Contents

1 Groups

1.1 Recap

We recall basic concepts from Groups (See level 7), such as

- Groups represent symmetries, and this is essentially what an action is, in the sense ofD_{2n} acts on n vertices and can therefore be thought of as a subgroup of S_n in this way and matrix groups are subgroups of $Sym(\mathbb{R}^n)$.

- A homomorphism, typically denoted ϕ, is a structure preserving map from a group to another group. It is called an isomorphism if it is a bijection.

- The first isomorphism theorem says $G/\ker(\phi) \cong \mathrm{Im}(\phi)$

- The order of an element divides the order of a group, for all x if G acts on something and G is finite then

$$|Orb(x)||Stab_G(x)| = |G|$$

- Cauchy's theorem says if p is prime and p divides $|G|$ then G has an element of order p.

- Groups can act on themselves by the left regular action or by conjugation. It follows that for every group G it is isomorphic to a subgroup of $Sym(G)$.

[Lecture 1 ends]

Example: The exp homomorphism from $(\mathbb{C}, +)$ to $(\mathbb{C} \setminus 0, *)$ has kernel $2ni\pi$ for integers n. So the isomorphism theorem implies

$$(\mathbb{C}\backslash 0,\ *) \cong (\mathbb{C},\ +)/2\pi i\mathbb{Z}$$

1.2 Isomorphism theorems

Theorem. (Second isomorphism theorem)

Let H be a subgroup of G and let K be a normal subgroup of G. Then $HK = \{hk \mid h \in H,\ k \in K\}$ is a subgroup of G and $H \cap K$ is normal in H and there is an isomorphism between HK/K and $H/(H \cap K)$

Proof. Lets prove HK is a subgroup. It contains the identity so we just need to apply the subgroup test. Set $x = hk$ and $y = h'k'$, then

$$yx^{-1} = h'k'k^{-1}h^{-1} = h'h^{-1}hk'k^{-1}h^{-1} = h'h^{-1}k''$$

by normality of K, so it is in HK, so HK is a subgroup. We will finish the proof next lexture. Luckily those readding this don't have to wait for the next lecture.

[Lecture 2 ends]

We need to show that $H \cap K$ is normal in H. This is just the kernel of the restriction of the homomorphism $H : G/K$ to H which is still a homomorphism. The kernel is exactly $H \cap K$. Also K is normal in HK (since it is normal in G). Now we apply the first isomorphism theorem to the homomorphism $H : G/K$ restricted to H. The image is $H/H \cap K$ but also the set of k-cosets in G that are representable by elements of H, which is just HK/K.

□

Proposition. (Correspondence)

Let $\phi : G \to G/K$, then there is a bijection between subgroups of G that contain K and subgroups of G/K, and the bijection is as follows:

Suppose K is contained in L which is in G, then K is normal in L, and L/K is a group and it is contained in G/K.

Also, we send A contained in G/K to the set of g such that gk is an element in A for some k in K.

Essentially given a subgroup of G/K we look at its pre-image and given a subgroup of G we look at its image.

Furthermore, if L is normal in G then it follows that L/K is normal in G/K $(gK)(LK)(gK)^{-1} = gLg^{-1}K = LK$ by normality of L and K.

Theorem. (Third isomorphism theorem)

Let K be a subgroup of L and L be a subgroup of G and suppose K and L are both normal subgroups of G. Then there is an isomorphism from (G/K)/(L/K) to G/L.

Proof. Define a map $\phi : G/K \to G/L$ sending the coset gK to the coset gL. If gK and g'K are two names for the same coset, then $g'g^{-1} \leq K \leq L$ so g'L=gL so this is well defined. It is clear that this is a homomorphism. The kernel is the g's such that gL=L, ie g is in L, so g is in L and G/K. But this intersection is exactly L/K. So the result follows by the first isomorphism theorem.

□

1.3 Simple groups

Proposition. Let G be abelian. Then G is simple if and only if G is isomorphic to a cyclic group of prime order.

Proof. The if part is simple because if it has prime order it has no non-trivial subgroups and therefore no non-trivial normal subgroups.

Otherwise (if G is abelian but with non-prime order we want to show it is not simple), we can build a subgroup with size a prime factor by Cauchy's theorem, and this is normal because G is abelian. So this proves the other direction for finite G.

If G is infinite, then either it is generated by a single element, in which case we can take $2\mathbb{Z}$ in $\mathbb{Z}$, or if it has a single generator we just take the subgroup generated by that, which is a non-trivial normal subgroup.

□

Theorem. Let G be a finite group. Then there exist a sequence subgroups H_n starting from G being H_1 such that each is normal in the previous one and eventually we get to the trivial group, and furthermore the quotient group H_i/H_{i+1} is simple.

Proof. If G is simple then we just have to take H_2 to be the identity and there's not much else we can do so we're done. Otherwise, let H_2 be a proper normal subgroup of maximal order in G.

We will show that G/H_2 is simple as we can then proceed inductively. If not, consider $\pi : G \to G/H_2$ with non-trivial kernel. Consider K to be the pre-image of N under the natural homomorphism G to G/H. Then K is a subgroup of G, and K is normal in G because

$$\pi(gkg^{-1}) = (gkg^{-1})H = (gH)(kH)(gH)^{-1} \in N$$

by normality of H and normality of N, and therefore K is a normal subgroup of G containing H, but if K is not H or G this contradicts H being the largest subgroup. Now given any coset gH, if it is in N that is equivalent to g being in K so gH is in K/H so N in G/H and K/H in G/H are the same set. But correspondence has already given us H and G as subgroups that contain H, and so it follows that this contradicts the assumption of H being the largest normal subgroup of G.

□

[Lecture 3 ends]

A group G can be thought of as a permutation representation. If there is a set X consider a homomorphism G to Sym(X).

If we have a homomorphism F from G to Sym(X) then we can think of an action as a function (g,x) to F(g).x.

Proposition. There is a bijection between homomorphisms G to Sym(X) and actions of G on X.

Proof. The idea is if we have an action of G on X we can think of it as a homomorphism between G and sym(X) and same the other way around, immediately from the definitions.

□

Notation:

If G acts on X we say G^X is the corresponding image in Sym(X) and G_X is the kernel which is a normal subgroup of G.

Example. Let H be a subgroup of G, then G acts on the set of left cosets of H by $g(g_1H) = (gg_1)H$.

If g lies in the kernel then this means that $gg_1H = g_1H$ for all $g_1 \in G$ so $g_1^{-1}gg_1 \in H$. In particular, the kernel is the intersection of all conjugates of H in G by supposing $g_1^{-1}gg_1 \in H$ is true for all g_1 and reversing the argument. Since this is a kernel, this means that for any subgroup H, the intersection of all its conjugates is normal.

Proposition. Let G be finite and H in G of index n. Then there exists a normal subgroup K in G contained in H such that G/K is isomorphic to a subgroup of S_n

Proof. Let G act on Sym(G/H), then K is its kernel which is contained in this and thus normal in G and contained in H.

□

Corollary. If G is not abelian and simple and H is a proper subgroup, then G is isomorphic to a subgroup of A_n and $n \geq 5$

Proof. Look at the kernel of the natural action G to G/H. Then by simplicity this is either the identity of G itself. This is the identity unless if H is G itself, so G is isomorphic to the image of this homomorphism which is in the symmetric group. But the sign of everything in G has to be 1 otherwise the kernel of this homomorphism is a non-trivial normal

subgroup, so the only possible way we are not done is if the kernel of the sign homomorphism in G is the identity. This is impossible as otherwise G would have order at most 2 and therefore not be abelian.

The $n \geq 5$ part comes from directly verifying that S_1, S_2, S_3, S_4 has no non-abelian simple subgroups. Note: S_4 is because any simple subgroup would have to not have the kernel of the sign homomorphism in it and thus must be in A_4 or C_2 but if not abelian it is in A_4 and it is not A_4 itself because A_4 is not simple due to having D_6 but by lagrange D_6 is the only non-abelian subgroup of A_4 so we are out of possibilities.

□

[Lecture 4 ends]

Observation: If we fix g in G, then $h \to ghg^{-1}$ is a permutation of G and it is a homomorphism. In fact, it is an isomorphism from G to itself.

Definition. A permutation of G is an automorphism if it is also a homomorphism (Or also an isomorphism)

Observation: The set of all automorphisms of any group G which we call Aut(G) with composition forms a group. It is a subgroup of Sym(G).

Example. The group $Aut\left(\mathbb{R}^2\right)$ contains $GL_2(\mathbb{R})$ as a subgroup. To show that this inclusion is a strict inclusion is a set-theoretic monster.

Definition. Let H be a subgroup of G. Then the normalizer of H in G written as $N_G(H)$ is the set of g in G such that $gHg^{-1} = H$. Then by definition, H is normal in $N_G(H)$. In fact this is the largest subgroup of G inside which H is normal.

Recall that a conjugacy class in S_n consists of the set of all elements of a fixed cycle type.

Theorem. Let $n \geq 5$, then A_n is simple.

Proof. Step 1 is to show that A_n is generated by 3-cycles. Step 2 is to show that any normal subgroup H in A_n that contains a 3-cycle contains all of them and thus is the whole of A_n. Step 3 is to show that any normal subgroup H in A_n is either the identity or contains a 3-cycle and is thus either the identity or the whole of A_n.

Proof of step 1:

Any g in A_n is a product of evenly many transpositions by definition. Consider pairs of transpositions like (a b)(c d), since any permutation is a product of such pairs.

One possibility: We have something like (a b)(a b), but this is not very interesting as it is the identity.

Another possibility: They share one entry, so we have (a b)(b c). Multiplying this out it is (a b c) which is a 3-cycle so we're good.

Final possibility: If they are distinct, then we have (a b)(c d)=(a c b)(a c d) by direct calculation. This is a product of 3-cycles, so we are done with step 1 as we can write the whole alternating group as a product of 3-cycles.

Proof of step 2:

Note that a normal subgroup is a union of conjugacy classes, and any two 3-cycles are conjugate in the symmetric group so in the symmetric group this statement is trivial. For any two 3-cycles S and S' there is a σ in the symmetric group such that $S = \sigma S' \sigma^{-1}$. Observe that if $n \geq 5$ then these only affect 3 elements so there are 2 elements disjointfrom them such that we can swap them and call that τ. Therefore if σ is odd we have S conjugate to S' in A_n by $\sigma\tau$. So done.

We are out of time so we will do step 3 next time.

[Lecture 5 ends]

Proof of step 3:

There are several cases. Here when I say 1,2,...,anything the argument is the same for $a_1, a_2, \ldots$ and I'm just writing 1,2,... to simplify.

Suppose H contains an element of the form $\sigma \coloneqq (1\ 2\ \ldots\ r)T$ with r at least 4 and T a permutation disjoint from this.

By normality of H any conjugate of this is in H. Let $\delta = (1\ 2\ 3)$ then conjugate by δ. So we have

$\delta^{-1}\sigma\delta$ in H. Then we have that T commutes with δ by disjointness. We can expand $\sigma^{-1}\delta^{-1}\sigma\delta$ which is known to also be in H.

$(r \ldots 3\ 2\ 1)(1\ 3\ 2)(1\ 2\ 3 \ldots r)(1\ 2\ 3)$ and the T's cancel. Now 1 stays where it is, 2 goes to 3, 3 goes to r, r goes to 2, and anything else goes to itself so we have a 3-cycle (2 3 r).

Therefore we reduce to the case that all cycles are at most 3 in size.

Now suppose H contains an element $\sigma \coloneqq (1\ 2\ 3)(4\ 5\ 6)T$ with T disjoint from 1,2,3,4,5,6. Then conjugating by $\delta \coloneqq (1\ 2\ 4)$ then since the T's are disjoint we have by algebra that $\sigma^{-1}\delta^{-1}\sigma\delta$ is a 5-cycle and we can apply the first case to get a 3-cycle.

Therefore we reduce to the case that there is a single 3-cycle and a bunch of transpositions, or just a bunch of transpositions.

Now suppose H contains an element $\sigma \coloneqq (1\ 2\ 3)\,T$ with T of order 2 disjoint from 1,2,3. Now here just square it then we know H contains a 3-cycle.

Now we have reduced to the case that we have a bunch of transpositions and that is it.

Now suppose H contains an element $\sigma \coloneqq (1\ 2)\,(3\ 4)\,T$ with T of order 2 disjoint from 1, 2, 3, 4. Then we can do the computation and conjugate trick to get to get $\sigma^{-1}\delta^{-1}\sigma\delta = (1\ 4)\,(2\ 3)$. Now conjugate this by (1 2 5) then we get $(1\ 3)\,(4\ 5)$. Now the product of $(1\ 4)\,(2\ 3)$ and $(1\ 3)\,(4\ 5)$ is (1 2 3 4 5) which is covered by the first case.

□

1.4 Sylow theorems

Theorem. Let p be a prime and G have order p^n with $n \geq 1$, then the center of G is non-trivial.

Proof. Let G act on itself by conjugation. The center is the set of all size 1 orbits (conjugacy classes). The size of G is p^n for some n, and this is the sum of all the orbits, and by the orbit stabilizer theorem the size of these orbits divide p^n so if they are not 1 they are divisible by p. Therefore the sum of the size of all conjugacy classes greater than size 1 is divisible by p and less than p^n so there are at least p conjugacy classes of size 1.

□

Proposition. If G is a group and Z[G] is the center then if $G/Z[G]$ is cyclic then G is abelian

Proof. By cyclicness there is a single coset xZ[G] that generates the quotient group. Therefore every coset has the form $x^m Z[G]$ for some m. This means every g in G can be written as $g = x^m z$ for some integer m and z in Z[G]. If $g = x^m z,\ h = x^n z'$ then we use the definition of the center to get

$$gh = x^m z x^n z' = x^{n+m} z z' = \cdots = x^n z'^{x^m} z = hg$$

Since any 2 of $x^m,\ z,\ x^n, z'$ commute.

□

Theorem. Let p be a prime and G a group of order p^2, then G is abelian.

Proof. This is immediate from the previous 2 propositions: $G/Z[G]$ has order 1 or p by the theorem 2 propositions ago which is cyclic so G is abelian by the previous proposition.

□

Definition. Let p be a prime and G have order p^n with $n \geq 1$, then we say G is a p-group.

Theorem. Let G be a p-group of size p^n, then G has a subgroup of size p^k for every 0<k<n.

Proof. The cases n=1, n=2 are clear by Cauchy's theorem. Now go by induction on n. If n>1 then we are good for k=0, 1, n trivially. Now let x be an element of the center of G not equal to the identity. Then the order of x is some power of p. Now some element y in <x> has order p and then <y> has order p and is normal due to being in the center. So we have a normal subgroup of order p. Now we take a quotient by this and apply the induction hypothesis and the result follows. A subgroup of order p^c in G/<y> corresponds to a subgroup of order p^{c+1} in G.

□

Remark. By the chinese remainder theorem if n and m are coprime then $C_n \times C_m \cong C_{nm}$.

[Lecture 6 ends]

Definition. Let G be a finite group of size $p^a m$ where p is prime and does not divide m. Then we define a Sylow p-subgroup of G to be a subgroup of order p^a.

Theorem.

1. Let G be a finite group and p a prime dividing the order of G. Then G has a sylow p-subgroup.

2. Any two sylow p-subgroups are conjugate. This will imply that there can only be one sylow p-subgroup in G up to isomorphism. (since any conjugate is the same up to isomorphism)

3. The number of sylow p-subgroups is 1 mod p and divides the order of G.

We will prove this but we need a lemma and will do some examples of applications.

Lemma. If there is only 1 sylow p-subgroup P in G then P is normal.

Proof. For any g in G, gPg^{-1} must be P since there is only 1 sylow p-subgroup, and thus it is a normal subgroup.

□

Proposition. Let n_p be the number of sylow p-subgroups in a simple non-abelian group G. Then the theorem above implies that $|G|$ divides $\frac{n_p!}{2}$ and that $n_p \geq 5$.

Proof. Let G act by conjugation on its Sylow p-subgroups, then this has trivial kernel since G is simple. If the kernel is G then P is normal, and is thus the whole of G. But then the center is non-trivial and a normal subgroup and by a previous theorem is not the identity, impliying G is abelian by simplicity.

Therefore the kernel is the identity. Therefore the homomorphism induced by the action is injective. Therefore G is isomorphic to a subgroup of S_{n_p}. But then arguing about simplicity + the kernel of the sign homomorphism and the fact that G has order greater than 2 (since it is not abelian) as we have done before implies G is isomorphic to a subgroup of A_{n_p} which implies the first part. Also, we can check that all non-abelian subgruops of $A_{<5}$ are non-simple which implies the $n_p \geq 5$ part.

□

Example (Using the theorem above):

Suppose we have a non-abelian simple group of order 132. Then by part 3 of the theorem there are either 1 or 12 sylow 11-subgroups as it must be 1 mod 11 and divide 132, but there are 12 by the above corrolary. For the same reason there must be 22 sylow 11-subgroups.

This is impossible because all 12 sylow 11-subgroups intersect trivially which means we have 120 elements of order 11, which means we cannot have enough elements of order 3. Therefore every simple group of order 132 is abelian, but we proved earlier any abelian simple group has prime order. Therefore there are no simple groups of order 132.

Now we will prove the main theorem.

Proof. **Proof of part 1 of the theorem:**

Let Ω be the set of subsets of G with order p^a. These are arbitrary subsets, not subgroups.

Let G act on Ω by $g\{g_1, g_2, \ldots, g_{p^a}\} = \{gg_1, gg_2, \ldots, gg_{p^a}\}$.

We note that $|\Omega| = \begin{pmatrix} n \\ p^a \end{pmatrix}$. We want to show that this is not divisible by p. Let $n = mp^a$ with m not divisible by p. Lets expand $(1+x)^{mp^a}$ and pretend like all coefficients as equal if they are equal mod p.

$$(1+x)^p = 1 + x^p + \sum_{n=1}^{p-1} \begin{pmatrix} p \\ n \end{pmatrix} x^n = (1+x^p)$$

Since $\frac{p!}{n!(p-n)!}$ is divisible by p.

$$(1+x)^{p^a} = ((1+x)^p)^{p^{a-1}} = (1+x^p)^{p^{a-1}} = \left(1+x^{p^2}\right)^{p^{a-2}} = \cdots = 1 + x^{p^a}$$

Now

$$(1+x)^{mp^a} = \left(1+x^{p^a}\right)^m = \sum_{n=0}^{m} \begin{pmatrix} m \\ n \end{pmatrix} x^{jp^a} mod\ p$$

Here the coefficient of x^{p^a} is m mod p and thus $\begin{pmatrix} mp^a \\ p^a \end{pmatrix}$ is not divisible by p.

Also, if U is in Ω and $H \leq G$ stabilizes U, then $|H|$ divides $|U| = p^a$. This is because hU=U for all h in H which means that the whole coset HU is contained in U. Then the cosets of H in U partition U so $|H|$ divides $|U|$.

Now $|\Omega| = |O_1| + |O_2| + \cdots + |O_n|$ where O are the orbits of the action. Since p does not divide $|\Omega|$ there is an orbit ϑ whose size is not divisible by p otherwise p would divide the RHS.

Let T be in ϑ, then since the orbit ϑ has size not divisible by p, this implies that the stabilizer of T is divisible by p^a, but also divides p^a from earlier, and this gives us a subgroup of order p^a.

[Lecture 7 ends]

Proof of part 2 of the theorem:

Let P be a sylow p-subgroup and let Q be any subgroup of G with size a power of p. Let Q act on G/P (the set of cosets) by q.gp=(qg)p. The orbits of this action have size divisible by p since the orbit is divisible by the size of the group. The total number of orbits is not divisible by p so there is a size 1 orbit. Therefore there is a g in G such that qgP=gP for all q in Q. It therefore follows that for all q in Q, $g^{-1}qg$ is in P, therefore the conjugate of Q with respect to g is in P.

Applying this to the case that Q is another sylow p-subgroup implies the claim.

Proof of part 3 of the theorem:

The proof of the first part is that the conjugation action of G on $Syl_p(G)$ has one orbit by part 2 and thus the size of the orbit divides the order of G so we just have to show the size is 1 mod p.

Let P be a sylow p-subgroup. Consider P acting on $Syl_p(G)$ by conjugation. Now orbits have size 1 or are divisible by p. But note that {P} is a size 1 orbit as conjugating P by anything in P gives back P itself, so we just need to show that all other orbits are divisible by p.

Suppose for a contradiction that {Q} is another size 1 orbit, meaning that for any h in P we have that in fact $hQh^{-1} = Q$. Then consider the normalizer of Q in G, then this contains P. Also, Q is a sylow p-subgroup in its own normalizer. We know that P is also a subgroup of the normalizer. But then by definition, Q is normal in its own normalizer and part 2 implies that P is conjugate to Q but by normality this implies P=Q so this is our contradiction.

□

Example. Let G be te group $GL_n(\mathbb{Z}/p)$ which is the n*n matrices in $\mathbb{Z}/p$ which are invertible with p a prime.

Lets figure out the size of G. Lets build an invertible matrix columnwise. There are p^n choices for the first column but really $p^n - 1$ because we do not want to pick 0.

For the second column we can pick anything but any of the p multiples of the first column. Therefore there are $p^n - p$ choices for the second column.

The third column should not be a linear combination of the first 2 columns. There are $p^n - p^2$ choices.

We end up with total choice count

$$(p^n - 1)(p^n - p)\left(p^n - p^2\right)\dots\left(p^n - p^{n-1}\right)$$

The number of factors of p in the brackets respectively are 0,1,2,...,n-1 so the total number of times p divides the above is $p^{\frac{n(n-1)}{2}}$.

Now we can find a sylow p-subgroup in here. We need to find a subgroup of order $p^{\frac{n(n-1)}{2}}$. One such subgroup is the set of upper triangular matrices with 1's on the diagonal. We have now found all of the sylow p-subgroups because we can just conjugate.

2 Rings

2.1 Basic properties

A ring (we will define this precisely) is something in which we can add and multiply. Examples include the integers, the integers mod n, or the real polynomials in a variable, and more. We can think of this as a sort of number system.

Definition. A ring is a set equipped with +, * and elements 0 and 1 are in the set.

+ is a function we refer to as addition and * is a function we refer to as multiplication. These are binary operations, so functions from ordered pairs of the sets to elements of the set.

We have the property that R under + with identity 0 is an abelian group.

We have that the operation * is associative, ie (a*b)*c=a*(b*c)

We have that for all a in the ring, 1*a=a*1=a

We also have that a*(b+c)=(a*b)+(a*c) always and (a+b)*c=(a*b)+(a*c)

We will call -x the additive inverse of x, which exists by the group property.

We say R is a commutative ring if multiplication is also commutative. In this course all rings we will work with commutative rings only, but there are non-commutative rings, such as certain sets of matrices.

Definition. A subring has the obvious definition – If a subset of a ring is closed under addition and multiplication and taking minus of elements then it is a subring.

Example. We have the integers which is a subring of the rationals which is a subring of the reals which is a subring of the complex numbers.

Definition. A field is a commutative ring where every non-zero element has a multiplicative inverse. This includes the rationals, the reals and the complex numbers, but not the integers. Here the non-zero elements form a group under multiplication.

Example. The gaussean integers (a+bi with a and b integers) is a ring. It is a subring of the complex numbers. We write it as $\mathbb{Z}$[i] to mean we start with $\mathbb{Z}$ and "adjoin" the element i.

Example. The ring $\mathbb{Q}\left[\sqrt{2}\right]$ is a subring of $\mathbb{R}$ which is the set of all $a + b\sqrt{2}$ with a and b rational.

The dual numbers from the vector calculus course are another example.

Definition. An element u of a rind R is a unit if there is an element v such that uv=1.

Note that 2 is a unit in $\mathbb{Q}$ but not $\mathbb{Z}$ so this does not interact well with subrings.

[Lecture 8 ends]

Proposition. Let R be a ring. Then for any r in R, 0*r=0.

Proof. Take 0+0=0 and multiply by r to get r0+r0=r0. We can cancel additively to get r0=0.

□

Note that if 1=0 then 0 is the only element since if there is another element then that times 0 is itself so it must be 0. So we get the "zero ring".

Proposition. Let R be a ring, then for any r in R, -r (the additive inverse) is equal to -1*r

Proof. r+(-1*r)=(1+-1)r=0r=0 by the distributive property.

□

Definition. Let R and S be rings, then the direct product $R \times S$ can be defined with operations coordinate wise. It is easy to verify in your head that this is a ring. Therefore stuff like $\mathbb{C} \times \mathbb{Z}$ is a ring.

Definition. Let R be a ring. A polynomial in x with coefficients in R is an expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

Where the a's are elements of the ring.

We interpret higher order terms as having zero coefficients. The index of the largest non-zero term is called the degree (as we know).

We have convention that the zero polynomial has degree $-\infty$ so that the degree of products is the sum of the degrees.

A polynomial is called monic if it has degree n and $a_n = 1$.

Definition. The polynomial ring R[x] is the set of all polynomials with coefficients in R. The operations are the obvious ones (Add coefficients for addition, multiply and distribute for multiplication) and the identity elements are 0 and 1.

We get the x^i coefficient of the product is $\sum_{j=0}^{i} a_j b_{i-j}$ where the original polynomials have coefficients a_n and b_n.

Remark. Any element of the ring R[x] gives a function R to R, since R is closed under addition and multiplication.

Definition. The ring of formal power series over $\mathbb{R}$ in the variable x is written as $\mathbb{R}[[x]]$ and we say nothing about whether it is a function or it converges or whatever, it is simply a list of infinite coefficients.

Example. Consider the element (1-x) in R[x]. In general this is not a unit since the inverse would have to be $\frac{1}{1-x}$. Even if you could multiply it by something and get a function that is the same as the identity function, a polynomial viewed purely as a list of coefficients cannot have an inverse.

However, in $\mathbb{R}[[x]]$ it does have an inverse given by $1 + x + x^2 + x^3 + \ldots$. However, something with 0 constant term does not have an inverse so it is not quite a field.

Definition. Write $R\left[x, x^{-1}\right]$ for the wring of all Laurent Polynomials, ie things of the form $f = \sum_{i \in z} a_i x^i$ with all but finitely many coefficients equal to 0. Here, something like x has an inverse given by $\frac{1}{x}$ but the polynomial 1-x does not have an inverse

Definition. A function between two rings is a homomorphism if the following hold:

1. $f(r_1 + r_2) = f(r_1) + f(r_2)$
2. $f(r_1 r_2) = f(r_1) f(r_2)$
3. $f(1) = 1$

Note that unlike in groups, property 3 is not automatic since multiplication is not always invertible.

As usual it is called an isomorphism if it is bijective and its inverse is also an isomorphism.

The kernel of f written ker(f) is the set of r such that f(r)=0, and the image is s in s such that s is f(r) for some r.

Lemma. A homomorphism f from R to S is injective if and only if it has zero kernel.

Proof. The same proof as in the groups course.

□

Definition. A subset I in R is called an ideal if it is the kernel of some ring homomorphism.

Ideals are closed under multiplication by arbitrary elements in the ring. If 1 is in an ideal it is the whole ring. An example of an ideal is $n\mathbb{Z}$ in $\mathbb{Z}$. In fact every ideal in $\mathbb{Z}$ has this form as we showed in the groups course when we showed that every subgroup of $\mathbb{Z}$ is of the form n$\mathbb{Z}$. Another example is polynomials with no constant term in polynomial rings.

Proposition. If $\phi : R \to S$ is a ring homomorphism then its kernel is an ideal.

Proof. Since ϕ is also a group homomorphism we know that its kernel is a subgroup. We note that we have that if a is in the kernel then $\phi(ab) = \phi(a)\phi(b) = 0$ so ab is also in the kernel, justifying that ideals are closed under multiplication by arbitrary ring elements.

□

Proposition. If an ideal contains any unit it is the whole ring.

Proof. This is because if u is a unit in the ideal then its inverse v exists and uv is in the ideal which is 1 so the ideal is the whole ring.

□

[Lecture 9 ends]

Let R be a ring and let A be any subset. Then the ideal generated by A written (A) is the set of all linear combinations of elements of A with coefficients in R, all of which are 0 except for finitely many.

Definition. An ideal is called principal if it can be generated by a single element.

Example. The subset of $\mathbb{R}[x]$ such that the constant term is 0 is an ideal because it is the kernel of the "take the constant term" homomorphism and it is principal because it is generated by the polynomial x.

Definition. Let I be an ideal in a ring R. Then the quotient ring is the set of cosets of I in R of the form r+I with 0 and 1 given by 0+I and 1+I and the operations given by

$$(a+I)(b+I) = ab+I \text{ and } (a+I)+(b+I) = (a+b)+I$$

and this is literally just the abelian group quotient structure. It's like reducing "mod" I.

Proposition. The quotient ring is actually a ring and the function that sends R to R/I by sending an element to its coset is a ring homomorphism with kernel I.

Proof. We see that R/I has 0 and 1 and is closed under addition, multiplication and inverses and has the distributive property. Multiplication is well defined because if $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$ then $r_i - r_i' \in I$ for I both 1 and 2. Now $r_1'r_2' = (r_1 + a_1)(r_2 + a_2)$ which is r_1r_2 plus something in I, since I is closed under addition and multiplication by arbitrary group elements. The map is a ring homomorphism because we see that it sends 1 to 1, 0 to 0 and preserves additive and multiplicative structure.

□

Example. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to C_n as a group with multiplication defined by usual modular arithmetic.

Example. Take (x) in $\mathbb{C}[x]$. Then the quotient $\mathbb{C}[x]/(x)$ can be represented by elements of the form

$$\left[a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\right] + (x)$$

but then this is only unique up to what the first coefficient is – the cosets are exactly the sets of constant a_0. Therefore $\mathbb{C}[x]/(x)$ is isomorphic to $\mathbb{C}$.

Proposition. (Euclidean algorithm for polynomials – this is the same thing that we did in the level 4 partial fractions proof) Let K be a field. Let f and g be polynomials in $K[x]$. Then there exists two polynomials r and q in $K[x]$ such that f=gq+r with $\deg(r) < \deg(g)$.

Proof. Let n be the degree of f so $f = \sum_{i=0}^{n} a_i x^i$. Let $g = \sum_{i=0}^{m} b_i x^i$ where a_n, b_m are not 0 so n and m are actually the degrees of f and g. If n<m we are done as we just set q=0 and r=f.

If $n \geq m$ we can proceed by induction on n. Note that if n=0 this is quite obvious.

Define $f_1 = f - \left(a_n b_m^{-1}\right) x^{n-m} g$ where we are using the fact that all non-zero elements have a multiplicative inverse. Now by construction $\deg(f_1) < n$. If n=m then $\deg(f_1) < n = m$ so we are done.

Otherwise if n>m write $f_1 = gq_1 + r_1$ where $\deg(r_1) < \deg(g) = m$ by the induction hypothesis.

Then write $f = a_n b_m^{-1} x^{n-m} g + q_1 g + r_1$ and then we are done.

□

Corollary. All ideals in $K[x]$ for K a field are principal

Proof. We use the euclidean algorithm from numbers and sets/groups to prove this for the integers, and we can do the same thing: Take the smallest degree element inside the ideal then by the euclidean algorithm everything has to be divisible by that or the remainder would be smaller.

□

However, $\mathbb{Z}[x]$ or $K[x, y]$ do not necessarily have this property, since one is not a field and the other is not in a single variable.

Definition. A principal ideal domain is a ring where every ideal is a principal ideal.

We will now do the three isomorphism theorems for rings, which is easy since it is basically the same as what we did for groups.

Theorem. Let $\phi : R \to S$ be a ring homomorphism, then the map $R/Ker(\phi) \to Im(\phi)$ is a well defined ring isomorphism.

Proof. Well defined-ness is something we just did, bijectivity follows from the group homomorphism property, and the fact that it is actually a homomorphism is by an earlier proposition.

□

Example. Consider the ring homomorphism from $\mathbb{R}[x] \to \mathbb{C}$ by sending $f(x) \to f(i)$. Then it is clearly surjective so the kernel is exactly polynomials f(x) such that $f(i) = 0$. But then since these are real polynomials, it follows that -i is also a root, so the kernel is exactly the polynomials that are divisible by $x^2 + 1$. So the kernel is the ideal generated by $x^2 + 1$ in the polynomial ring $\mathbb{R}[x]$.

Therefore $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.

Theorem. Let R be a subring of S and J is in ideal in S. Then $J \cap R$ is an ideal in R and $(R + J) / J$ is a subring of S/J. Furthermore $R/R \cap J \cong R + J/J$. The + just means the set of all $\{r + j, r \in R,\ j \in J\}$

Proof. Define a function from R to S/J by sending r to r+J, and the kernel of this is exactly J, but the kernel is contained in R so it is $R \cap J$ so $R \cap J$ is an ideal. The image is exactly $\{r + J, r \in R\}$ which is $R + J/J$ so by the previous theorem the result follows.

□

[Lecture 10 ends]

Theorem. (Correspondence, rings version) If I is an ideal in R then there is a bijection between subrings of R containing I and subrings of R/I.

Proof. Send L in R/I to the set of r in R such that r+I is in L, and if S is a subring containing I send it to the quotient ring S/I.

□

Similarly there is a correspondence between ideals of R/I and ideals of R containing I.

Theorem. Let I be an ideal in R and J be another ideal with I contained in J. Then J/I is an ideal in R/I and $(R/I)/(J/I)$ is isomorphic to R/J.

Proof. Define a function from R/I to R/J that sends the coset r+I to the coset r+J. This is well defined by the groups part. This is a ring homomorphism and its kernel is J/I. Therefore J/I is an ideal in R/I since it is a kernel. And the image of this homomorphism is R/J so the result follows from the first isomorphism theorem.

□

Lemma. Let R be any ring, then there is a unique homomorphism $\mathbb{Z} \to R$ sending 1 to 1_R. This is because we have to send k in $\mathbb{Z}$ to $1_R + 1_R + \cdots + 1_R$ k times.

Notice that the zero ring has no homomorphisms to non-zero rings because we would have to send 0 to both 0 and 1. But we can send a non-zero ring to a zero ring by sending everything to 0.

Definition. Let i be the ring homomorphism $\mathbb{Z} \to R$. Then ker(i) is an ideal in $\mathbb{Z}$ equal to either 0 or n$\mathbb{Z}$. In the second case we call n the characteristic of R, and we say the characteristic is 0 otherwise.

Example. In a ring like $\mathbb{Z}/6\mathbb{Z}$ we notice that 2*3=0 but 2 and 3 are not 0.

Definition. An integral domain is a non-zero ring R where we cannot have two non-zero elements whose product is 0. In other words, ab=0 implies a=0 or b=0.

Definition. A zero divisor is a non-zero a in R such that there exists a non-zero b such that ab=0. An example is 2 and 3 in $\mathbb{Z}/6\mathbb{Z}$.

Proposition. Any field is an integral domain

Proof. If $ab = 0$ with b not 0 then $abb^{-1} = 0b^{-1} = 0$ so a=0.

□

We note that any subring of a field is also an integral domain.

Proposition. Let R be a finite integral domain, then R is a field

Proof. Let a in R be non-zero, The function $\mu_a : R \to R$ sending $r \to a * r$ is a group homomorphism but not a ring homomorphism. Since R is an integral domain it has 0 kernel. Therefore μ_a is injective. Since r is finite, μ_a is also surjective, so in particular there is some element that is sent to 1, and this is the inverse we want. So a is a unit. Since a was arbitrary, anything is a unit so we are done.

□

Definition. Let R be an integral domain. A field of fractions of R is a field F satisfying

1. R is a subring of F
2. Every x in F can be written as ab^{-1} for a and b in R and b^{-1} the multiplicative inverse of b in F.

Example. The field $\mathbb{Q}$ is a field of fractions of $\mathbb{Z}$.

Theorem. Every integral domain R has a field of fractions

Proof. Define a set $S = \{(a, b) \in R \times R \mid b \neq 0\}$. Think a divided by b. We define an equivalence relation by (a,b) equivalent to (c,d) if and only if ad=bc in R.

□

Claim: This is actually an equivalence relation

Proof. Symmetric and reflexive are trivial so we just need to check that it is transitive.

Suppose (a,b)∼(c,d) and (c,d)∼(e,f). So ad=bc and cf=de. We want to show that af=be.

Multiplying the two equations by f and e respectively we get adf=bcf and bcf=bde, so adf=bde. So we get d(af-be)=0. Since d is non-zero by definition and we are in an integral domain we can cancel it to get the result.

□

Ok so we have an equivalence relation. Now define F to be the set of equivalence classes in S. We just need to show that this is actually a field. We will conveniently denote (a,b) as $\frac{a}{b}$. We define to add and multiply the same way we do with fractions and then we have a field.

Ie,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$$

This is a ring because we can check the properties and it will work. For example, define $\frac{0}{1} = 0, \frac{1}{1} = 1$.

If $\frac{a}{b}$ is not 0 then $\frac{a}{b}$ is not $\frac{0}{1}$ so a*1 is not b*0 so a is not 0 so $\frac{b}{a}$ is a valid multiplicative inverse.

We define a homomorphism R to F by sending r to $\frac{r}{1}$. Clearly this is a ring homomorphism. Observe that the kernel is 0 so the image is isomorphic to R, well we basically already knew that anyway.

Note that $\frac{a}{b} = \left(\frac{a}{1}\right)\left(\frac{b}{1}\right)^{-1}$ so we have a field of fractions.

[Lecture 11 ends]

We need some definitions that honestly I don't know how useful they will be.

Proposition. Let R be a ring. Then R is a field if and only if the only ideals of R are 0 and R

Proof. If R is a field and I have an ideal I in R and R is not the zero ideal then I must contain a unit (since everything but 0 is a unit in a field) and an earlier proposition says I contains a unit implies I=R so we have done this direction.

If the only ideals are 0 and R then take some non-zero element r in R. Then the ideal generated by r (consisting of all multiples of r) is R and therefore 1 is in the ideal generated by r and therefore r is a unit, and since r was arbitrary every non-zero element is a unit.

□

Definition. An ideal I in R is called maximal if it is not equal to R and any ideal it contains is equal to either R or itself.

Proposition. An ideal I in R is maximal if and only if R/I is a field.

Proof. R/I is a field if and only if its ideals are 0 and R/I itself by the previous proposition. Now we can apply the ideal correspondence result from earlier then we are done.

□

Definition. An ideal I not equal to R is called prime if whenever ab is in the ideal, either a or b is in the ideal.

Example. An ideal nℤ in ℤ is a prime ideal if and only if n is 0 or 1 or prime

It follows that 0 is a prime ideal only in an integral domain.

Proposition. An ideal I in R is prime if and only if R/I is an integral domain

Proof. If I is prime then let (a+I) and (b+I) be cosets in R/I. Suppose the product of a+I and b+I which is ab+I is 0 if and only if ab is in I, ie R/I is an integral domain, then we want to show that I is prime. But wait we know that if ab+I is 0 then ab is in I. But then by the integral domain property either a or b lies in I since either a+I or b+I is 0+I so we have a prime ideal.

Conversely if we have a prime ideal then if ab+I is I then either a+I or b+I is 0 so R/I is an integral domain.

□

Corollary. Every maximal ideal is prime

Proof. We know that every field is an integral domain, and an ideal I is maximal implies R/I is a field hence an integral domain which implies I is prime by the previous 2 propositions.

□

Proposition. The characteristic of an integral domain is either 0 or a prime number.

Proof. Consider the unique homomorphism $\mathbb{Z} \to R$. Characteristic n implies that nℤ is the kernel by definition, so by the first isomorphism theorem for rings, a subring of R given by the image of this homomorphism is $\mathbb{Z}/n\mathbb{Z}$. But if R is an integral domain then so is $\mathbb{Z}/n\mathbb{Z}$ so n must be prime.

□

Definition. Let a and b be elements of an integral domain R. We say a divides b if there exists some c in R such that b=ac. Equivalently, we can say that the ideal generated by b is contained in the ideal generated by a.

2.2 Integral domains and UFDs

From now on if I say R is any kind of domain, R is assumed to be an integral domain.

Definition. We say a,b in R are associates if a=bc for c in R a unit or equivalently the ideals generated by a and b are equal, or equivalently a and b divide eachother.

This can get really complicated, for example in the formal power series ring,the power series x and $x + x^2 + x^3 + x^4 + \ldots$ are associates because $1 + x + x^2 + x^3 + \ldots$ is a unit with inverse $1 - x$. But it is easier to check that these two power series generate the same ideal.

Definition. An element r in R is irreducible if (analgous to a prime in ℤ), ie r is not 0, not a unit, and cannot be factored into two non-units.

Definition. An element p in R is a prime element if p is not 0, not a unit and if p divides xy then either p divides x or p divides y.

Proposition. A non-zero element r in R is prime if and only if the ideal generated by r is a prime ideal

Proof. Let (r) be a prime ideal for r not 0. By definition of a prime ideal, r cannot be a unit. Suppose r divides ab, then ab is in (r), but (r) is a prime ideal so a is in (r) or b is in (r) so we have a prime ideal. Conversely, let r be a prime element and then yeah we know what to do if ab is in (r) then ab divides r so a or b is in (r) so we have a prime ideal.

□

Proposition. Prime elements in a ring R are irreducible.

Proof. If r is prime and r=ab then r either divides a or r divides b. So assume for example that r divides a, so a=rc for c in R. So r=rcb so cb=1 and therefore b is a unit, so we always have a unit if we try to factorize r, so r is irreducible.

□

[Lecture 12 ends]

Example. Let R=$\mathbb{Z}\left[\sqrt{-5}\right]$ as a subring of $\mathbb{C}$. This is obviously an integral domain because it is a subring of a field (as we have previously proven).

Define N to be a norm on R that goes from $\mathbb{Z}\left[\sqrt{-5}\right] \to \mathbb{N} \cup 0$, where we send any element to the square of its size, ie $a + b\sqrt{-5} \to a^2 + 5b^2$. Clearly, this function is multiplicative, ie $N(A)N(B) = N(AB)$.

We note that all units in R have norm 1 because if some unit had norm more than 1 that would imply existence of an element with norm less than 1 by multiplicitivity. Also all norm 1 elements are units because the only ones are 1 and -1.

In this ring, 2 is irreducible because $N(2) = 4$ so in order to factor it we would have to factor it into stuff with norm 2 and 2, but no element with norm 2 is in this ring.

This is not obvious, 2 is not irreducible in every ring, in some rings we could write it as $(1 + i)(1 - i)$.

Similarly, 3 and $1 \pm \sqrt{-5}$ are irreducible in this ring.

However, 2 is not prime in this ring. This is because $6 = 2 * 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$, so we do not have uniqueness of factorization. We don't have that 2 divides ab implies 2 divides a or 2 divides b, since 2 does not divide $1 \pm \sqrt{-5}$ in R.

Definition. A Euclidean domain is an integral domain R with the property that there exists a function N on R that goes from $R \setminus \{0\} \to \mathbb{N} \cup 0$ which has the property that

1. $N(ab) \geq N(b)$ for all non-zero a,b
2. If a,b are in R with b not 0 there exists q and r in R such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

Notice how this resembles properties of the integers.

Example. Consider $\mathbb{Z}\left[\sqrt{-1}\right]$ with the same norm as in the previous example.

We want to check that this norm makes our ring into a euclidean domain. We need to check property 2 (since property 1 is obvious).

Consider elements a and b in our ring, and suppose b is not 0. Consider the ratio $\frac{a}{b} \in \mathbb{C}$, then there is a point in $\mathbb{Z}\left[\sqrt{-1}\right]$ such that the distance from this point to $\frac{a}{b}$ is <1.

Ie, everything is in one of the circles shown in figure 1.

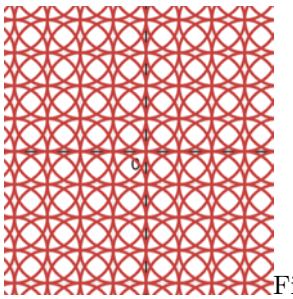
Figure 1

Now write $\frac{a}{b} = q + c,\ |c| < 1$. Then $a = bq + bc$ where $|bc| < b$ so we know the second property is satisfied so we have a euclidean domain.

Definition. A principal ideal domain is an integral domain such that every ideal is principal

Proposition. Every euclidean domain is a principal ideal domain

Proof. Same proof that every subring of $\mathbb{Z}$ is n$\mathbb{Z}$.

□

Example. The ring of polynomials in the integers is not a euclidean domain or a principal ideal domain, for example R=$\mathbb{Z}$[x] with the ideal of polynomials with even constant term. If this is generated by a single element, it must divide 2, and it is not 1 or -1 or it would generate all integer polynomials, and if it is 2 then we would not get non-constant polynomials.

Now we know that we cannot divide with smaller remainder in integer polynomials. For example, we cannot divide x by 2.

Definition. An integral domain is a unique factorization domain if every element is a product of irreducibles in a unique way up to ordering or multiplication by units

Lemma. In a principal ideal domain, any irreducible is prime.

Proof. Let p in R be irreducible. Suppose p divides ab and p does not divide a. Consider the ideal that p and a generate. This must be a principal ideal by definition so we can find some d that generates this ideal, and then we know d divides both a and p. Since d divides p we can write $p = q_1 d$ and by irreducibility of p, we know that either d is a unit or q_1 is a unit.

If q_1 is a unit write $d = q_1^{-1} p$, but d divides a so p divides a which we assumed it did not. Therefore the ideal generated by d is the whole ring. Therefore $1 = rp + sa$ for some r and s, so $b = rbp + sab$. But p divides the right hand side (since p divides ab) so p also divides b.

□

[Lecture 13 ends]

Lemma. Let R be a principal ideal domain, then if I have a countably infinite sequence of ideals contained in the next like $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ there exists some N>0 such that for all n>N all the ideals in the chain are the same.

Proof. Note that in $\mathbb{Z}$ this is familiar since we can't have infinite chains of divisors.

Now consider I as the union of all ideals in the chain. Then this is an ideal and we are in a PID so it is a principal ideal, therefore it is generated by some element r. So the sequence stabilizes when we get to some point in the chain containing r.

□

Theorem. Every principal ideal domain is a unique factorization domain (converse is false)

Proof. First we will show that r in R is a product of irreducibles in some way. If r itself is irreducible then we're done. So assume not then write $r = r_1 s_1$ with neither equal to a unit (since r is not a unit so we can do this). If r_1, s_1 are products of irreducibles then we are done. So assume, for example, that r_1 is not a sequence of irreducibles. Now repeat this process and then we get a chain of elements that cannot be written as products of irreducibles.

We now get a chain of ideals generated by each of the elements in this chain. But then this has to eventually become constant by the previous lemma, so say it stabilizes to r_N. So for all $n \geq N$, we have $(r_n) = (r_{n+1}) = (r_{n+1}s_{n+1})$ so s has to be a unit, so this is a contradiction. So we do have a factorization, we just don't know if it's unique.

Suppose for a contradiction that $p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$, then we want to show that these are the same up to ordering or multiplication by units.

We know p_1 divides $q_1 q_2 \dots q_m$, but because irreducible implies prime in a PID as proved earlier, we know p_1 is prime and thus divides some q_i which is irreducible and thus is associate to p_1. Now we do what we did in numbers and sets and cancel p_1, q_i and repeat this process and keep going until we are done – if we cancel everything from one side then we will get that a product of a bunch of irreducibles is a unit. But this is false because it implies one of these irreducibles is an inverse to the rest of them and hence is a unit.

□

Note that in any UFD, irreducible implies prime. This is because if p divides ab then factor a and factor b and one of them must have p in its factorization (or an associate of p).

We also know now that every euclidean domain is a UFD.

Definition. Let $a_1, \dots, a_n \in R$. We say d is a greatest common divisor of these if it divides all the a_i's and is divisible by all other common divisors.

Similarly we say m is a least common multiple if it is divisible by all a_i for all i and divides all other common multiples.

Theorem. Let R be a UFD, then GCDs and LCMs exist and are unique up to associates.

Proof. The idea is to do what we did for the integers: for GCDs we take the intersection of the prime factorizations (smallest power of each of the primes) and for LCMs we take the union (largest power of each of the primes). Note that this is consistent for integers where really GCDs are actually only unique up to + or – signs.

□

Now we will discuss factorization in polynomial rings.

We know that if the polynomial ring is over a field then we have a euclidean domain and therefore a unique factorization domain. We already knew we had unique factorization for polynomials. In fact the above proof really isn't surprising since we used euclid-like properties to prove that and UFD for integers in earlier levels.

We know an element is irreducible if and only if it is prime because we have a UFD.

Let f be irreducible and consider the ideal generated by f in the polynomial ring K[x] where K is a field. Then this is a prime ideal by a previous proposition. So suppose this is contained in another ideal J, then J=(g) for some g since we have a PID. Then $f = gh$ for some polynomial h, but f is irreducible so either g or h is a unit, so (f) must be a maximal ideal.

Definition. Let R be a UFD and f be a polynomial $a_0 + a_1x + \cdots + a_nx^n$ in R[x]. The content of f which we write as C(f) is defined to be $\gcd(a_0, a_1, \ldots, a_n)$. If C(f) is a unit we say that the polynomial is primitive.

Theorem. (Gauss's Lemma) Let R be a UFD and take a polynomial f in R[x]. If f is primitive then f is reducible in R[x] if and only if f is reducible in F[x] where F is the field of fractions of R.

As an example, 2x+2 in $\mathbb{Z}$[x] is reducible as 2(x+1) but in $\mathbb{Q}$[x] it is irreducible up to units since 2 now becomes a unit. However, this is not a contradiction because we do not have a primitive polynomial.

[Lecture 14 ends]

As an example, since $x^3 + x + 1$ does not have any integer polynomial factors, we can conclude it does not have any rational polynomial factors, ie no rational roots. But we need to actually prove the lemma.

To prove this we need another lemma which says that if R is a UFD and in the polynomial ring of R if f and g are primitive then their product is primitive. The proof is we can say $f = a_0 + a_1x + \cdots + a_nx^n$ and $g = b_0 + b_1 + \cdots + b_mx^m$ both primitive and with non-zero leading coefficient, so we just need to show that the gcd of the coefficients of $f * g$ is also 1. So Suppose there is some non-unit irreducible p in R such that p divides every coefficient of $f * g$. Suppose that k and l respectively are the smallest integers such that p does not divide a_k and p does not divide b_l. Then the x^{k+l} coefficient of $f * g$ is given by $\sum_{i+j=k+l} a_ib_j$ which we are assuming is divisible by p, but notice that this is not possible because by the "smallest" assumption, p divides every term except for one, which is the a_kb_l term and therefore p does not divide the whole thing so we have our contradiction.

Define the content of a polynomial to be the greatest common divisor of all the coefficients, then by the same logic as above (factoring out the content first), content is multiplicative up to units.

We will now prove Gauss's lemma. Note that if f is reducible in R[x] then we can write it as gh where g and h both have content 1 and therefore have to have degree at least 1 it is trivially reducible in F[x] by just using the same factorization as we know that g and h will not be units since they don't have degree 0. So suppose f is reducible in F[x]. Then we can find a and b in our ring R such that if we change $f = gh$ to $abf = (ag)(bh)$ then ag and bh are in R[x]. Now we will consider the content of ag and bh. Since f has content 1 since we are supposing it is primitive in R[x], it means that $(ag)(bh)$ has content ab, so Content(ag) and Content(bh) multiply to ab times a unit.

But then we can cancel the ab's since everything has content ab, and then we get that f is reducible in R[x].

Proposition. Let R be a UFD and F a field of fractions. Let g in R[x] be primitive. Then if I have some f in R[x] divisible by g in F[x], then it is also divisible by g in R[x].

Proof. Write f=gh in F[x]. Now for some b, $bf = g(bh)$, and now there is some c=Content(h) such that $bf = g(ch_1)$ with h_1 primitive. But now b divides the right hand side so it divides ch_1 since g is primitive, so we get that g divides f in R[x].

□

Theorem. Let R be a UFD, then R[x] is a UFD.

Proof. Let f be in R[x]. Then write $f = cf_1$ with f_1 primitive and factorize the content c. Therefore we write

$$f = p_1p_2 \ldots p_nf_1$$

with the p's irreducible. Now try to factorize f_1 as much as possible into products of polynomials with smaller degrees until we have a product of irreducibles.

Now write $f_1 = q_1q_2q_3 \ldots q_m$ where each q is irreducible, and each has degree at least 1 because f_1 is primitive. So we just have to show that this factorization is unique. Uniqueness is known for the p parts by properties of content, and uniqueness for the q's is because if

$$f_1 = q_1q_2 \ldots q_m = r_1r_2 \ldots r_l$$

But now we can conclude uniqueness in F[x] since we have the Euclidean algorithm for polynomials in fields. But by Gauss's lemma, since we have a factorization that is unique up to associates in F[x] it is also unique up to associates in R[x].

□

Corollary. The polynomial ring in 2 variables $\mathbb{Z}[x, y]$ is a UFD if we view it as $\mathbb{Z}[x][y]$.

[Lecture 15 ends]

We will prove a theorem which feels random but hopefully it will be useful later.

Theorem. Let R be a UFD and let f be a degree n primitive polynomial $a_0+a_1x+\cdots+a_nx^n$ in R. Let p in R be irreducible and suppose p does not divide a_n, p divides all other coefficients, and p^2 does not divide a_0. Then f is irreducible in R[x] and therefore F[x] where F is the field of fractions of R.

Proof. Suppose $f = gh$ where

$$g = r_0 + r_1x + \cdots + r_kx^k, h = s_0 + s_1x + \cdots + s_lx^l$$

Clearly it cannot be the case that p divides either of r_k or s_l. Also p must divide exactly one of r_0 and x_0.

Suppose p divides r_0.

Let j be the smallest index such that p does not divide r_j.

Now clearly

$$a_j = r_0s_j + r_1s_{j-1} + \cdots + r_js_0$$

and here every term has a factor of p in it except for the last one because p divides neither of s_0, r_j (as p is prime since we have a UFD). Therefore p does not divide a_j. But now j=n because we supposed that is the only a coefficient which p does not divide. Therefore g has degree n which implies the degree of h is 0. But we supposed f is primitive which means we do not have a proper factorization, so this completes the proof.

□

Ok turns out this actually is useful:

Example. $x^n - p$ for a prime p has no rational roots

Example. Let p be a prime and consider the polynomial

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Now $f(x) = \frac{x^p-1}{x-1}$. Now consider $h(y) = f(y+1)$. We can calculate

$$h(y) = \frac{(1+y)^p - 1}{y} = y^{p-1} + \begin{pmatrix} p \\ 1 \end{pmatrix} y^{p-2} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix}$$

Now the last term is p and the rest are clearly divisible by p, so f has no rational roots.

2.3 Gaussean integers

We will now explore the ring of gaussean integers, which is $\{a + bi : \ a, b \in \mathbb{Z}\}$.

This has a norm $N(a + bi) = a^2 + b^2$ and we know it is a euclidean domain and hence a unique factorization domain. In this ring the units are exactly the things with norm 1 which are 1, -1, i and -i. In this ring, 2 is not a prime because $2 = (1 + i)(1 - i)$. However, 3 is prime, because $N(3) = 9$ so we would need some element of norm 3 which clearly does not exist.

Note that if $p = a^2+b^2$ then $p = (a+bi)(a-bi)$ and conversely if $p = (a+bi)$ (something) then $N(a+bi)\,N$ (something) $= p^2$ so both norms must be equal to p since there is no other way to decompose p^2 which means $p = a^2+b^2$.

Also anything with prime norm is prime.

Proposition. The primes in $\mathbb{Z}$[i] up to associates are either

1. 1+i
2. The primes in $\mathbb{Z}$ which are 3 mod 4
3. z in $\mathbb{Z}$[i] with $z\overline{z} = p$ where p is 1 mod 4.

This is related to (and in fact implies) something we proved in misc results which says that a prime is the sum of 2 squares if and only if it is 1 mod 4, however we do not need this but that proof is so beautiful I recommend you check it out anyways.

Proof. To prove this we will first show that if p is a prime and F_p is the field of integers mod p then the group $F_p^\times$ of non-zero elements under multiplication is isomorphic to C_{p-1}.

The proof of the lemma is that there is some generator, ie some t such that t^{p-1} is not only 1 mod p but for all x less than p-1, t^x is not 1 mod p. Here t is called a primitive root, and we just need to prove the existence of such a primitive root.

For each number a between 1 and p-1, by Fermat's little theorem or Lagrange's theorem, the order of a in our multiplicative group must divide p-1. For each d dividing p-1, let $\psi(d)$ be the number of a's with order d, then we want to show that $\psi(p-1) > 0$. Let n be any number dividing p-1 and write p-1=nk, then write

$$X^{p-1} - 1 = X^{nk} - 1 = (X^n - 1)\left((X^n)^{k-1} + (X^n)^{k-2} + \cdots + X^n + 1\right)$$

Note that the polynomial $X^{p-1} - 1 = 0 \bmod p$ has exactly p-1 integer solutions mod p: 1,2,...,p-1.

On the other hand, we know that the ring of polynomials in F_p cannot have more roots than the degree because the factor theorem holds with the same proof as in the real numbers, and we can do long division since we are in a field.

Therefore, $X^n - 1 = 0 \bmod p$ has at most n roots, and

$$(X^n)^{k-1} + (X^n)^{k-2} + \cdots + X^n + 1 = 0 \bmod p$$

has at most nk-n roots. The only way this can happen is if the number of roots is maximized since $X^{p-1} - 1$ has all nk roots and there are at most nk roots in

$$(X^n - 1)\left((X^n)^{k-1} + (X^n)^{k-2} + \cdots + X^n + 1\right)$$

Therefore if n divides p-1, $X^n - 1 = 0 \bmod p$ has exactly n integer solutions mod p.

On the other hand, if X=a is a solution, then $a^n = 1 \bmod p$ so the order of a divides n. For each divisor d of n, take the a's with order d and then these are exactly the solutions to $X^n - 1 = 0 \bmod p$. Therefore, if d_i are the divisors of n, then the number of solutions to $X^n - 1 = 0 \bmod p$ is exactly equal to $\psi(d_1) + \psi(d_2) + \cdots + \psi(d_r)$. But we know from earlier there are n solutions, so we conclude that

$$\psi(d_1) + \psi(d_2) + \cdots + \psi(d_r) = n$$

Now recall from numbers and sets that $\phi(n)$ is the number of integers from 0 to n that are coprime to n. We want to show by induction that $\phi = \psi$. Clearly, we have that $1 = \phi(1) = \psi(1)$.

Next, we verify that

$$\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n$$

There is a nice trick we can do: If we consider the fractions $\frac{C}{n}$ for integers $1 \leq c \leq n$, then the stuff coprime to d_i corresponds to exactly the fractions which are $\frac{C'}{d_i}$ when fully simplified, but every fraction has some divisor on the denominator when fully simplified, so the result follows.

Now by strong induction, we can determine ϕ and ψ given what it is for all its factors except for n itself. But now the statement is equivalent to the statement $\phi(p-1) > 0$ which is clearly true because 1 is coprime to p-1.

Now the proof of the proposition is as follows.

Step 1: We want to show that the given elements are all prime.

If $p = 3 \bmod 4$ it is not equal to $a^2 + b^2$ because a sum of 2 squares mod 4 can never be 3 (try the cases where a is even or odd), so it is prime.

If $N(z) = p$ then z is clearly irreducible since the norm is multiplicative.

Step 2: We want to show that the given elements are all the primes.

Let z in the gaussean integers be a prime, then $\overline{z}$ is also irreducible by symmetry. Now we note that $N(z) = |z|^2 = z\overline{z}$. Let p (a prime number in the normal integers) divide N(z) in $\mathbb{Z}$. Suppose that this p is 3 mod 4, then p divides $z\overline{z}$ which means p divides one of z, $\overline{z}$, but since they are just conjugates this implies p divides both, so p^2 divides N(z), and we want irreducibility which means that in fact p=z. We will show next lecture that if p is 1 or 2 mod 4 then N(z)=p.

[Lecture 16 ends]

If p is 1 mod 4 then $p - 1 = 4k$ for some integer k. But we also know that the multiplicative groups of numbers mod k is isomorphic to C_{4k} and this has a unique element of order 2, and we know that this must be -1 mod p. We know also that there is an element a of order 4 which means $a^2 = -1 \; mod \; p$. This means p divides $a^2 + 1$ so $p|(a+i)(a-i)$, and p is not irreducible since it clearly does not divide $(a+i)(a-i)$ and in the case p=2 we get $p = (1+i)(1-i)$. Therefore if p divides a gaussean integer it is certainly not irreducible. Furthermore, this factorization is unique up to units because the gaussean integers are a UFD.

Now suppose z is a gaussean prime and a prime of 1 or 2 mod 4 divides its norm, then $N(z) = z\overline{z}$. But now p is not irreducible so we get $p = z_1\overline{z_1}$ which divides $z\overline{z}$. But we are supposing that z is irreducible, so we must have that $z_1 = z$ up to units or conjugates.

□

Corollary. Any integer n can be written as a sum of 2 squares (possibly including 0) if and only if when we write it as a product of primes, the prime factors which are 3 mod 4 have even powers.

Proof. If n is $x^2 + y^2$ then we have $n = N(x+iy)$ and we must be able to factorize $x+iy$ and since we know the gaussean primes the result follows. Conversely, if n is a product of primes in this way then we can split the 3 mod 4 factors into 2 and split the other factors into 2 gaussean primes and then we can write n as a product of something with its conjugate, but if $n = (x+iy)(x-iy)$ then this implies $n = x^2 + y^2$.

□

2.4 The rest of rings

Definition. A complex number is called an algebraic integer if it is the root of a monic polynomial with roots in the integers.

Definition. We say that $\mathbb{Z}[\alpha]$ is the smallest ring containing $\mathbb{Z}$ and α or equivalently it is the set of polynomials in α with integer coefficieints.

Proposition. Let α be an algebraic integer, then if we take the homomorphism $\mathbb{Z}[x] \to \mathbb{C}$ that sends $g(x) \to g(\alpha)$, then

its kernel is a principal ideal generated by some irreducible and monic polynomial.

Proof. The kernel is all polynomials that are 0 evaluated at α. We want to show that they must be divisible by some minimal polynomial.

By definition of an algebraic integer we have non-zero kernel. Now take the polynomial of minimal degree with α a root and call this f_α, and it is primitive since we can clear factors. Now let I be the ideal generated by f_α. Then for some h in I, write $h = f_\alpha q + r$ in $\mathbb{Q}[x]$. We will clear denominators and write $ah = af_\alpha q + ar$ for some integer a. However, r must be 0 since it has lower degree than f_α but we supposed f_α was the minimal polynomial with α a root but α has to be a root of r. Therefore we know that $ah = af_\alpha q$ for some polynomial q. We also know (since f_α is primitive) that the contents of ah and aq are equal. But we know that a divides the content of ah because h is a polynomial in the integers, therefore we know that aq has content divisible by a so we can cancel the a's. We now get that f_α divides h as we wanted to show.

We note that f_α is irreducible because if we can factor it non-trivially one of them must have α as a root.

□

As an example, $\sqrt{2}, i, \sqrt{-3}, \frac{1+\sqrt{-3}}{2}, \sqrt[67]{420}$ are algebraic integers.

Proposition. If an algebraic integer is rational it is an integer

Proof. Let f_α be the minimal polynomial with α a root, which we know is monic since there must be monic polynomials in the ideal generated by this. By gauss lemma f_α is irreducible in $\mathbb{Q}$[x] but we know that if α is rational then $x - \alpha$ is a factor in $\mathbb{Q}$[x] so that must be the polynomial we started with (since we have something irreducible) but we are supposing we have an integer polynomial to begin with and so α must be an integer.

□

[Lecture 17 ends]

Definition. A ring is called noetherian if it satisfies the ascending chain condition, ie if I have a countably infinite sequence of ideals contained in the next like $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ there exists some N>0 such that for all n>N all the ideals in the chain are the same.

Proposition. A ring is noetherian if and only if all ideals are finitely generated

Proof. Suppose ideals are finitely generated. Given a chain of ideals consider their union. This is an ideal, so it is finitely generated, say by $r_1, r_2, \ldots, r_k$. But for each i there is an N such that r_i is in I_n, so after the maximum of these N's the chain stabilizes.

Conversely, if I is not finitely generated we can find a chain like

$$(r_1) \subseteq (r_1, r_2) \subseteq (r_1, r_2, r_3) \subseteq \ldots$$

□

Theorem. (Hilbert basis theorem) If R is noetherian then R[x] is noetherian.

Proof. Let J be an ideal in R[x], then we want to show that J has a finite generating set. So let f_1 in J have minimal degree. If $J = (f_1)$ then done so suppose not and choose $f_2 \in J \backslash (f_1)$ of minimal degree. Continue in this fashion to produce some sequence of f_i's. Suppose for contradiction all of them are non-zero.

Let a_i be the leading coefficient of f_i. This is an element of R.

We know that the ideal chain $(a_1), (a_1, a_2), \ldots$ stabilizes after m steps because R is noetherian.

Consider the polynomial $g = \sum_{i=1}^{m} b_i f_i x^{\deg(f_{m+1})-\deg(f_i)}$ where b_i is such that $a_{m+1} = \sum_{i=1}^{m} a_i b_i$, possible because R's ideal chain stabilizes after m steps.

By construction g has the same degree and the same leading coefficient as f_{m+1}, so the polynomial $f_{m+1} - g$ has smaller degree than f_{m+1} but it is generated by the first m f's, contradicting minimality.

□

Proposition. If R is noetherian and I is an ideal in R then the quotient R/I is noetherian.

Proof. Let J be in R/I and J' be the corresponding ideal in R. If $r_1, r_2, \ldots, r_m$ generates the J' then because J is the image of J' under the homomorphism $R \to R/I$ this means that $r_1 + I, r_2 + I, \ldots, r_m + I$ generates J.

□

Note: Subrings need not be noetherian. Take the non-noetherian ring as a polynomial ring of $\mathbb{C}$ in countably many variables. But if F is the fraction field of R then F is notherian because it's a field but R in F is not noetherian.

3 Modules

3.1 Basic properties

Definition. Let R be a ring and (M,+) be an abelian group. If we adjoin another operation * then we get an R-module if the operation $*\ : R \times M \to M$ satisfies

1. $(r_1 + r_2) * m = r_1 * m + r_2 * m$
2. $r * (m_1 * m_2) = r * m_1 + r * m_2$
3. $r_1 * (r_2 * m) = (r_1 r_2) * m$
4. $1_R * m = m$

Note that a logical consequence is that $r * e = r * (e + e) = r * e + r * e$ so $r * e = e$

Remark. If R is a field then an R-module M is just a vector space.

We say we are **scaling** by elements of R.

Remark. Any abelian group G is a $\mathbb{Z}$-module if n*g is defined as $g + g + g + \ldots + g$ n times (add g inverse for negative n).

Example. In any ring R the product $R^m = R \times R \times R \ldots R$ is an R-module.

Example. If I is an ideal then I is an R-module by sending $(R \times I) \to I$ sending $(r, x) \to rx$. Also, R/I is also an R-module by sending $(r, x + I) \to (rx + I)$.

Example. Let V be a vector space over k and let α be a linear map $V \to V$. Then we can make V into a $k[x]$ module by sending $(k[x] \times V) \to V$ by sending $(f(x), v) \to (f(\alpha) v)$. This depends on the choice of α.

[Lecture 18 ends]

Example. Take a ring homomorphism $\phi : R \to S$. This makes S into an R-module. This is because we can send $(r, s) \to \phi(r)\, s$. For example, $\mathbb{C}[x] \to \mathbb{C}[x]/x^2$ makes $\mathbb{C}[x]/x^2$ a $\mathbb{C}[x]$-module. But we already know that quotients in R are R-modules.

We also have things like the natural homomorphism $\mathbb{C}[x] \to \mathbb{C}[x, y]$ but we already know how to scale by elements of $\mathbb{C}[x]$ so it's not very interesting.

Definition. Let M be an R-module. A subgroup N of M is called a submodule if for every n in N and every r in R, r*n is in N.

Example. Suppose that R and M are both the rational numbers. Then if we take the integers as a subgroup of M, it is not a submodule, because it is not closed under scaling by elements of R.

If R is a field, a submodule is the same as a vector subspace.

Definition. Let N in M be an R-submodule. Then the quotient module is the abelian group M/N with the R-module structure on the cosets given as

$$(r, m + N) \to (rm) + N$$

It is easy to check that this is well defined and gives an R-module.

Let M,N be R-modules. An R-module homomorphism ϕ is a group homomorphism with the property that

$$\phi\left(r * m\right) = r * \phi(m)$$

A bijective R-module homomorphism is called an isomorphism.

We will now do the same theorems we did for groups and rings. This time we will not fully prove them because the proof is a copy of proofs we have already done.

Theorem. Let $\phi : M \to N$ be a homomorphism of R-modules. Then the kernel of ϕ which we will call K is an R-submodule of M and the image of ϕ is an R-submodule of N and there is an isomorphism between this and M/K.

The proof is the same as the groups one. We just need to check that the image is closed under scaling, but this is just the definition of a homomorphism.

We have other theorems for modules where again the proof is the same.

Theorem. Let K and L be submodules of M, then the set of all K+L is a submodule of M and there is an isomorphism between (K+L)/K and L/(K∩L).

To prove this we just need to check that the isomorphism actually preserves scaling. It is the same as the proof of the second isomorphism theorem for groups, just keeping in mind that all the homomorphisms we use in that proof preserve scaling.

Theorem. Let N be a submodule of L be a submodule of M. Then there is an isomorphism between M/L and (M/N)/(L/N).

Again, the proof is exactly the same.

There is a correspondence between submodules of M/N and submodules of M that contain N.

Definition. Let M be an R-module. For m in M its annihilator is Ann(m) and it is the the set of elements r in R such that r*m=e. We can also consider annihilators of subsets of M.

We can consider the intersection over all of M of all annihilators.

Observation: The annihilator of any subset S of M is an ideal in R. This is because if I have an element that scales all of the elements of S to 0 then our annihilator is closed under multiplying this by elements of R.

We can talk about submodules generated by m (just m multiplied by anything in R).

Proposition. For m in M there is an isomorphism $R/Ann(m) \to Rm$.

Proof. Consider the function $R \to M$ that sends $r \to rm$. This is an R-module homomorphism, so by the first isomorphism theorem the result follows.

□

Definition. An R-module M is finitely generated if there exists a finite set of elements in M that generate M, ie the module of linear combinations of this finite set is all of M.

Lemma. An R-module M is finitely generated if and only if there exists a surjective R-module homomorphism $R^k \to M$ for some K.

Proof. If M is finitely generated then we can write

$$M = Rm_1 + Rm_2 + \cdots + Rm_k$$

so we can set a homomorphism $R^k \to M$ by sending

$$(R_1, R_2, \ldots, R_k) \to R_1 m_1 + R_2 m_2 + \cdots + R_k m_k$$

Conversely if we have such a homomorphism set the image of $(0, 0, \ldots, R_i, \ldots, 0)$ to be m_i then because homomorphisms preserve structure we are done.

□

Corollary. Let M be finitely generated, then if N is a submodule then M/N is finitely generated

Proof. Take $R^k \to M$ by the previous proposition. Then the composition $R^k \to M \to M/N$ is another homomorphism which shows that M/N is finitely generated.

Note that a finitely generated module can have non-finitely-generated submodules.

As an example, take the ring $\mathbb{C}[x_1, x_2, \ldots, x_n]$ and M=R. This is clearly finitely generated because we just take the trivial homomorphism from R to R. But if we take the ideal $(x_1, x_2, \ldots)$, ie the set of things with no constant term, this is not finitely generated.

□

[Lecture 19 ends]

Definition. Let $M_1, M_2, \ldots, M_k$ be R-modules. Then the direct sum written $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ is the group $M_1 \times M_2 \ldots M_k$ with the action $r(m_1, m_2, \ldots, m_k) = (r * m_1, r * m_2, \ldots, r * m_k)$.

Definition. Let $m_1, m_2, \ldots, m_k$ be elements of M. We say this set is linearly independent if $\sum r_i m_i = 0$ implies all $r_i's$ are 0.

Definition. A subset S⊆M freely generates M if S generates M, and any function $f : S \to N$ for another R-module N extends to an R-module homomorphism ϕ_f: $M \to N$ such that $\phi_f(s) = f(s)$ for all s in S.

Definition. A module M is free if it is freely generated by some subset S of M. In this case we call S a basis.

Example. Consider the $\mathbb{Z}$-module C_2. If it were freely generated the only possibility for a basis is the set $S = \{1\}$ (Since S can never have 0). But this is not free because if we set N=$\mathbb{Z}$ and $f(1) = 1$ we wouldneed a nonzero homomorphism $C_2 \to \mathbb{Z}$ which does not exist.

However $\mathbb{Z}^k$ is a free $\mathbb{Z}$-module is you set S to all sets like (0,0,...,1,...,0).

Proposition. If S is a subset of M then the following are equivalent:

i) S generates M freely

ii) S generates M and S is linearly independent

iii) Every m in M is uniquely expressible as $m = \sum r_i m_i$ for m_i in S.

Proof. Clearly ii implies iii because by generation there is an expression and by linear independence it is unique. Also iii implies ii because existence implies generation and uniqueness implies linear independence.

Let S generate M freely. If S is not linearly independent then we can write $\sum r_i m_i = 0$ in an interesting way. Suppose, for example, that r_1 is not 0. Define a function $f : S \to R$ by semding $m_1 \to 1$ and the other $m_i's \to 0$. This therefore extends to a homomorphism $M \to R$. But then if we try to compute $\phi(0)$ we get both 0 and r_1 which is a contradiction.

We now will prove iii implies i then we will be done. If every m in M is uniquely expressible as $\sum r_i m_i$ then given a function $S \to N$ just define $\phi_f(m) = \sum r_i f(m_i)$. This is well defined by uniqueness. Also this is clearly a homomorphism since we defined it to be compatible with r-scaling.

□

Definition. Let M be finitely generated and let $\theta : R^k \to M$ be a surjective homomorphism that gives generators. Then the kernel of θ is called the module of relations for θ. We say M is finitely presented if for some surjective homomorphism θ, the kernel of θ is finitely generated.

Proposition. Let R be a nonzero ring and suppose R has a maximal ideal. If R^n is isomorphic to R^m then n=m.

Proof. If I is an ideal of R and M is an R-module then $IM = \{\sum r_i m_i : r_i \in I,\ m_i \in M\}$ is an R-submodule. But then consider the quotient M/IM. If r is in I then the map that sends something in M/IM to $r * (M/IM)$ is the zero map because $rm + IM$ is the zero coset. Therefore we can make M/IM into an R/I – module by (r+I)(m+IM) = (rm + IM).

Let I in R be maximal, then R^n/IR^n and $R^m/IR^m$are both vector spaces over R/I. Since recall that quotienting by a maximal ideal gives a field.

We know from vectors and matrices that if we have a vector space over a field then dimension is unique. So the result follows.

□

Note that all noetherian rings have maximal ideals (since if a ring didn't have a maximal ideal we could make an infinite chain of ideals contained in eachother). In fact, we could show that every ring has a maximal ideal and get the result for general rings, but we don't need that for the purposes of this course.

[Lecture 20 ends]

Fix a euclidean domain R with its norm $N : R \to \mathbb{Z}_{\geq 0}$.

By Euclid's algorithm, if I have a,b in R we can find x,y in R such that $ax + by = \gcd(a, b)$. The proof is the same as in numbers and sets.

3.2 Classification theorem

Definition. Let A be a matrix with entries in R. Then the elementary row operations are:

ER1: Add $c \in R$ times the i'th row to the j'th row

ER2: Swap row i and row j

ER3: Multiply row i by a unit in R.

Definition. Matrices A and B are said to be equivalent if A can be obtained from B by elementary row operations and the corresponding elementary column operations.

Example. Over $\mathbb{Z}$, the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ cannot be changed into $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Theorem. Any n*n matrix is equivalent to one of the form

$$\begin{pmatrix} d_1 & & & & & \\ & \ddots & & & 0 & \\ & & d_n & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

This is called smith normal form.

Proof. If A=0 then we are done.

Otherwise, set $A_{ij} \neq 0$ for some i,j. then perform row/column ops to make $A_{11} \neq 0$, possible as we can rearrange rows and columns.

1. For each j, if A_{1j} is not divisible by A_{11} write $A_{1j} = qA_{11} + r$ with $N(r) < N(A_{11})$

Use column operations to make everything in the first row equal to its r. Then swap columns to reduce the N-value of A_{11} then repeat finitely many times so that the first row is all 0 except A_{11}. Then do the same thing for the first column. At this point, we can make A_{11} divide the rest of the first row and first column. We now have a matrix like

$$\begin{pmatrix} d & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix}$$

We can do the same thing to C but then it does not gurantee that $A_{11}|A_{22}$. So suppose some A_{ij} in C is not divisible by d. Then write $A_{ij} = dq + r$ where $N(r) < N(d)$. Now add column 1 to column j, and subtract q times the resulting row 1 to row i. This gives r in the A_{ij} position. Now swap this r back to the 11 position. Now we can reclear the first row and first column. Now repeat at most finitely many times until d divides everything in C.

Now we can actually do the same thing to C and recurse and then the output will be as claimed.

□

Recall that for a matrix A, a k*k minor is the determinant of A if we delete all but k rows and columns.

Definition. For a matrix A, the k'th Fitting ideal $Fit_k(A)$ in R is generated by the k*k minors of A.

Proposition. If A and B are equivalent in the sense above then $Fit_k(A) = Fit_k(B)$ for all k.

Proof. We'll check that row and column operations don't change the ideals Fit_k.

Note that because determinants of matrices equal their transpose, $Fit_k(A) = Fit_k\left(A^T\right)$ so we just need to check row operations.

If we add a multiple of one row to another, then if they are both in the minor or the one we add to is not in the minor, then by determinant properties we do not affect anything.

Let C be a k*k submatrix and suppose the row we add to is the j'th row in C but the i'th row is not in C. Then we can compute the determinant of the new matrix after adding c times row i to row j, by expanding by the new row j, which is $[C_{jk} + cA_{ik}]$ for varying values of k.

We now get $Det(C') = Det(C) + cDet(D)$ where D is got by replacing row j of C with row i of A. But Det(C) and Det(D) are in the fitting ideal so done. And

The other 2 elementary row operations are trivial.

□

Corollary. If A has smith normal form (ie the diagonal form we proved we can get to in a previous theorem), then $Fit_k(A)$ is as follows:

Note that any k*k submatrix has a row that is at least the first, at least the second, and so on, and by the divisibility property its determinant must be divisible by $d_1 d_2 \dots d_k$. But also $Fit_k(A)$ by the minor with the first k rows and columns contains $d_1 d_2 \dots d_k$, and by R being a PID it is generated by $d_1 d_2 \dots d_k$. Therefore, the d_i's are uniquely determined, since $Fit_k(A)$ exists and is something, but we can read off the d's from it.

Proposition. Let R be a PID and R^m be a module with the obvious scaling operation. Any submodule of R^m can be generated by m or fewer elements.

Proof. Let N be a submodule of R^m. Consider some ideal I in R generated by the set of all $(r_1, r_2, \dots, r_m) \in N$. Then R is a PID so let this be generated by the m elements $(0, \dots, a_i, \dots, 0)$. So we know that $a_i | r_i$ for each i, thus everything generated by the $(0, \dots, a_i, \dots, 0)$ and thus everything generated by $(r_1, r_2, \dots, r_m)$, thus everything in N, is generated by the elements $(0, \dots, a_i, \dots, 0)$.

□

[Lecture 21 ends]

Theorem. Let R be a Euclidean domain and let N be a submodule of R^m. Then there exists a basis $V_1, V_2, \dots, V_m$ of R_m such that N is generated by $d_1 v_1, \dots, d_r v_r$ for some $0 \leq r \leq m$ and $d_i \in R$ and d_i always divides d_{i+1}.

Proof. By the previous proposition N can be generated by $x_1, x_2, \dots, x_n$ for $n \leq m$. This is since every euclidean domain is a PID. Now consider the matrix that has columns $x_1, x_2, \dots, x_n$, then the module is the image of this matrix. Now put this matrix into smith normal form (we make it have a bunch of 0 columns as necessary to make it square).

Now these operations give us a new basis for N, and this is exactly the basis we claimed exists in the theorem. So done.

□

Theorem. For a Euclidean domain R, any submodule of R^m is free.

Proof. Recall that free means we have a linearly independent generating set. So the result follows from the previous theorem.

□

Theorem. Let R be a Euclidean domain. Let M be a finitely generated R-module. Then M is isomorphic to

$$R \oplus \dots \oplus R \oplus R/d_1 \oplus \dots \oplus R/d_r$$

where $d_i \neq 0,\ d_i | d_{i+1}$.

Proof. Let $\gamma : R^m \to M$ be a surjective homomorphism (since M is finitely generated). Now pick a basis $v_1, v_2, \dots, v_m$ such that $\ker(\gamma)$ is generated by $d_i v_i$ for i from 1 to r. So by the first isomorphism theorem we have that

$$M \cong R^m / (d_1 v_1, d_2 v_2, \dots, d_r v_r)$$

The ideal is also possibly generated by $0 v_i$ for i from r+1 to m. So this accounts for all the factors in

$$R \oplus \dots \oplus R \oplus R/d_1 \oplus \dots \oplus R/d_r$$

□

Theorem. When R=$\mathbb{Z}$ this gives a way to classify all abelian groups. We see that they are products of cyclic groups such that if you put their size in order then each one's size divides the size of the next one.

Now the classification of all finitely generated abelian groups is just $\mathbb{Z}^n \times$ (Finite abelian group).

Example. If we have an abelian group generated by 3 elements a,b,c such that $2a + 3b + c = 0$ and $a + 2b = 0$ and $5a + 6b + 7c = 0$, then we can write it as $\mathbb{Z}^3/\text{Span}\begin{pmatrix} 2 & 1 & 5 \\ 3 & 2 & 6 \\ 1 & 0 & 7 \end{pmatrix}$. We can calculate the smith normal form of this using fitting ideals, it turns out to be $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$, so we have the abelian group C_3.

Proposition. Let R be a Euclidean domain with a,b in R such that gcd(a,b)=1. Then

$$R/(ab) \cong (R/a) \times (R/b)$$

Proof. Consider $\phi : R/(a) \bigoplus R/(b) \to R/(ab)$ that sends

$$(r_1 + (a), r_2 + (b)) \to (br_1 + ar_2 + ab)$$

This is well defined (easy to check), and it is surjective because $ax + by = 1$ for some x and y, by the euclidean algorithm and the gcd property, so this is surjective as it follows that anything is in the image.

This is injective because if $br_1 + ar_2 = r_3ab$ (needed to be in the in the kernel), then we know that $a \,|ar_r, a|\, abr_3$, therefore $a|br_1$. But a is coprime to b so $a|r_1$. By the same argument $b|r_2$. Therefore we have the identity element of $R/(a) \bigoplus R/(b)$. Therefore the kernel is trivial, so injective, so done.

□

Theorem. Let R be a Euclidean domain and let M be a finitely generated R-module. Then M is isomorphic to

$$N_1 \oplus \cdots \oplus N_t$$

where N_i is either R or $R/(p^n)$ for some prime p and some $n \in \mathbb{N}$.

Proof. Take $R \oplus \cdots \oplus R \oplus R/d_1 \oplus \cdots \oplus R/d_r$. Write each d_i as a product of prime powers and apply the previous proposition.

□

Now fix a vector space V over a field F. Fix α as a linear transformation from V to V. Make V into an $F[x]$ module by sending $(f, v) \to f(\alpha)\, v$. Call this module V_α.

Observe that if the dimension of V is finite then V_α is finitely generated as an F[x] module.

Example. Suppose $V_\alpha \cong F[x]/(x^r)$ as an $F[x]$-module. Then they are automatically isomorphic as F-modules. The right hand side has basis $\left(1, x, x^2, \ldots, x^{r-1}\right)$, and the left hand side is a vector space over F with a corresponding basis. But now the endomorphism α sends $f \bmod x^r \to xf \bmod x^r$.

Under this basis, α has the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

Which means we have successfully reproduced the proof of jordan normal form for nilpotent matrices that I gave in vectors and matrices, only difference is it was layered in a bunch of abstract nonsense.

[Lecture 22 ends]

Example. Let p be a polynomial and suppose $V_\alpha \cong F[x]/p(x)$ where deg(p)=r. Then there is a basis for the RHS given by $\left(1, x, x^2, \ldots, x^{r-1}\right)$. If

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + 1x^r$$

then the matrix for the map from $F[x]/p(x) \to F[x]/p(x)$ given by multiplication by x is given by

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{r-1} \end{pmatrix}$$

This means that since α is multiplication by x under the given isomorphism, there is a basis for V where α takes this form.

Theorem. (Rational canonical form) Let α be an endomorphism on V (ie a map from V to V). Then

$$V_\alpha \cong \frac{F[x]}{(f_1)} \bigoplus \cdots \bigoplus \frac{F[x]}{(f_s)}$$

where each one divides the next one and there exists a basis of V such that α is (in block form) $(C(f_1), C(f_2), \ldots, C(f_s))$ where C is the companion matrix, ie the matrix as in the above example. Here $f_i | f_{i+1}$ for every i.

Proof. Apply the classicification theorem for modules over Euclidean domains. Here we are viewing V_α as a finitely generated F[x]-module.

□

Theorem. (Jordan canonical form)

Let α be an endomorphism on V with V a vector space over $\mathbb{C}$. Then $V_\alpha \cong \bigoplus \frac{\mathbb{C}[x]}{(x-\lambda_i)^{a_i}}$ where i goes from 1 to t for some t.

Proof. Apply the prime powers version of the classification theorem.

□

This actually works for any field which is algebraically closed, meaning we can factor any polynomial into degree 1 polynomials.

We will now talk a bit about multivariable polynomial rings.

Let K be a field and consider its polynomial ring in n variables. Given polynomials $f_1, f_2, \ldots, f_s$ and another polynomial f we want to determine when f is contained in the ideal $(f_1, f_2, \ldots, f_s)$.

In the case of one variable every ideal is principal so we just need f to be divisble by the gcd.

Consider the example in K[x,y] of the ideal generated by $\left(x^2 + y^2 + 1, x - y\right)$. Ideals are not necessarily principle here. It is difficult to decide if something is in this ideal.

We will say that $x^a y^b \succ x^c y^d$ if $a > c$ or $a = c$ and $b > d$. Its like the alphabetical ordering. As an example, $x^3 > x^2 y > xy^5 > y^{100}$.

This allows you to define the concept of a leading term.

We now basically have a Euclidean algorithm where instead of over $\mathbb{Z}$ but it is over $\mathbb{Z}^2$, which is still well ordered with the alphabetical ordering. We can write $f = a_1 f_1 + \cdots + a_s f_s + r$ where no term of r is divisible by any leading term of any f_i.

We hope that r is 0 if and only if f is in the ideal. However, unfortunately, only the "only if" direction is true.

Definition. A generating set $g_1, \ldots, g_t$ for an ideal I is a Grobner basis if every polynomial in I has a leading term divisible by the leading term of some g_i.

If we can find a Grobner basis for an ideal, we would be done. There is an algorithm to find a Grobner basis.

The problem is cancellation of leading terms in the generating set. Given f, g, define $S(f, g)$ as

$$\frac{LCM\left(LT\left(f\right), LT\left(g\right)\right)}{LT(f)} f - \frac{LCM\left(LT\left(f\right), LT\left(g\right)\right)}{LT(g)} g$$

Start with the generating set $\{f_1, \ldots, f_s\}$. Repeat the following:

Step 1: For each f, g pair in the generating set, compute the S polynomial.

Step 2: Divide $S(f, g)$ by everything in the generating set using the same algorithm as above. If the remainder is non-zero, add that remainder to the generating set.

Continue until all S-polynomials are 0.

This terminates by theHhilbert basis theorem.

This gives a Grobner basis because it solves the problem of cancellation of leading terms by adding what any new leading terms would be if they cancelled.

[Lecture 23 ends]