8000 fall 2006 day one

Introduction.

We will begin with the study of commutative groups, i.e. modules over the integers Z. We will prove that all fin gen abelian groups are products of cyclic groups. In particular we will classify all finite abelian groups. Then we will observe that the same proof works for modules with an action by any Euclidean or principal ideal domain, and generalize these results to classify f.g. modules over such rings, in particular over the polynomial ring k[X] where k is a field. This will allow us to deduce the usual classification theorems for linear operators on a finite dimensional vector space, since a pair (V,T) where T is a linear operator on the k space V, is merely a k[X] module structure on V. We recall some familiar definitions.

A **group** is a set G with a binary operation GxG--->G which satisfies:
(i) associativity, a(bc) = (ab)c, for all a,b,c, in G;
(ii) existence of identity: there is an element e: ea = ae = a for all a in G.
(iii) existence of inverses: for every a in G, there is a b : ab = ba = e.

A **subgroup** of G is a subset $H \subset G$ which is a group with the same operation. H has the same identity as G, and the inverse for any element in H is its inverse in G.

A group G is **commutative**, or **abelian,** if also **(iv)** ab = ba for every a,b, in G.

Remarks: We will study mostly commutative groups in the first part of the course, and we will usually write them additively instead of multiplicatively, thus we write the identity as 0. Two advantages of commutative groups are the following: if G (commutative) has elements a,b, such that na = 0 = mb, where n,m are positive integers, and if p = lcm(n,m), then G has an element c such that pc = 0. Also the subset of elements a of G such that na = 0 for some integer n>0, i.e. the set of elements of "finite order", is a subgroup of G. Thus it is easier to understand the "orders" of the elements of a commutative group. Also it is easier to construct the "coproduct", sometimes called the "direct sum", of a family of commutative groups.

All groups are assumed commutative until we say otherwise.
Important Examples: i) the set Z of integers is a group for addition; **ii)** if n is an

integer, the multiples of n form a subgroup $nZ \subset Z$; **iii)** the rationals form a subgroup of the reals for addition $Q \subset R$; **iv)** the positive rationals form a multiplicative subgroup of the positive reals $Q^+ \subset R^+$; **v)** S^1 = the complex numbers of length one, form a multiplicative subgroup of the non zero complex numbers, called the circle group.

It is efficient to use a subset of the elements of a group to represent all others, and the number of elements so needed helps measure the size of the group.
A subset $S \subset G$ **generates** G if there is no subgroup containing S except G, equivalently if every non zero element of F can be written as a finite linear combination $n_1a_1 + ...+n_ka_k$, where all a_i are in S and the n_i are integers. If G is written multiplicatively it means all elements except e can be written as a finite product $\prod a_i^{n_i}$. **Examples:** {1} or {-1} generates Z. The empty set generates the trivial group {0}. The interval (0,d) generates (R,+) if $d > 0$. The positive primes generate Q^+. G is **finitely generated, fin gen, or f.g.,** if G has a finite set of generators. G is **cyclic** if one generator suffices. Z is cyclic. Q^+ and S^1 are not finitely generated.

We proceed to the classification of fin gen abelian groups. The relevant concepts are **products, quotients, isomorphisms,** and **linear maps**.

Fundamental constructions (on abelian groups)
I) Products: Given an indexed family of (abelian) groups $\{G_i\}_I$, form the cartesian product set $\prod_I G_i$ of functions from the index set I to the union of the groups G_i where the vaue of each function at i lies in G_i. Define the operation pointwise on functions, i,.e. multiply or add the values of the functions. If I = {1,...n}, the elements are ordered n tuples of elements, one from each G_i, added componentwise, like vectors. The identity is the function whose value at each i is the identity of G_i.

II) Coproducts: This is similar to the construction as above, except the functions must have the value 0 except possibly at a finite number of indices. Hence it is the same if the index set I is finite. It is denoted by an upside down product or a summation sign, $\sum_I G_i$. The coproduct of a family of (abelian) groups is a subgroup of the product.

If all groups G_i are equal to the integers Z, we call their coproduct a "**free abelian group**" on the set I, i.e. a group of form $\sum_I Z_i$. We also write Z^n for the product (or sum) of n copies of Z. The set of **standard basis vectors** $\{e_i = (0,...,0,1,0,....0)$ where there are n entries and the 1 is in the ith place, for $i =1,....,n\}$, generates Z^n. Other product groups are R^n, $S^1 x R$, and $S^1 x S^1$= the torus group.

III) Quotients: If $H \subset G$ is a subgroup, the quotient group G/ H is the set of equivalence classes of elements of G for the relation $x \equiv y$ iff x-y belongs to H. Write [x] for the equivalence class of x and add by setting [x]+[y] =[x+y], after checking this is independent of choice of representative elements of the classes.

A fundamental quotient group is Z/(nZ), the additive group of integers "mod n". When we define isomorphism, we will see that the circle group is isomorphic to a quotient group $S^1 \cong R/Z$; and $S^1 x S^1 \cong (R/Z)x(R/Z) \cong (RxR)/(ZxZ)$. The interchange of quotients and products is more subtle than it may appear, and will play a crucial role in the proof of the fundamental theorem we are seeking. The fact that renders the interchange easy here is that each factor group in the denominator is a subgroup of the corresponding factor in the numerator. When this is not the case the problem is more difficult.

Each product $(Z/n_1Z)x(Z/n_2Z)x....x(Z/n_kZ)$ is a finite abelian group. Our goal is to show these products give essentially all finite abelian groups. To make this precise, we must define when we will say two groups are essentially the same.

A map of groups f:G-->H (abelian or not) is a **homomorphism**, or a map, if for all a,b, in G, f(ab) = f(a)f(b), or if f(a+b) = f(a) + f(b). It follows that f(0) = 0 , and f(-x) = -f(x), or that f(1) = 1 and $f(x^{-1}) = [f(x)]^{-1}$. The set of homomorphisms from G to H is denoted **Hom(G,H)**. When G,H are abelian it is also an abelian group under pointwise addition, [but it is not even a group if H is not abelian.]

Examples of homomorphisms: The inclusion of a subgroup $H \subset G$ is a homomorphism; The map G--->G/ H taking an element x to the class [x] is a homomorphism; The ith projection $\prod_I G_i$--->G_i taking a function to its value at i, or taking a vector to its ith component, is a homomorphism. The injection

G_i--->$\sum_I Z_i$ taking an element x of G_i to the function having value x at i and value 0 elsewhere, is a homomorphism. [This puts x in the ith component of a vector and 0's elsewhere.] The map R--->S^1 taking t to e^(2πit) is a homomorphism.

Important invariants of a homomorphism

To understand a homomorphism we focus on what goes to 0, and what things get "hit" by it. If f:G-->H is a homomorphism of groups (abelian or not), the subset kerf = {x in G : f(x) = 0} = the **kernel of f,** is a subgroup of G. The subset Im(f) = {y in H: y = f(x) for some x in G} = the **image of f,** is a subgroup of H.
The quotient H/Im(f), defined **for abelian groups only,** is the **cokernel of f.**

An **isomorphism** is a homomorphism with an inverse homomorphism. A homomorphism f:G-->H , is an isomorphism if and only if there is a homomorphism g:H--->G such that fog = id(H), and gof = id(G).

How to recognize an isomorphism: A homomorphism f:G-->H is an isomorphism if and only if it is bijective, if and only if kerf = {0} and Im(f)= H.

How to define homomorphisms: 0

0) For any G, Hom(Z,G) ≅ G, by sending f to f(1).

1) To define a homomorphism to a product G--->$\prod_I G_i$, define one G--->G_i into each G_i. I.e. Hom(G, $\prod_I G_i$) ≅ $\prod_I$Hom(G,G_i), by taking f:G---> $\prod_I G_i$ to the family of compositions $\pi_i$of, where π_i is the projection $\prod_I G_i$ --->G_i.

2) To define a homomorphism out of a coproduct $\sum_I G_i$--->H, define one out of each summand G_i--->H, i.e. Hom($\sum_I G_i$,H) ≅ $\prod_I$Hom(G_i,H) by taking f:$\sum_I G_i$-->H to the family of compositions foß$_i$, where ß$_i$ is the injection G_i--->$\sum_I G_i$.

3) To define a map from Z^n--->Z^m, by 0) and 2), define n maps Z--->Z^m, i.e. choose a matrix of n column vectors from Z^m, where the ith column is the image under the map of the ith standard basis vector e_i = (0,...,0,1,0,...,0).
I.e. Hom(Z^n, Z^m) ≅ $Mat_{mxn}(Z)$.

4) To define a map G/H--->K, define a homomorphism f:G---K such that f(H) = {0}, i.e. Hom(G/H,K) ≅ Hom((G,H), (K,{0})) (maps of pairs), by taking f:G/H--->K, to the composition foπ:G--->K, where π:G--->G/H is the projection.

5) If f:G--->H is surjective, the map G/kerf--->H in 4) is an isomorphism.

Examples: The map R--->S^1 sending t to e^(2πit) induces an isomorphism R/Z--->S^1, by 5) above. The maps Z--->(Z/ r_iZ), induce a map Z^n--->(Z/r_1Z)x...x(Z/r_nZ) and an isomorphism Z^n/[(r_1Z)x...x(r_nZ)]--->(Z/r_1Z)x...x(Z/r_nZ).

If P is the index set of positive prime integers, the map $\sum_P Z_p$--->Q^+ taking $\{r_p\}$ to the (essentially finite) product $\prod_P p^{(r_p)}$ is an isomorphism by the fundamental theorem of arithmetic, so Q^+ is (isomorphic to) a free abelian group.

Our first big theorem is the following.
Theorem: If G is a finitely generated abelian group, there exist integers n, m≥ 0, and a sequence of integers $r_1,...,r_m \geq 2$, such that G ≅ Z^n x (Z/r_1Z)x...x(Z/r_mZ). These r's can be chosen so that $r_1 | r_2 | ... | r_{m-1} | r_m$, i.e. each one divides the next; if so, then all the integers are uniquely determined by the isomorphism class of G.

We call n the rank of G and the integers $r_1,...,r_m$ the invariant factors. G is determined by (n, $r_1,...,r_m$). If n = m = 0, there are no r's and G = {0}.

Exercises: If Tor(G) = {x in G: for some n>0, nx = 0}, Tor(G) is a subgroup of G, called the torsion subgroup. [This is not a subgroup if G is not abelian.]

Cor: If G ≅ Z^n x (Z/r_1Z)x...x(Z/r_mZ), then Tor(G) ≅ (Z/r_1Z)x...x(Z/r_mZ), and G/Tor(G) ≅ Z^n . Tor(G) is a uniquely defined subgroup of G, and the free part is a uniquely defined quotient group. Since Z^n is a subgroup of the right hand product, such an isomorphism picks out a subgroup of G isomorphic to Z^n, but this subgroup, and the isomorphism of G with the product, is not uniquely determined.

Proposition: If G is a fin gen abelian group, with m generators, there is a homomorphism f:Z^n--->Z^m , with n ≤ m, such that G ≅ coker(f) = Z^m/f(Z^n).

proof: The surjectivity $Z^m \to G$ is easy, and the surjection of Z^n onto the kernel of $Z^m \to G$ follows by an inductive proof that the kernel is finitely generated.

Note that although the denominator may be isomorphic to Z^m, there is no reason for each factor to be a subgroup of just one factor of Z in the numerator. Hence there is no obvious way to write the quotient of products of Z, as a product of quotients of Z, as we did earlier. Still it can be done, as we show next. The key point is that this is true when the matrix of f is diagonal, and a matrix of integers can always be diagonalized without changing the isomorphism class of the cokernel.

Proposition: If A is the matrix of $f: Z^n \to Z^m$, and if B is a matrix obtained by elementary row and column operations from A, then the cokernels $Z^n/A(Z^m) \cong Z^n/B(Z^m)$, are isomorphic.
proof: B is a composition of A with isomorphisms of domain and target.

Proposition: Every matrix A of integers can be reduced by elementary row and column operations, to a diagonal matrix B.
proof: This is essentially the usual Gauss elimination process. It relies on the fact that two integers have a gcd which is a linear combination of the two integers, and which can be obtained by repeated divison, or subtraction.

Corollary: The existence part of the theorem is true (subject to proving the 3 previous propositions.

Proof of existence and uniqueness of the cyclic decomposition.
Theorem: If G is any finitely generated abelian group, then G is isomorphic to a product of a finite number of cyclic groups, with the number of factors equal to the minimum number of generators, and such that the orders of successive finite factors divide each other.

Moreover, given generators and explicit generating relations among them for G, we can actually calculate the decomposition, by diagonalizing a matrix of integers whose columns are the coefficient vectors for the relations.

Proof: We want to split G as a product of cyclic subgroups, so it is useful to

understand when this sort of splitting is easy.

Basic splitting lemma 1: If f:H--->Z--->0 is any surjective homomorphism onto Z, then H is isomorphic to kerf x Z.
[Define a right inverse for f, and use that to define the splitting.]

Lemma 2: Any subgroup of Z^m is finitely generated and in fact free on at most m generators.
proof: induction on m. true for m = 1, since a subgroup H of Z is generated by an element of H of smallest absolute value. If true for k-1, consider the projection q:Z^k--->Z, where $q(c_1,....,c_m) = c_1$, where kerq = Z^(k-1). Then q(H) is a subgroup of Z hence generated by one generator, thus is either {0} or isomorphic to Z.

If q(H) is {0} then H lies in Z^(k-1) and we are done by induction. If q(H) is isomorphic to Z then we get a surjection q:H--->Z--->0. Hence by the basic splitting lemma, H is isomorphic to kerq x Z. Since kerq is a subgroup of Z^(k-1), we are again done by induction. **qed.**

Lemma 3: G is isomorphic to the cokernel of a matrix of integers.
proof: Let $x_1,...,x_m$ be generators for G, and define the map p:Z^m--->G by $p(c_1,....,c_m) = c_1x_1+....+c_mx_m$. p is surjective and H = kerp has some finite set of generators, say $y_1 = [a_{11},....,a_{m1}]$,....., $y_n = [a_{1n},.....,a_{mn}]$. Then define a map f:Z^n--->Z^m by sending e_i to y_i for i = 1,...,n. This map has m by n matrix [f] whose columns are the vectors y_j. Cokerf = Z^m/Im(f) which by choice of f, equals Z^m/ker(p), which by the fundamental isomorphism theorem, is isomorphic to G. **qed.**

Lemma 4: Every integer matrix f can be brought to diagonal form, by a sequence of elementary invertible row and column operations, i.e. multiplying rows and columns by 1 or -1, interchanging two rows or two columns, and adding an integer multiple of one row to another row, or adding an integer multiple of one column to another column.
proof: It suffices to see how to transform a row of two entries [a b] into one of form [d e], where d divides a and e. By Euclid's algorithm, repeatedly subtracting multiples of one entry from the other, we reach a pair [d e], where d = gcd(a,b) also

divides e. Transform the first row and column until the upper left entry divides all others. If an entry is not divisible by the upper left entry, Euclid makes the new upper left entry a factor of the original one. Hence applying Euclid no more times than the number of prime factors of the original upper left entry, we reach a matrix where the upper left entry divides all other entries in first row and column. Then we make all those zero. [Thus it is prudent to put an integer there which has small gcd with some other entry.] By induction we can diagonalize the rest of the matrix the same way. **qed.**

Lemma 5: Any diagonal matrix of integers can be further transformed until all entries on the diagonal successively divide each other.
proof: If the matrix is diagonal, add all columns to the first column, and rediagonalize, obtaining an upper left entry which is divides all original diagonal entries. Then proceed by induction to re diagonalize the remaining smaller matrix, until eventually one has a diagonal matrix where all diagonal entries divide each other successively. **qed.**

Lemma 6: If an m by n matrix is diagonal, and if $n \geq m$, with diagonal entries $a_1,...,a_m$, then its cokernel is isomorphic to $Z/a_1 \times ....x\ Z/a_m$. If $m > n$, then the diagonal entries are $a_1,...,a_n$, and if we set $a_{n+1},...,a_m = 0$, then again the cokernel is isomorphic to $Z/a_1 \times ....x\ Z/a_m$.
exercise:

Note: Lemmas 1-6 prove the theorem. Since our diagonalizing process reduces the number of generators, if we start from a minimal set, the process must give that same number of factor groups. If the diagonal matrix is A, then some diagonal entries a_i have $|a_i| = 1$ if and only if the generating set was not minimal, and some columns of A are zero if and only if the set of relations was not minimal.

Uniqueness of invariant factors.
Theorem: If G is a finitely generated abelian group, there is a <u>unique</u> sequence of integers r, s, $n_1,...,n_s$, with $r,s \geq 0$, all $n_i \geq 2$, such that for all $i = 1,..,..,s$, $n_i | n_{i+1}$, and G isomorphic to $Z^r \times Z/n_1 \times ...x\ Z/n_s$. r is the rank of G and if $s > 0$, $\{n_i\}$ are the invariant factors.

Thus the isomorphism classes of finitely generated abelian groups correspond one to one with such sequences of non negative integers. I.e. although each isomorphism class contains many different looking groups, it contains exactly one of this form.

First we separate the finite factors from the infinite ones by defining TorG = elements of finite order in G. If $G \approx Z^r \times Z/n_1 \times ... \times Z/n_s$, then TorG $\approx$ $Z/n_1 \times ... \times Z/n_s$, and $G/TorG \approx Z^r$.

Lemma: $Z^r \approx Z^t$ implies r = t.
Exercise. Thus rank is well defined.

To recover the invariant factors n_i from G intrinsically, we will exploit the fact that cyclic factors of different orders give rise to elements of different orders. We will do this somewhat indirectly, using the fact that the map p^t:G--->G multiplication by p^t, has kernel equal to the elements of order dividing p^t. We will focus in fact on the images of these maps. The prime factorization of every n_i and hence n_i itself, is entirely determined by the images of these maps as follows. This clean approach appears in van der Waerden. The technique will re - appear later as a procedure for constructing Jordan forms of matrices from kernels of powers of operators.

Lemma: If $H \approx Z/n_1 \times ... \times Z/n_s$, p is a prime integer, and $r \geq 1$, then $p^{r-1}H/p^rH$ is a group of order p^k where k is the number of factors n_i which are divisible by p^r. If
$n_i | n_{i+1}$, for all i, these must be the last k factors.

This proof is a straightforward application of the standard isomorphism theorems, so we review those. The first one is the primary one, the others being applications of it. As usual all groups are abelian.
1) If f:G--->H is a homomorphism, there is a unique induced homomorphism g:G/kerf--->H which is injective, and such that
G--->G/H--->H equals f. If f is surjective, g is an isomorphism.
proof: we seek to define g([x]) = f(x), since that will be the only map that could

make the composition equal to f. For this to be well defined, it is sufficient that whenever [x] = [y], that g take the same value on [x] and [y]. But g([x]) = f(x), and g([y]) = f(y), so it suffices that [x] = [y] implies f(x) = f(y). But [x] = [y] implies that x-y is in kerf so f(x-y) = 0 = f(x) - f(y), hence f(x) = f(y).

Now that g is well defined, it is a homomorphism by definition, and to check injectivity we ask whether g([x]) = 0 implies [x] = [0]. But g([x]) = f(x) so g([x]) = 0 implies x is in kerf, hence [x] = [0]. If f was surjective, trivially so is g, hence g is an isomorphism.

2) If K is a subgroup of H and H a subgroup of G, we claim $G/H \approx (G/K)/(H/K)$.
proof: Just define a map from G---->G/K sending x to [x] as usual, and compose with the similar map to (G/K)/(H/K). Since H/K consists of elements [x] of G/K where x is in H, the kernel of G-->G/H--->(G/K)/(H/K), is those elements x of G belonging to H. By part 1) above we have our result.

3) If H,K are subgroups of G, not necessarily nested, then $(H+K)/K \approx H/(H\text{meet}K)$, where "meet" means "intersect".
proof: same as before, define a map from H--->H+K sending x to x, and compose with H+K--->(H+K)/K. The kernel is then HmeetK. so we have an injection from H/(HmeetK)--->(H+K)/K. But we claim it is also surjective, since if x+y belongs to H+K, with x in H and y in K, then [x+y] = [x] mod K, so x maps to [x] = [x+y], and hence H---(H+K)/K was surjective, hence induces an isomorphism H/(HmeetK)--->(H+K)/K.

Now we examine some cyclic groups, maps between them, and quotients.
1) let m be any integer, then we multiply on a product $G = G_1 x ... x G_s$ by multiplying separately on each factor, hence we have $mG = mG_1 x ... x mG_s$ where mH denotes the image of the map "multiplication by m".

2) If p is a prime number which does not divide n, then
p^t:(Z/nZ)--->(Z/nZ) has kernel zero, hence is surjective.
proof: In the ring Z/nZ, p^t is a unit.

3) If $t \leq r$, then $\{p^{t-1}(Z/p^rZ)\}/\{p^t(Z/p^rZ)\} \approx Z/pZ$.
proof: since multiplication of equivalence classes is done by multiplying their

representatives, we have

$\{p^{t-1}(Z/p^rZ)\} \approx \{p^{t-1}Z\}/p^rZ)$, hence

$\{p^{t-1}(Z/p^rZ)\}/\{p^t(Z/p^rZ)\} \approx \{p^{t-1}Z/p^rZ\} /\{p^tZ/p^rZ\}$.

Now since $t-1< t \leq r$, the group $p^r Z$ is a subgroup of $p^t Z$, which in turn is a subgroup of $p^{t-1}Z$. Hence the second isomorphism theorem above gives $\{p^{t-1}Z/p^rZ\} /\{p^t Z/p^r Z\} \approx \{p^{t-1}Z/p^t Z\}$.

Now define a map $Z\text{--->}p^{t-1}Z$, by multiplication by p^{t-1} and compose to get $Z\text{--->}p^{t-1}Z/p^tZ$. The kernel is those numbers which when multiplied by p^{t-1}, turn out to be multiples of p^t, i.e. the kernel is all multiples of p. So we have by the first isomorphism theorem, that $Z/pZ\text{--->}p^{t-1}Z/p^tZ$, is an isomorphism. QED.

4) If $t \geq r$, then $p^t:(Z/p^r Z)\text{--->}(Z/p^r Z)$ has kernel equal to all of $(Z/p^r Z)$, hence the image $p^t(Z/p^r Z)$ is zero.

Cor: If $t > r$, then $\{p^{t-1}(Z/p^r Z)\}/\{p^t(Z/p^r Z)\} = \{0\}$.

5) If $H \approx Z/n_1 \text{ x } ...\text{x } Z/n_S$, p is a prime integer, and $r \geq 1$, then $p^{r-1}H/p^r H$ is a group of order p^k where k is the number of factors n_i which are divisible by p^r.
proof: This follows from combining the results above with a hw problem.

I.e. factor each $n_i = p^{r_i} m_i$ where p does not divide m_i. Then we have $H \approx Z/n_1 \text{ x } ...\text{x } Z/n_S \approx Z/m_1 \text{ x } ...\text{x } Z/m_S \text{ x } Z/p^r1 \text{ x } ...\text{x } Z/p^rs$.

Then $p^{t-1}G/p^t G$ can be computed separately on each factor, and gives zero for each factor of form Z/m_i, and gives zero also for each factor Z/p^{r_i} where $t > r_i$, and gives one copy of Z/pZ for each factor Z/p^{r_i} where $t \leq r_i$. This proves the first part of the lemma. I.e. we get k factors of Z/pZ if exactly k of the n_i are divisible by p^t. The part about the factors being the last k factors under our divisibility condition is easy.

This completes the uniqueness, hence the full proof of the decomposition theorem for finitely generated abelian groups. Next we look at a few rings R more general than Z, where we can imitate these theorems for abelian groups admitting a multiplication action by R.

Appendix: Artin's short, unconstructive proof of existence of the cyclic decomposition for finitely generated abelian groups.
Theorem: If G is a finitely generated abelian group, then G is isomorphic to a product of cyclic groups, where the number of factors equals the minimal number of generators for G. In fact we may arrange that the orders of successive finite cyclic factors divide each other.

proof: We leave the case of one generator to the reader. If there is a finite generating set for G satisfying no relations, then G is generated by a linearly independent set and hence is isomorphic to a product of copies of Z, done. So assume relations exist.

Then among all finite generating sets for G choose one: $\{y_1,x_2,...,x_n\}$ satisfying a relation $a_1y_1+a_2x_2+....+a_nx_n$, with a non zero coefficient of smallest absolute value, which we may assume is a_1.

Divide every a_i with $i > 1$ by a_1, i.e. write $a_i = q_i\, a_1 + r_i$, where r_i has smaller absolute value than a_1. Since the minimal generating system $\{x_1, x_2,..., x_n\}$ where $x_1 = y_1 +q_2\, x_2 - ....+q_n\, x_n$, satisfies the relation $a_1\, x_1+r_2\, x_2+....+r_n\, x_n$, it follows that all $r_i = 0$, for $i > 1$, i.e. a_1 divides every a_i with $i > 1$. In particular $|a_1|$ is the annihilator of x_1, i.e. $a_1\, x_1 = 0$, but no integer of smaller absolute value than a_1 annihilates x_1.

If $c_1\, x_1+c_2\, x_2+....+c_n\, x_n$ (*) is any relation among the new generating set, and if we divide c_1 by a_1, hence $c_1 = q\, a_1+r$, with $|r| < |a_1|$, then subtracting $q\, a_1\, x_1 = 0$ from the relation (*), gives the relation $rx_1+c_2\, x_2+....+c_n\, x_n = 0$, with $|r| < |a_1|$, whence $r = 0$, i.e. a_1 divides c_1.

Now define a map G---> $<x_1>$ = the subgroup of G generated by x_1, by

sending the element $x = c_1 x_1+c_2 x_2+....+c_n x_n$ to $f(x) = c_1 x_1$. Although this expression is not unique, the map is well defined since we have just shown that if $x = c_1 x_1+c_2 x_2+....+c_n x_n = 0$, then a_1 divides c_1, and hence $f(x) = c_1 x_1 = 0$.

Lemma: If H is a subgroup of G, and f:G--->H is a map such that f(x) = x for all x in H, then the map G---> H x ker(f), defined by the maps f, and f-id, is an isomorphism which is inverse to the map H x kerf---> G defined by the inclusions..

The lemma applied to the subgroup $<x_1>$ in G and the map f:G---> $<x_1>$ defined above, shows that G is isomorphic to $<x_1>$ x ker(f) = (Z/a_1) x ker(f). Since ker(f) is generated by $x_2,...,x_n$, and $x_1,...,x_n$ is a minimal generating set for G, thus $x_2,...,x_n$ is a minimal generating set for kerf, so by induction kerf is a direct product of n-1 cyclic subgroups. Hence we have our decomposition of G.

To get the successive divisibility condition, note that if $c_2 y_2+....+c_n y_n = 0$ is any relation among a minimal set of generators of kerf, then since $a_1 x_1 = 0$, we see that $a_1 x_1 + c_2 y_2+....+c_n y_n = 0$, is a relation among a minimal set of generators of G in which the minimal coefficient a_1 occurs. Thus by a previous argument (in the 3rd paragraph), a_1 divides all the coefficients c_i with $i > 1$. Hence the decomposition of kerf will involve only cyclic factors whose order is divisible by a_1. Since by induction they also divide each other successively, we are done. **QED.**

Note: This argument shows the theorem is true, but gives no clear way to find a decomposition for a specific group which is presented by generators and relations. Thus our matrix reduction technique is preferable in concrete examples.

Observe Artin's proof also used Euclid's algorithm, to get contradictions to minimality of some integers. If these integers were not minimal at first, Euclid's algorithm could be used to reduce their size, eventually obtaining minimal such integers. That would have been equivalent to the row and column operations we have described. Thus the matrix proof is a concrete version of Artin's.

Perhaps Artin took a classical matrix proof, and rendered it shorter by removing the matrices, in accord with his philosophy that matrices should only be used when a specific computation is needed.

8000 Day Two: Brief course on commutative rings

Rings and Ideals

The classification of finitely generated abelian groups was in two steps.
1) Using the action of the ring of integers on an abelian group we presented the given group as the cokernel of a matrix of integers.
2) Then we diagonalized the presentation matrix using the fact that the gcd of two integers is a linear combination of those two integers.

We can use this method to classify more general abelian groups, not necessarily finitely generated as groups, but finitely generated in terms of the action of some other ring. To extend the proof we will need a ring in which any two elements have a gcd which is a linear combination of those elements. Such a ring is called a principal ideal domain. Of course our understanding of such more general groups will be no better than our understanding of the corresponding ring and its ideals.

To present the generalized argument we must pause to develop the concepts of rings, ideals, and abelian groups with an action by a ring R, i.e. "R - modules".

Review of basic definitions and properties of rings and ideals

Rings: A ring is an abelian group under addition which also has another associative operation called multiplication, which distributes over addition, and which has an identity element called $1 \neq 0$. If multiplication is commutative, the ring is called commutative. We assume our rings are commutative unless explicitly stated otherwise.

A unit in a ring is an element which has a multiplicative inverse. It is extremely important to determine which elements of a ring are units.

Examples: Polynomials in one or more variables with integer or rational coefficients, Z[X], Z[X,Y],...,Q[X], Q,[X_1,...,X_n] are commutative rings. Square matrices larger than 1x1, with entries in a ring, such as 2x2 integer matrices, form a non commutative ring.

Ring maps: A (unitary) ring map, or homomorphism, is a function between two rings f:R-->S that preserves addition, multiplication, and takes 1 to 1. Thus a

(unitary) homomorphism takes units to units. A ring map is an isomorphism iff it has a 2 sided inverse homomorphism. We assume all our ring maps are unitary and all our rings are commutative.

Polynomials: If R is a (commutative) ring, define the (commutative) ring of polynomials R[X] over R, to consist of all formal linear combinations of non negative powers of X, e.g. R[X] = {a0 + a1X + a2X^2+....+anX^n, where the ai are in R} and as usual X^i X^j = X^(i+j). A polynomial is monic if the leading coefficient an = 1.

Examples: If R is a ring, there is a unique ring map Z-->R. If f:R-->S is a map of rings, and c is any element of S, there is a unique ring map R[X]-->S extending f and sending X to c. It is called "evaluation at c" if f:R-->R is the identity map. If R is a ring, there is a ring map from the rationals Q-->R if and only if the unique ring map Z-->R is injective and every non zero element of Z becomes a unit in R. If R is a ring the map R[X][Y]-->R[X,Y] which is the natural injection of R[X] and takes Y to Y, is an isomorphism.

Ideals: An ideal I of a ring R is a subgroup that is also closed under multiplication by R. (In a non commutative ring we must distinguish left, right and two sided ideals, according to which side we multiply on by R.)

The kernel of a ring homomorphism f:R-->S is the ideal of elements x in R s.t. f(x) = 0.

An ideal is proper (different from R) if and only if it does not contain any units, iff it does not contain 1.

If I is a proper ideal of R, (two sided if R is not commutative) the quotient group R/I has a natural ring structure, such that R--->R/I is a ring map with kernel I.

A ring homomorphisms R/I-->S is equivalent to a ring homomorphism R -->S that sends every element of I to zero, i.e. every ring map f:R-->S with I in the kernel of f, factors uniquely as R-->R/I-->S.

Two elements a,b of a ring are associates if a = ub, where u is a unit. An element u is a unit if and only if u is associate to 1. If a divides b, then every associate of a divides every associate of b.

An ideal I is generated by a subset of elements $\{x_i\}$ of I, iff each non zero element of I is an R linear combination of some finite subset of the $\{x_i\}$, iff I is

the smallest ideal of R containing the set $\{x_i\}$. If the same finite subset of elements $\{x_i\}$ can be used to generate every element of I, then I is finitely generated. An ideal is principal if it has one generator.

A ring is called noetherian if every ideal is finitely generated, and principal if every non zero ideal is principal.

Domains: A zero divisor is a non zero element x such that xy = 0 for some non zero element y. Every associate of a zero divisor is also a zero divisor. A ring R is a domain, or integral domain, or entire, if it has no zero divisors, i.e. if xy = 0 implies at least one of x or y = 0.

A proper ideal I is prime iff when ab belongs to I, then at least one of a or b is in I, equivalently iff R/I is a domain. A non zero, non unit element x is prime iff the principal ideal Rx = (x), is proper and prime, i.e. iff x divides ab only when x divides at least one of a or b.

In a domain, two elements are associates if and only if they divide each other, if and only if they generate the same principal ideal.

A principal domain is called a pid (principal ideal domain).

Fields: R is a field if every non zero element is a unit. A unit is never a zero divisor so a field is always a domain.

A proper ideal I is maximal iff it is not contained in another proper ideal. A ring is a field iff the only proper ideal is $\{0\}$. An ideal I is maximal iff R/I is a field. It follows that in any ring a maximal ideal is prime.

Euclidean domains: A domain R is Euclidean, if there is a "size" function $|\ |: R-\{0\} \to Z^{\geq 0} = \{\text{non negative integers}\}$, such that for any $b \neq 0$, and any a, there exist q,r such that a = qb + r, and either r = 0, or $|r| < |b|$. I.e. if b does not divide a, at least the remainder r is smaller than b. A Euclidean domain is a pid, since it follows that an ideal is always generated by any one of its elements of smallest size.

A Euclidean domain R is strongly Euclidean, if for all a,b, $|a| \leq |ab|$, and if equality holds precisely when b is a unit.

GCD's: A greatest common divisor, or gcd, of two elements x,y, (or any finite number of elements) in a domain, is an element z such that z divides both x and y, and if the common factors of x and y are precisely the factors of z. An associate

of a gcd of x,y, is also a gcd of x,y. I suppose 0 is the gcd of (0,0) or we could require x,y are not both 0. Gcd's need not always exist.

Unique factorization: An element x of a domain is irreducible if x is not zero and not a unit, and whenever x = bc, then either b or c is a unit. A prime element of a domain is irreducible, but not always vice versa.

A domain is factorial, or a unique factorization domain, or a u.f.d., if every non zero, non unit, can be expressed as a product of irreducible elements, and if whenever $x = \prod b_i = \prod c_j$, with all b_i, c_j irreducible, then there is the same number of b's and c's, and possibly after renumbering, each b_i is associate to the corresponding c_i.

Two elements of a ufd are relatively prime iff 1 is a gcd.

Fraction field: If R is a domain, its field of fractions is the ring ff(R) = {a/b: a,b, are in R, $b \neq 0$, and a/b = c/d if and only if ad = bc}. This is a field containing R, (actually it contains the isomorphic copy {a/1: a in R} of R), and is contained in every other field containing R. Hence a ring is a domain if and only if it is contained in some field.

Integral elements: If a ring F contains a domain R, we say an element x of F is integral over R, if x satisfies a monic polynomial with coefficients in R. A domain R is integrally closed, or integrally closed in its field of fractions, or normal, if the only elements x in ff(R) which are integral over R are elements of R itself.

Relations among these properties:

We will prove for domains, that strongly Euclidean implies Euclidean implies principal implies u.f.d. implies normal. None of these implications can be reversed.

Exercises: The following are like statements about integers and proved exactly the same way.

Pushups and free throws:

1) If P is a proper ideal, then R/P is a domain iff P is prime, and R/P is a field iff P is maximal. (E.g. (0) is maximal in a field.) Hence maximal ideals are prime.

2) A prime element of a domain is also irreducible. In a ufd, an element is prime if and only if it is irreducible.

3) An element x of a domain R, is irreducible iff (x) is maximal among all principal ideals of R, (but not necessarily maximal among all ideals).

4) Every Euclidean domain is a p.i.d. (Prove an ideal is generated by any "smallest" element.)

5) In a strongly Euclidean domain, every non zero non unit can be factored into a product of one or more irreducibles. (Induct on size.)

6) If k is a field, k[X] is strongly Euclidean where |f| = deg(f).

7) In a pid, a gcd of x,y is any generator of the ideal (x,y), hence in a pid, any gcd of x,y is a linear combination of x,y. Hence in a pid, x,y are rel. prime iff the ideal (x,y) = (1) = R, iff one can solve ax+by = 1, for a,b.

8) R is a domain iff the polynomial ring R[X] is a domain.

9) If $\{I_j\}$ is any linearly ordered indexed set of proper ideals in a ring R, i.e. if for any two ideals I_j and I_k, one is contained in the other, then their union is a proper ideal.

10) In a ufd, if x,y are relatively prime, and x divides ay, then x divides a. (Use 7.)

11) Any two elements x,y of a ufd, have a gcd given as follows. If the prime factorization of x is $\prod p_i^{r_i}$, and that of y is $\prod p_i^{s_i}$, then the gcd of x,y is the product $\prod p_i^{\min(r_i,s_i)}$.

12) All ufd's are normal. [Imitate the proof of the "rational root" theorem.]

Now we recall **Zorn's lemma:** In any partially ordered set S, a "chain" or

"linearly ordered subset" $\{x_i\}_I$, is a subset such that any two elements x_i, x_j are comparable, i.e. either $x_i \leq x_j$ or $x_j \leq x_i$.

Zorn's lemma says: If S is non empty, and each chain in S has an upper bound in S, then S contains some "maximal" elements, i.e. elements which admit no strictly larger comparable element.

We assume Zorn's lemma, which follows from the axiom of choice. [A proof is in the appendix to Lang, Algebra.]

Corollary: Every ring (with identity) contains maximal ideals.

proof: We have already checked that the union of a linearly ordered collection of proper ideals is a proper ideal, and thus an upper bound for the collection. We are finished by Zorn. **QED.**

Trickier stuff:

Rings which have unique factorization.

We assume all our rings are domains.

As in the exercise above, existence of factorization is easily proved in any strongly Euclidean domain by induction on size, but it also follows more abstractly, in any noetherian domain, as follows.

Definition: A partially ordered set satisfies the ascending chain condition, or ACC, if all strictly increasing sequences of elements are finite in length.

The next result is basic.

Lemma: The set of ideals in a ring R satisfies the ACC for the inclusion relation iff every ideal is finitely generated, i.e. iff R is noetherian.

proof: If some ideal I is not finitely generated, let a_1 be any element of I. Then (a_1) does not equal I, so there is some element in I - (a_1), say a_2. Then (a_1,a_2) is strictly larger than (a_1) but not equal to I, so we have a chain of two ideals (a_1) contained in (a_1,a_2). Then we can choose another element a_3 of I - (a_1,a_2) and then we have a strictly increasing chain of three ideals: (a_1) in (a_1,a_2) in (a_1,a_2,a_3). Continuing, we obtain after an infinite amount of time, or even a finite amount of time, if we work faster and faster, an infinite sequence of strictly increasing ideals, which contradicts the ACC.

Conversely, and here is the trickier part, if ACC does hold, we must show no infinite weakly increasing sequence of ideals, I_1, I_2, I_3,....., can be strictly increasing. The trick is to take the union I of all the ideals. As above, this union

is itself an ideal, hence finitely generated, say by $x_1,\ldots,x_n$. But then all the x_i are contained in some one of the ideals in the chain, say I_N. Then the remainder of the ideals in the sequence contain all the generators of the full union I, hence all the rest of the ideals are all equal to I and to I_N. So the infinite sequence of ideals is not strictly increasing. **QED.**

Exercise: In a noetherian ring R, any collection of ideals contains one which is maximal for that collection. In particular, by considering the set of all proper ideals, we get a new proof of the existence of maximal ideals of R, without using Zorn.

Lemma: In any noetherian domain R, e.g. any p.i.d., every non zero non unit can be expressed as a finite product of irreducible elements.
proof: Let x be any non zero non unit. First we claim x has an irreducible factor. If x is irreducible we are done. If not then x decomposes as a_1b_1, where neither a nor b is a unit, nor has an irreducible factor. Hence we have $b_1 = a_2b_2$, where again neither a_2 nor b_2 is a unit, nor has an irreducible factor. Continuing we obtain an infinite strictly increasing sequence of principal ideals (x) in (b_1) in (b_2) ....., which contradicts the noetherian hypothesis.

Now we claim x actually factors into irreducibles. If x is irreducible we are done. If not, then $x = a_1b_1$ where a_1 is irreducible. If b_1 is irreducible, we are done, and if not and a_2 is an irreducible factor of b_1, then we have $x = a_1a_2b_2$. If b_2 is ireducible we are done, and if not we can continue. Since the sequence of principal ideals (x), (a_1), (a_2),...is strictly increasing it must be finite, and hence we eventually have an irreducible factorization of x. **QED.**

Note: First, the two stage argument is essential, to keep control of the contradiction; i.e. a contradiction cannot be obtained by assuming only that x = ab, where a and b are not both irreducible. Second, unlike the case of a strongly Euclidean domain, there is no estimate here for the number of steps needed for the factorization.

Corollary: In any pid, every non zero, non unit, factors into a finite product of irreducibles.

So much for existence of irreducible factorizations. For uniqueness, we assume

the factors are not just irreducible, but prime.
Lemma: In a domain R, let $x = \prod x_i = \prod y_j$ where all x_i and y_j are *prime* elements. Then we claim there is the same number of x's as y's, and after renumbering, each x_i is associate to the corresponding y_i.
proof: Since x_1 divides the left side hence also the right, by definition of prime element (and induction), x_1 must divide some factor y_j on the right. But since all prime elements of a domain are irreducible, then x_1 is associate to y_j. renumbering the y's we may assume y_j is $y_1 = ux_1$, where u is a unit. Then after canceling x_1 on both sides, and replacing y_2 by its associate uy_2, we are done by induction on the number of factors occurring on the left. **QED.**

Lemma: In a pid R, every irreducible element is also prime.
proof: If x is irreducible, then the ideal (x) is maximal among all principal ideals. But since R is a pid, then (x) is a maximal ideal, hence also a prime ideal, so x is a prime element. **QED.**

Corollary: Every p.i.d. is a u.f.d.
proof: Since a pid is noetherian, this follows from the two previous lemmas. **QED.**

Remark: The corollary is not reversible, i.e. most ufd's are not principal. We have proved a noetherian ring in which irreducibles are prime is a ufd.

Dimension of a ring: The Krull dimension of a ring R is the maximal number n such that R contains a strict chain of length n+1 of proper prime ideals. Thus a field has Krull dimension zero, and the integers have Krull dimension one. A domain which is not a field has Krull dimension one iff every non trivial prime ideal is maximal, e.g. any pid.

Dedekind domains: A Dedekind domain is a one dimensional noetherian, normal domain. Pid's are Dedekind, but not vice versa.

Fact: R is a pid iff R is a one dimensional noetherian ufd. [Use ex.6, p.283, Dummitt-Foote.] There are noetherian ufd's of arbitrary finite dimension $k[X_1,...,X_n]$ (see Gauss' thm. below), and even non noetherian ufd's $k[X_1,...,X_n,....]$, of infinite dimension.

Remark: Gcd's do not exist in general except in ufd's, i.e. a noetherian domain is a ufd if and only if any two elements have a gcd (Sah, p.113).

Unique factorization of polynomials over factorial rings

Next we reproduce Gauss' famous argument for unique factorization of integral polynomials.

Proposition(Gauss): If R is a ufd, so is R[X].

Definition: A polynomial in R[X] is called primitive if 1 is a gcd of its coefficients.

Lemma(Gauss)**:** The product of two primitive polynomials is primitive.

proof: f is primitive iff for every prime element p of R. f remains non zero in (R/p)[X]. If f and g are primitive, both remain non zero in (R/P)[X]. Since p is a prime element of R, (R/P) is a domain, and so is (R/p)[X]. Thus fg is also non zero in (R/p)[X] for all primes p of R, so fg is also primitive. **QED.**

With this lemma, it is a straight forward but slightly tedious exercise to deduce that R[X] is a ufd. from the fact that K[X] is a ufd, where K is the fraction field of R.

Exercise: (Assume R a ufd.)

(i) If f is any polynomial in R[X], there is some d in R such that f/d is a primitive polynomial in R[X]; d = gcd of coefficients of f, is unique up to associates.

(ii) If f is a polynomial in K[X] not in R[X], there is some d in R such that df is a primitive polynomial in R[X], and d = lcm of denominators of coefficients in lowest terms of f, is unique up to associates.

(iii) The units of R[X] are precisely the units of R.

Lemma: If f is primitive in R[X] then f is irreducible in R[X] iff it is so in K[X].

proof: Asume f irred. in K[X], and that f = gh with g,h in R[X]. Then either g or h, say g, is a unit in K[X], hence a non zero element of K. But g belongs to R[X], so g is a non zero element of R. Since f is primitive, and h belongs to R[X], g is a unit in R, and f is irreducible in R[X].

If f is irred. in R[X], assume f = gh, with g,h in K[X], and neither is in R[X], then after multiplying out by the product of the lcm's of the lowest terms denominators

of g,h, we have a primitive polynomial on the right but not the left, a contradiction. If both g,h belong to R[X], by hypothesis one is a unit in R[X], hence also a unit in R and K and K[X], and we are done. So we may assume g is in R[X] and h is not. Then for appropriate d,e in R, as in the exercise above, we have f = gh = (d/e)(g/d)(eh), where f, (g/d), and (eh), are primitive in R[X]. Hence d and e are associates, and we have f = (g/e)(eh), where (g/e) and (eh) are both in R[X], hence one is a unit in R[X], i.e. in R. Thus either g or h is a unit in K, hence K[X], and f is also irreducible in K[X]. **QED.**

Lemma: If R is a ufd, then every primitive non zero non unit f in R[X] factors into irreducible elements of R[X].
proof: By hypothesis f has degree > 0. Since K[X] is a ufd, $f = \prod g_i$ where all gi are irreducible in K[X]. If all g_i belong to R[X] then they are primitive hence irreducible by the previous result and we are done. As before, some of them must belong to R[X] or else we find a non unit d of R such that df is a product oif primitive polynomials of R[X], a contradiction. In any event, we again find elements d,e of R such that $f = (d/e)\prod h_i$ where the h_i are primitive elements of R[X] each a non zero R multiple of the corresponding g_i , hence each h_i still irreducible in K[X]. Then each h_i, being primitive, is also irreducible in R[X], and we are done. **QED.**

Corollary: If R is a ufd, every non zero non unit f in R[X] factors into irreducible elements of R[X].
proof: If f is not primitive, write f = cg where g is primitive in R[X] and c is a non unit in R. Factor f as above into porimitive irreducibles, and factor c into irreducibles in R. These are still irreducible in R[X]. **QED.**

Lemma: If f is primitive in R[X], g any element of R[X], and if f divides g in K[X], then f already divides g in R[X]. In fact if g = fh, with h in K[X], then h is in R[X].
proof: Assume g = fh, with g in R[X], and h in K[X]. If h is not in R[X], as above there is some c in R, not a unit, with cg = f(ch), where f and ch are primitive in R[X], but cg is not, a contradiction. **QED.**

Corollary: An irreducible element of R[X] is prime if R is a ufd.
proof: Assume f is irreducible in R[X] and hence primitive, and that f divides gh,

with g,h in R[X]. Since K[X] is a ufd, and f is still irreducible in K[X], f is prime in K[X], so f divides either g or h in K[X]. Since g,h are in R[X], the previous result shows that f divides one of them in R[X]. Hence f is prime in R[X]. **QED.**

Corollary: If R is a ufd, so is R[X].
proof: We have shown R[X] has factorization into irreducibles, and that every irreducible in R[X] is prime. But factorization into primes is always unique.
QED.

Corolalry: If k is a field or ufd, then $k[X_1,...,X_n]$ is a ufd.
proof: By induction, since $k[X_1,...,X_n]$ is isomorphic to $k[X_1,...,X_{n-1}][X_n]$.

Corollary: If k is a field or ufd, then $k[X_1,...,X_n,....]$ (= polynomials in infinitely many variables) is a ufd.
proof: A given polynomial involves only a finite number of variables, and cannot factor into a product of factors which involve other variables. Hence a polynomial in $k[X_1,...,X_n]$ which is irreducible there is also irreducible in $k[X_1,...,X_n,....]$. This proves existence of irreducible factorizations. But these rings also have the same units, so a polynomila irreducible in $k[X_1,...,X_n,....]$ is also irreducible in $k[X_1,...,X_n]$. Thus if f is in $k[X_1,...,X_n]$, any two irreducible factorizations of it in $k[X_1,...,X_n,....]$ actually belong to $k[X_1,...,X_n]$, hence are equivalent there and also in $k[X_1,...,X_n,....]$. **QED.**

It is very useful to have some way to recognize irreducible polynomials.
Corollary: (Eisenstein): Assume R is a ufd, f in R[X] is a polynomial of positive degree n, and p is a prime element of R that divides every coefficient a_i of f with $i < n$, but not the leading coefficient a_n, and that $p^{\wedge}2$ does not divide the constant term a_0 of f. Then f is irreducible in K[X], where K = ff(R).
proof: If f were reducible over K , the factors would have degree at least one, and the factors can be chosen in R[X]. [I.e. if $f = c(f).f_0$, if f = gh, with g,h, in K[X], we have $f_0 = c(f)^{-1}g.h$, and we showed then that $f_0 = g_1h_1$ where g_1 and h_1 are the primitive versions of $c(f)^{-1}g$, and h. Then $f = c(f)f_0 = c(f)g_1h_1$, is a factorization of f in R[X].] Thus f = gh, where g,h are in R[X] and have degree ≥ 1.

If we reduce mod p, we get $[f] = [c]X^{\wedge}n = [g][h]$, in $(R/(p))[X]$, where

[c] is not [0]. Thus both [g] and [h] have non zero leading terms of degree < n. We claim both [g] and [h] have zero constant terms.

Although (R/p)[X] is not a ufd, X is a prime element of this domain since the quotient by X is R/p, a domain. Factorization by prime elements is unique in any domain, so the factors [g] and [h] of $[c]X^{\wedge n}$ must be associate to monomials of positive degree in X, hence neither has a constant term. Then gh = f has constant term divisible by $p^{\wedge 2}$, a contradiction. **QED.**

The previous criterion has a vast generalization as follows.

The valuation associated to a prime.

Let p be a prime in a ufd R, with fraction field K. define a function $v_p: K^* \to Z$ from non zero elements of K to the integers, as follows: if x = a/b with a,b in R, then write $a = cp^r$, and $b = dp^s$, where p does not divide either c or d, and define $v_p(x) = v_p(a/b) = v_p(a) - v_p(b) = r-s$. Thus $v_p(x)$ is "the number of times p divides x", i.e. the number of times it divides the numerator minus the number of times it divides the denominator. Thus an element x of K is in R iff $v_p(x) \geq 0$ for every prime p in R.

In geometry we think of the primes p as points, the elements x as functions, and the functions x with $v_p(x) < 0$ are the ones with poles at p, while those with $v_p(x) > 0$ have zeores at p. The absolute value of v_p gives the order of the zero or pole at p.

Note that the exponent i of X^i is nothing but the valuation $v_X(X^i) = i$, determined by the prime element X of R[X]. So we are in some sense looking at f as a polynomial in the two variables X and p.

Eisenstein-Dumas: Assume R is a ufd, and $f = \sum a_i X^i$ is a polynomial of degree n over R with $a_0 \neq 0$. Graph the integer lattice points $(i,v_p(a_i))$ in the plane ZxZ, and connect up the "first" and "last" points, $(0,v_p(a_0))$ and $(n,v_p(a_n))$, by a line segment L. If the following two conditions hold:
(i) all intermediate lattice points $(i,v_p(a_i))$ for $0<i<n$, lie on or above L, and **(ii)** $\gcd(n, v_p(a_n)-v_p(a_0)) = 1$,
then f is irreducible over K = ff(R) = fraction field of R.
proof of Dumas criterion:(see Van der Waerden, 2nd ed. vol.1, page 76).

Corollary:(Eisenstein). See statement above.

proof: Here we have a line segment L which has height ≤ 1 everywhere on the interval [0,n], and by hypothesis all intermediate points have height ≥ 1. Moreover, $v_p(a_0) = 1$, $v_p(a_n) = 0$, so gcd(n,-1)=1.

Corollary:(reverse Eisenstein): If p is prime and divides all a_i for i >0 but not a_0, and p^2 does not divide a_n, then f is irreducible over K.
proof: Here the line segment L goes from (0,0) to (n,1) instead of from (0,1) to (n,0), hence has the same slope, and all the intermediate lattice points are still above it.

Recall the usual root - factor theorem implies that a polynomial of degree ≤ 3 with no root over a field, is irreducible. Here is a related result.
Corollary: Let q be a prime integer, and consider f(X) = X^q -c, where c lies in a ufd R. If c has no qth root in R, then f is irreducible over K = ff(R).
proof: Since c has no qth root in R, there is some prime factor p of c such that p does not divide $v_p(c)$. Thus $\gcd(p,v_p(a_0)) = 1$. Since there are only the two extreme lattice points, and $v_p(a_q) = 0$, we are done.

Corollary: Irreducibility of polynomials in two variables:
If n, m are relatively prime, then $X^n - Y^m$ is irreducible in k[X,Y], where k is a field. E.g. X^2-Y^3 is irreducible in k[X,Y].
proof: Regard k[X,Y] as the polynomial ring k[Y][X] over the ufd k[Y], where Y is a prime element. Note $X^n - Y^m$ is primitive.

Corollary: If $a \neq 0,1$, then $Y^2 - X(X-1)(X-a)$ is irreducible in k[X,Y].
proof: Usual Eisenstein applies to this monic hence primitive polynomial, for the prime element X, in the ring k[X][Y].

8000 Day Three: Brief course on modules over a commutative ring

Next we define the concept of an "action" of a (commutative) ring R on an abelian group. Then all the constructions made for abelian groups generalize in exactly the same way.

If M is an abelian group, an R module structure on M is a ring map s:R--->End(M) = {group homomorphisms M--->M}, where End(M) is a (usually non commutative) ring with composition as multiplication, hence the identity map acts as the element 1.

Using the map s, we can "multiply" elements of M by elements of R, i.e. by definition we set rx = (s(r))(x), and the usual properties hold, (ab)x = a(bx), (a+b)x = ax +bx, 1x = x, and a(x+y) = ax+ay.

We define $\mathrm{End}_R(M)$ as the subring of End(M) consisting of those group homomorphisms which commute with multiplication by all elements of R. Note: $\mathrm{End}_Z(M) = \mathrm{End}(M)$, but for other rings R, $\mathrm{End}_R(M)$ is usually smaller than End(M). The homomorphisms in $\mathrm{End}_R(M)$ are called R module maps, and similarly for the subset $\mathrm{Hom}_R(N,M)$ of Hom(N,M).

An R homomorphism with an R module inverse is called an R isomorphism.

If R--->End(M) is an R module structure on M, the kernel of the map R--->End(M) is the ideal ann(M) = {those elements r in R such that rx = 0 for all x in M}. An R module structure is called faithful if ann(M) = {0}. For any R module structure, M has a natural induced faithful R/ann(M) module structure.

Thus M has an R module structure iff some quotient R/I is isomorphic to a subring of End(M), and M has a faithful R module structure if and only if R itself is isomorphic to a subring of End(M).

A subgroup N of the R module M is a submodule iff N is closed under multiplication by elements of R.

If f:M-->N is an R module map, the subset of elements x of M such that f(x) = 0, is a submodule of M called the kernel of f. The submodule of N of all elements of form f(x) for x in M, is called the image of f.

Ex. A finitely generated abelian group cannot have a Q module structure.

Ex. An ideal of R is the same as a submodule of R.

A submodule is generated by a subset of elements $\{x_i\}$ of M, if each

element of M is an R linear combination of some finite subset of the $\{x_i\}$. If the same finite subset of elements $\{x_i\}$ can be used to generate every element of M, then M is finitely generated.

A module is noetherian if every submodule is finitely generated. A ring is noetherian if and only if it is noetherian as a module. A module is cyclic if it has one generator. Thus an ideal is cyclic iff it is principal. A cyclic module is isomorphic to R/I for some ideal I. In a p.i.d. every non zero ideal I is isomorphic to R as modules.

Submodules and Quotient modules

If N is a submodule of M, the quotient group M/N has a natural structure of R module such that M-->M/N is a module map with kernel N. A homomorphism f:M-->P with N contained in the kernel of f, factors uniquely as M-->M/N-->P.

Products and direct sums of families of modules

If $\{M_i\}_I$ is an indexed collection of R modules, the product module $\prod_I M_i$ is the family of functions s from I to the union of the M_i such that s(i) belongs to M_i for every i in I.

An R module map N-->$\prod_I M_i$ is equivalent to an indexed family of R module maps N-->M_i.

The direct sum of an indexed family $\{M_i\}_I$ of modules is the submodule $\sum_I M_i$ of $\prod_I M_i$ consisting of those functions f whose value is zero at all but a finite number of elements i of I. Thus for a finite index set I, the product and sum are the same.

We denote the product (or sum) of n copies of R by R^n. Any module isomorphic to R^n is called a free R module of rank n. We also denote by M^n the sum (or product) of n copies of M.

An R module map $\sum_I M_i$ -->N is equivalent to an indexed family of R module maps M_i-->N.

For each element x of M, there is a unique R module map f:R-->M such

that f(1) = x. Consequently, $\mathrm{Hom}_R(R^n, M) \approx M^n$.

An R module map f:R^n-->R^m is defined by a unique m by n matrix of entries of R, whose jth column is the vector f(ej) where $e_j = (0,...,1,...,0)$, and the 1 is in the jth position.

A sequence of R homomorphisms is called <u>exact</u> iff the image of each map equals the kernel of the next map.

Exercises

1) A submodule of a ring R is the same thing as an ideal.

2) If 0--->A--->B--->C--->0 is an exact sequence of R module maps, then B is noetherian iff both A and C are noetherian. (Hint: A,C fin. gen. implies B is also.)

3) If R is a noetherian ring, then R^n is a noetherian R module.

4) If R is noetherian and M a fin gen R module, then M is noetherian.

Hilbert "basis" theorem.

The next result gives lots of noetherian rings. The concept of R module makes the proof slightly shorter, so we placed it here.

Proposition(Hilbert): If R is noetherian, so is R[X].

proof: If I is any ideal of S = R[X] we want to find a finite number of generators for I. Consider the set J of all leading coefficients of elements of I, and check that J is an ideal of R hence finitekly generated say by $a_1,...,a_n$. Then for i = 1,..,n, choose an element f_i of I that has leading coefficient equal to a_i. Let r be the maximum of the degrees of the polynomials $f_1,...f_n$. If f is any polynomial in I of degree $\geq$ r, by multiplying the f_i by suitable poiwers of x, we obtain polynomials g_i of the same degree as f, and whose leading coefficients generate the ideal of all leading coefficients of elements of I. Hence there is an R linear combination of the g_i which ahs the same degree and the same leading coefficient as does f. This linear combination is also an R[X] linear combination of the f_i. Thus we have for some polynomial coefficients h_i, that $\sum h_i f_i$ - f has lower degree than f.

Repeating this we eventually can lower the degree of f until it is less than r. I.e. for some polynomial coefficients k_i we get that $\sum k_i f_i$ - f belongs to I and

also to S(r) = the module of polynomials in R[X] of degree less than r. Since the module S(r) is generated over R by $1,X,....,X^{r-1}$, it is finitely generated over R, hence noetherian as R module, hence certainly also as R[X] module. Thus I intersect S(r) is a finitely generated R[X] module, so we can choose a finite number of R[X] generators $t_1,...,t_m$ for it. Then $\sum k_i f_i - f = \sum -w_i t_i$ for some polynomials w_i, and $f = \sum k_i f_i + \sum w_i t_i$. Hence the finite set $\{k_i, t_j\}$ generates I over R[X]. **QED.**

Diagonalization of matrices over a pid

Next we observe that the pid property is exactly the property of the integers needed to do the key step of the classification of finitely generated abelian groups.

Proposition: We can diagonalize a matrix over any pid, by invertible matrix operations, but not ones obtained from elementary row and column operations. I.e. if M is an m by n matrix, with entries in a pid R, there exist *invertible* (but not *elementary*) matrices A,B over R, such that AMB is diagonal, in the sense that all entries x_{ij}, with $i \neq j$, are zero.

proof: Using the same procedure as with integer matrices, it suffices by induction to show that we can arrange for the upper left entry of M to divide all the other entries in the first row and column. We get to use the elementary row and column operations, but we will supplement them by an additional invertible matrix multiplication which does not arise from a product of elementary matrices.

Recall the key step was to show that we can replace a first row of M containing [a b * * * .....], where a does not divide b, by [d c * * * .....] where d is a proper divisor of a. By interchanging columns, if a fails to divide any entry in the first row, we can also replace a by a proper divisor. Similarly, if a fails to divide any entry in the first column we can replace a by a proper divisor.

Since a has only a finite number of proper divisors in a ufd, hence in any pid, this process can only be repeated a finite number of times. Hence eventually, the upper left entry will divide all other entries in both the first row and column, and can be used to replace all other entries by zeroes. Then induction allows the matrix to be reduced to diagonal form.

Now to accomplish this, since R is a pid, make the key replacement by an invertible matrix operation as follows. If a does not divide b, then gcd(a,b) = d has strictly fewer prime factors than a, and d can be written as a linear

combination d = ax+by, where after dividing through by d, we see that the gcd of x,y is 1. Hence we can write 1 = zx + wy. This lets us construct a matrix B with first two rows [x -w 0 0 0 .... 0] , and [y u 0 0 0 .....0]. This matrix multiplies our original one from the right to yield upper left entry ax+by = d = gcd(a,b).

Moreover this matrix can be completed to an invertible one B, since the 2 by 2 determinant in the upper left corner is 1. I.e,. we just put zeroes in all the rest of the first two column entries, and put an identity matrix in the bottom right corner. **QED.**

Corollary: A finitely generated module N over any p.i.d. R, is isomorphic to a product of cyclic modules R^r x R/(x_1) x ....x R/(x_s), where no x_i is a unit or zero, and each x_i divides x_{i+1}. Moreover, the ideals (x_i) are uniquely determined by the isomorphism class of N, as well as the integers r and s.

proof sketch: As before, if N has m generators, we map R^m onto N, and since R is noetherian, the kernel of this map is finitely generated, so we can map some R^n onto this kernel, thus realizing N as the cokernel of a map f:R^n --->R^m, hence as the cokernel of a matrix M. Then diagonalizing the matrix by invertible operations as above, does not change the isomorphism class of the kernel and cokernel. But for a diagonal m by n matrix with diagonal entries z_1,...,z_m, dividing each other, (some of the early ones possibly equal to 1, and some of the last ones possibly equal to 0), the cokernel is easily shown to be isomorphic to the product R/(z_1) x .....x R/(z_m). Then we delete the factors at the beginning having z = 1, since those cyclic quotients R/(z) are {0}. Then put the factors from the end, with z = 0, at the beginning, since they are = R. Then letting the x_i's be the z's that are different from 1 and 0, we have our decomposition. The uniqueness of the x_i is no easier, but no harder, than before. For uniqueness of the rank r, see below. **QED.**

First we prove the vector space case, since this proof is sometimes omitted in elementary courses.

Proposition: If K is a field, and $K^n \approx K^m$, then n = m.

proof: An isomorphism K^n --> K^m is represented by an m by n invertible matrix of entries in K. Since K is a field, it is also a pid, so we can diagonalize this matrix by invertible matrix multiplication, and obtain an invertible diagonal matrix. Such a matrix must be square, so n=m. **QED.**

Now assume that N is an R module and I is an ideal of R. Then define IN as the submodule of N generated by all products rx where r is in I and x is in N. This equals all R linear combinations of form $\sum a_i x_i$ where the a_i are in I and the x_i are in N.

Exercise: For a product of R modules, $N = N_1 \times \dots \times N_S$, we have $IN \approx IN_1 \times \dots \times IN_S$.

Cor: If I is a maximal ideal of R, then $R^n/IR^n \approx (R/I) \times \dots \times (R/I) \approx K \times \dots \times K$, where K is the quotient field R/I.

Cor: If $R^n \approx R^m$, for any ring R, then n = m. Hence the rank r of a finitely generated module over a pid is well defined.
proof: If $R^n \approx R^m$ then $K^n \approx K^m$, so by vector space theory n = m. **QED.**

Note: Over a Euclidean domain such as k[X], we can carry out the diagonalization, hence the decomposition of a finitely generated module more constructively, as we did for integers. I.e. in that case the gcd of two elements can be obtained by repeated subtraction, following Euclid. This will be used in the next chapter to find canonical forms of matrices and hence of linear maps of finite dimensional vector spaces.

APPENDIX:
A glimpse of the geometry of rings
If R is a domain, and P a prime ideal, define the "localization" of R at P to be the ring R_P of formal quotients a/b, where a,b are in R, b is not in P, and a/b = c/d iff ad=bc as usual. Then a one dimensional noetherian ufd is a pid, so if R is a Dedekind domain then R_P is a pid for every prime ideal P. I.e. a Dedekind domain R is <u>locally</u> principal.

Note that a ring R is itself an R module, and hence the concept of a sub R module of R, i.e. an ideal, has interest. If R is not a pid, then ideals of R may require several generators. The theory of factorization of individual elements of R deals only with principal ideals. E.g. in C[X,Y] principal ideals (f) correspond to plane curves f=0, while maximal ideals (X-a, X-b), requiring 2 generators,

correspond to points (a,b). It takes an argument to prove all maximal ideals have this form.

"Weak nullstellensatz"

Theorem: The correspondence taking $p = (p_1,...,p_n)$ to $(T_1-p_1,...,T_n-p_n)$ is one to one between points of $C^{\wedge n}$ and maximal ideals of $C[T_1,...,T_n]$.

Proof: The case n = 1 is the definition of algebraically closed. So assume $n \geq 2$. We will use induction. By substituting $(T_i-p_i) + p_i$ for T_i and expanding, we can write every polynomial in the T_i as a polynomial in the T_i-p_i. This shows that evaluation at p, is a surjection onto k with kernel the ideal $(T_1-p_1,....,T_n-p_n) = (T-p)$. This ideal is thus maximal and so the correspondence above is well defined from points to maximal ideals. It is also injective since if $u \neq p$, say $u_i \neq p_i$, then T_i-u_i does not belong to the kernel of evaluation at p, hence the ideals (T-u) and (T-p) are different.

Thus the main point is surjectivity. Let m in k[T] be a maximal ideal. It suffices to show for all i, that m contains an element of form T_i-p_i since then m contains $(T_1-p_1,...,T_n-p_n)$. Since both ideals are maximal they are then equal. So fix i, say i = 1, and consider the map $C[T_1]\text{—>}C[T_1,...,T_n]/m$, and its kernel m in $C[T_1]$. If the kernel were (0), then since C[T]/m is a field, the fraction field $C(T_1)$ would embed in C[T]/m. But C[T]/m is generated as C vector space by the monomials in the T_j's hence has countable vector dimension over C. On the other hand we claim the set $\{1/(T_1-p_j)\}$ for all p_j in C, is independent, and uncountable, a contradiction.

To check this write $\sum_j c_j/(T_1-p_j) = 0$ where the $\{p_j\}$ are finitely many distinct elements of C, and $\{c_j\}$ are any elements of C, and multiply out the denominators, i.e. multiply by $\prod_j (T_1-p_j)$. We get $\sum_j c_j (\prod_{k\neq j} (T_1-p_k))= 0$. Setting $T_1 = p_l$, we get $c_l(\prod_{k\neq l} (p_l-p_k)) = 0$. Since $\prod_{k\neq l} (p_l-p_k) \neq 0$, we must have $c_l = 0$ for all l. Hence the set $\{1/(T_1-p_j), p_j \text{ in } C\}$ is indeed independent over C.

Now that the kernel of $C[T_1]\text{—>}C[T_1,...,T_n]/m$, is not (0), it must equal some prime ideal of form $(f(T_1))$ in $C[T_1]$ where $f(T_1)$ is irreducible. Since C is algebraically closed, the only irreducible polynomials are linear so f may be assumed to be of form T_1-p_1 for some p_1 in C, as desired. **QED.**

Fact: If K is a subfield of C, containing Q and of finite dimension as a vector

space over Q, define O, the ring of integers in K, to be the set of all those elements of K which are integral over Z. Then O is a finite Z module, hence a finitely generated abelian group, and in fact a Dedekind domain, i.e. a normal domain of Krull dimension one. These rings are of great importance in algebraic number theory. E.g. if they were all ufds, which they are not, Fermat's last theorem would have been proved a lot sooner.

Assume R is a noetherian domain.
Definition: A polynomial is monic if it has leading coefficient 1.
An element of the fraction field K of a domain R is integral over R if it is the root of a monic polynomial in R[X].
A domain R is normal, or integrally closed, if the only elements of K that are integral over R are elements of R.

Exercise1: Any ufd is normal. [hint: look at the proof of the "rational root" theorem from precalculus.]
Exercise2: In a ufd R, prove all "minimal" prime ideals are principal. I.e. if the only prime ideal contained in P is {0}, then P is principal.
Exercise3,4,5: If R is a domain in which all non zero prime ideals are minimal, prove R is a pid. (see DF, problem 6, parts a,b,c, page 283.)

Fact: If R is a normal noetherian domain, then for all minimal primes P of R, the localization R_P is a pid. Note this is weaker than the analogous property for a ufd. Both facts allow us to define the order of the zero or pole of a rational function along a subvariety of codimension one.
Definition: If R is a domain, the fraction field K, of R, is defined as the set of all formal quotients {x/y: x,y are in R, and $y \neq 0$}, subject to the equivalence relation, x/y = a/b iff xb=ay. This is a field containing the isomorphic copy {x/1: x is in R} of R.
Definition: If R is a domain and P a prime ideal, the "partial" fraction ring R_P, called "the localization of R at P", is the following subring of K.
R_P = {x/y in K such that y is not in P}. Since P is prime, the product of two such fractions is another such fraction.

Exercise6: Prove that the ideal PR_P generated by P in R_P is maximal, and that all elements of R_P not in this ideal are units. Conclude that there is only this one

maximal ideal in R_P. [R_P is called a "local ring".]

Example: If k is a field, and R = k[X,Y] is the ring of polynomial functions on the affine plane k^2, then (X,Y) = P is a maximal, hence prime, consisting of polynomial functions vanishing at the point (0,0). Then R_P is the ring of those rational functions which are defined at (0,0), i.e. whose denominators do not vanish at (0,0).

Exercise7: If R is normal, P prime, prove R_P also normal.
Exercise 8: If R is ufd, P prime, prove R_P also ufd.
Exercise 9-10: If k = Z/2Z, find all k[X] module structures on k^3 up to isomorphism (which extend the usual k module structure).

Geometry of normal, and factorial rings.
A ring is <u>factorial</u> if it is a ufd, and <u>locally factorial</u> if all R_P are ufd's.

Assume k is algebraically closed, k = the complex numbers C. Let $R = k[T_1,...,T_r]/I$, $S = k[T_1,...,T_s]/J$, where I,J are prime ideals. Let X = Z(I) be the common zero locus in k^r of the polynomials in I, and Y = Z(J) in k^s.
<u>Assume</u> there is a dense polynomial map f:X--->Y inducing via pullback, an <u>injective</u> ring map of polynomial functions S--->R, and an <u>isomorphism</u> on rational functions ff(S)--->ff(R).
1. Then X,Y are <u>irreducible</u> algebraic sets, and there is a <u>dense open set</u> U in Y such that the <u>restriction</u> $f:f^{-1}(U)$--->U is an <u>isomorphism</u>.

(the next two parts are both called Zariski's "main theorem")
2. Moreover, if S is a <u>normal</u> ring, then we can choose U such that for all y in Y-U, $f^{-1}(y)$ is <u>either empty or of dimension ≥ 1</u>. In particular, <u>if f has all finite fibers, then f is an open embedding of X into Y</u>, hence <u>a bijective polynomial map to a normal variety is an isomorphism.</u>

3. If S is <u>locally factorial</u>, then for every irreducible component E of the closed set $X-f^{-1}(U)$ where f is not an isomorphism, <u>E has codimension = one in X</u>, while <u>f(E) has closure in Y of codimension ≥ 2</u>.

A variety X = Z(I) is called normal or locally factorial if its ring R is such.

Definition: A singular point of an algebraic variety X is a point near which it does not "look like a manifold".
If $X = Z(I)$, and $R = k[T_1,...,T_r]/I$, as above, define dim(X) = Krull dimension of R. If X is n dimensional, and P the maximal ideal of a point x, then X is singular at x if and only if it takes more than n generators to generate PR_P.

Fact: If R is the ring of polynomial functions on the affine variety X as above, and x is a non singular point with maximal ideal P, the local ring R_P is always a ufd. I.e. all non singular varieties are locally factorial.

It was Zariski who discovered the geometric meaning of normality, and made it part of a general program of studying varieties.

Theorem: If I = (g) is a principal prime ideal in $k[T_1,...,T_S]$, and Y = the zero locus of g, then:
1) Y is normal if and only if the singular locus of Y has codimension ≥ 2 in Y.

2) Y is locally factorial if (but not only if) the singular locus has codimension ≥ 4 in Y. (Grothendieck)

3) On a normal variety, a rational function that is regular off a set of codimension ≥ 2, is actually globally regular (Hartogs, or Riemann extension property).

4) Removing the singular locus of a normal variety over C cannot disconnect the variety, not even locally in the complex topology.