ such that the nilradical $(\operatorname{rad} A)^m = 0$
In other notation, $\sqrt{0}^m = 0$
Consider the polynomial ring with infinitely many variables and take a quotient.

$$A = \frac{\mathbb{Z}[x_1, x_2, x_3, \cdots]}{(x_1, x_2^2, x_3^3, \cdots)}$$

Now, $\forall m, (\operatorname{rad} A)^m \neq 0$
Counterexample!
Lemma (p95) Let A be local domain, noetherian, $\dim A = 1$
Note that $\dim A = 1$ means nonzero primes are maximal.
Let M be a maximal ideal of A
A: $0 \neq I \triangleleft A$ [proper] implies $\exists n$ such that $M^n \subset I$
B: $M^n \neq M^{n+1} \forall n$

Proof. A: $\sqrt{I} = \bigcap_{I \subset P} P$
Since $\dim A = 1$ we have $\sqrt{I} = M$
Thus, by 7.14 we're done.
B: We already did with nakayama's lemma

□

Proposition 77 (AM 9.2)**.** Let A be a local noetherian domain, $\dim A = 1$. Let $k = A/M$. TFAE:
i: DVR
ii: A IC
iii: M principal
iv: $\dim_K M/M^2 = 1$
v: $0 \neq I \triangleleft A \implies I = M^k$
vi: $\exists x \in A$ s.t. $(0 \neq I \triangleleft A \implies I = (x^k)$ for some k)

Canonical example: $A = \mathbb{Z}_{(p)}$ where $x = p$

Proof. i $\implies$ ii: 5.18, 'valuation ring is IC'
ii $\implies$ iii: "hardest part"
Choose $0 \neq a \in M$
$A \implies \exists n$ such that $M^n \subset (a), M^{n-1} \not\subset (a)$
Choose $b \in M^{n-1}, b \notin (a)$
Let $x = \frac{a}{b} \in \operatorname{Frac}(A)$
Claim: $M = Ax$

Proof. $b \notin (a) \implies x^{-1} \notin A$
So x^{-1} not integral over A
$\implies x^{-1}M \not\subset M$ by 5.1 contrapositive
$x^{-1}M = \frac{b}{a}M \subset \frac{M^n}{a} \subset A$
Thus, $x^{-1}M$ is an ideal not contained in a max ideal
So, $x^{-1}M = A$ and thus $M = Ax$
iii $\iff$ iv:
M principal implies $\dim_k M/M^2M = 1$
by B say $M \neq M^2$; thu $\dim -kM/M^2 = 1$
$\impliedby$ 2.8
iii $\implies$ v: 8.8
postponed.
vi $\implies$ i:
Note that $M = (x)$
Note that $(x^k \neq x^{k+1})$ by B
Define $\nu : A-$
Define $\nu : A - \{0\} \to \mathbb{Z}_{\geq 0}$
$\nu(a) = k$ if $a \in (x^k) - (x^{Pk+1})$
define $\nu : K^\times - \mathbb{Z}$
$\nu(\frac{a}{b}) = \nu(a) - \nu(b)$

□

□

Correction to DD theorem
Recall: if A is domain, tfae: a: A DD, b: i: A is noetherian, ii: $\dim A = 1$, iii: $\forall P, A_P$ is DVR

Theorem 29 (AM 9.3)**.** : Let A be a noetherian domain with $\dim A = 1$
a: A is IC
b: $\forall P, A_P$ is DVR

$A \implies B.$: proof comes from 9.2, 5.13.
5.13: integrably closed is a local property

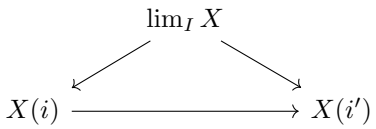
□

Class 41: 04/24

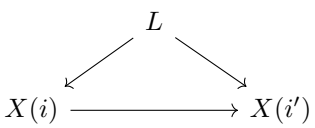
Limits, Colimits, Completion

Functor $X : I \to \mathcal{C}$ "I-diagram in $\mathcal{C}$ "

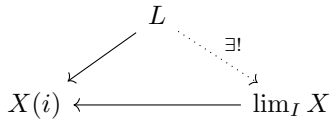
Definition 98. $\lim_I X$ is an object in $\mathcal{C}$ with map $\lim_I X \to X(i) \forall i \in I$ such that:
1: $\forall i \to i'$ we have:



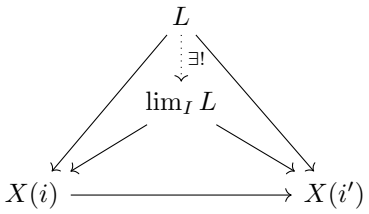
2: 'Initial'
$\forall (L \in \mathcal{C}, \{L \to X(i)\}_{i \in I})$



$\exists! L \to \lim_I X$ such that:



Define $\operatorname{colim}_I X$ by reverse arrow.
$X(i) \longrightarrow \operatorname{colim}_I X$



If (co)limit exist, they are unique (upto isomorphism)
(co)limits exists:
$\mathcal{C} = Ab, A$-mod, Group, Ring, CRing, Top, Set etc
(co)liit doesn't exist: $\mathcal{C} =$ Field.
Let $I = ., \mathcal{C} = A$-mod
$\lim_I X = X_0 \times X_1$
$\operatorname{colim}_I X = X_0 \oplus X_1$
Example: I discrete category (only morphisms are id)
$\lim_I X = \prod X(i)$
$\operatorname{colim}_I X = \bigoplus X(i)$
Note that $\prod X(i) \supset \bigoplus X(i)$, inclusion strict for infinite I

Theorem 30. If $\mathcal{C} = A$-mod then (co)limits exist.

Proof. Consider functor $X : I \to \mathcal{C}$
We can construct the limit as a submodule:

$$\lim_I X \subset \prod_i X(i)$$

'submodule of compactible tuples'
$\lim_I X = \{(x_i) \mid X(i \to i')(x_i) = x_{i'}\}$
$\operatorname{colim}_I X = \frac{\bigoplus X_i}{(\{x_i - X(i \to i')x_i\})}$

□

Example:
Suppose $I = (\mathbb{N}, \geq)$
Then we have 'morphisms' $5 \to 3$ aka $5 \geq 3$
Then, functor means we hve morphisms:

$$\cdots \to X_4 \to X_3 \to X_2 \to X_1$$

Then, $\lim_{(\mathbb{N},\geq)} X$ is called $\lim_{n\to\infty} X(n)$
This is called an "inverse limit"
Note: $\lim_{n\to\infty} X(n) \to X_k$ for all k
Think of limits as 'intersections' and colimits as 'unions'
If the morphisms are 'inclusion':

$$\cdots \subset X_3 \subset X_2 \subset X_1 \subset X_0$$

Then $\lim_{n\to\infty} X_n = \bigcap_{n=1}^{\infty} X_n$
Classic example: p-adic

$$\cdots \to \mathbb{Z}/p^3 \to \mathbb{Z}/p^2 \to \mathbb{Z}/p$$

Then p-adic integers $\hat{\mathbb{Z}}_p = \lim_{n\to\infty} \mathbb{Z}/p^n$

Note that all these are rings so essentially $I \to \text{CRing}$.
$I \triangleleft A$
We can have $\cdots \to A/I^3 \to A/I^2 \to A/I$
Then $\hat{A}_I = \lim_{n\to\infty} A/I^n$
Application:
Krull's Intersection Theorem Let A be a noetherian and A is either local or a domain.
Then $A \to \hat{A}_I$ is injective, ie $\cap I^n = 0$
Consider categories:

$$\begin{array}{ccc} \cdot & \longrightarrow & \cdot \\ \downarrow & & \\ \cdot & & \end{array}$$

colim is called pushout

$$\begin{array}{ccc} & & \cdot \\ & & \downarrow \\ \cdot & \longrightarrow & \cdot \end{array}$$

limit is called pullback
Now suppose $X : I \to \mathcal{C}$ and consider SES:

$$0 \to X' \to X \to X'' \to 0$$

Question: colimit and limit SES??

Galois Theory

Suppose

$$\begin{array}{ccc} & & E \\ & \overset{Galois}{\nearrow} & \\ F & & \end{array}$$

What if extension not finite?
Example of not Galois:

$$\begin{array}{ccc} & & \mathbb{Q}[\sqrt[3]{2}] \\ & \nearrow & \\ \mathbb{Q} & & \end{array}$$

Not Galois since not contain all roots.
But we also have $\overline{\mathbb{Q}}/\mathbb{Q}, \overline{\mathbb{F}_p}/\mathbb{F}_p$
Makes sense as union of finite extensions:
$\text{Gal}(E/F) \coloneqq \lim_{E/L/_{finite}F} \text{Gal}(L/F)$. Note:

$$\begin{array}{ccc} & & \lim_K \text{Gal}(L/K) \\ & \nearrow & \\ L & & \\ & \overset{\text{finite galois}}{\nearrow} & \\ F & & \end{array}$$

Fundamental Theorem of Galois Theory: $\exists$ 1-1 correspondence between closed subgroups of $\text{Gal}(E/F)$ and $E/L/F$
by $H \mapsto E^H$
Note:

$$\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$